Algebra & Number Theory

Volume 13

2019

No. 9

A probabilistic approach to systems of parameters and Noether normalization

Juliette Bruce and Daniel Erman

msp

ALGEBRA AND NUMBER THEORY 13:9 (2019)
dx.doi.org/10.2140/ant.2019.13.2081

A probabilistic approach to systems of parameters and Noether normalization

Juliette Bruce and Daniel Erman

We study systems of parameters over finite fields from a probabilistic perspective and use this to give the first effective Noether normalization result over a finite field. Our central technique is an adaptation of Poonen's closed point sieve, where we sieve over higher dimensional subvarieties, and we express the desired probabilities via a zeta function-like power series that enumerates higher dimensional varieties instead of closed points. This also yields a new proof of a recent result of Gabber, Liu and Lorenzini (2015) and Chinburg, Moret-Bailly, Pappas and Taylor (2017) on Noether normalizations of projective families over the integers.

Given an n-dimensional projective scheme $X \subseteq \mathbb{P}^r$ over a field, Noether normalization says that we can find homogeneous polynomials that induce a finite morphism $X \to \mathbb{P}^n$. Such a morphism is determined by a system of parameters, namely by choosing homogeneous polynomials $f_0, f_1, \dots, f_n$ of degree d where $X \cap V(f_0, f_1, \dots, f_n) = \varnothing$. Such a system of polynomials $f_0, f_1, \dots, f_n$ is a system of parameters on the homogeneous coordinate ring of X. More generally, for $k \leq n$ we say that $f_0, f_1, \dots, f_k$ *are parameters on* X if

$$\dim \mathbb{V}(f_0, f_1, \dots, f_k) \cap X = \dim X - (k+1).$$

By convention, the empty set has dimension -1.

Over an infinite field any generic choice of $\leq n+1$ linear polynomials will automatically be parameters on X. Over a finite field we can ask:

Questions 1.1. Let $\mathbb{F}_q$ be a finite field and $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ be an n-dimensional closed subscheme:

(1) What is the probability that a random choice $f_0, f_1, \dots, f_k$ of polynomials of degree d will be parameters on X?

(2) Can one effectively bound the degrees d for which such a finite morphism exists?

We will provide new insight into these questions by studying the distribution of systems of parameters from both a geometric and probabilistic viewpoint.

The first author was partially supported by the NSF GRFP under Grant No. DGE-1256259. The second author was partially supported by NSF grants DMS-1302057 and DMS-1601619.
MSC2010: primary 13B02; secondary 11G25, 14D10, 14G10, 14G15.
Keywords: Noether normalization, system of parameters, closed point sieve.

For the geometric side, we fix a field $\boldsymbol{k}$ and let $S = \boldsymbol{k}[x_0, x_1, \dots, x_r]$ be the coordinate ring of $\mathbb{P}^r_{\boldsymbol{k}}$. We write S_d for the vector space of degree d polynomials in S. In Section 4, we define a scheme $\mathscr{D}_{k,d}(X)$ parametrizing collections that do not form parameters. The $\boldsymbol{k}$-points of $\mathscr{D}_{k,d}(X)$ are

$$\mathscr{D}_{k,d}(X)(\boldsymbol{k}) = \{(f_0, f_1, \dots, f_k) \text{ that are } \textit{not} \text{ parameters on } X\} \subset \underbrace{S_d \times \cdots \times S_d}_{k+1 \text{ copies}}.$$

We prove an elementary bound on the codimension of these closed subschemes of the affine space $S_d^{\oplus k+1}$.

Theorem 1.2. *Let $X \subseteq \mathbb{P}^r_{\boldsymbol{k}}$ be an n-dimensional closed subscheme. We have*:

$$\operatorname{codim} \mathscr{D}_{k,d}(X) = \begin{cases} \geq \binom{n-k+d}{n-k} & \text{if } k < n, \\ = 1 & \text{if } k = n. \end{cases}$$

This generalizes several results from the literature: the case $k = n$ is a classical result about Chow forms [Gelfand et al. 1994, 3.2.B]. For $d = 1$ and $k < n$, the bound is sharp, by a classical result about determinantal varieties.[1] The bound for the case $k = 0$ appears in [Benoist 2011, Lemme 3.3]. If $k < n$, then the codimension grows as $d \to \infty$ and this factors into our asymptotic analysis over finite fields. It also leads to a uniform convergence result that allows us to go from a finite field to $\mathbb{Z}$.

For the probabilistic side, we work over a finite field $\mathbb{F}_q$ and compute the asymptotic probability that random polynomials $f_0, f_1, \dots, f_k$ of degree d are parameters on X. The following result, which follows from known results in the literature, shows that there is a bifurcation between the $k = n$ and $k < n$ cases, reflecting Theorem 1.2.

Theorem 1.3 [Bucur and Kedlaya 2012; Poonen 2013]. *Let $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ be an n-dimensional closed subscheme. The asymptotic probability that random polynomials $f_0, f_1, \dots, f_k$ of degree d are parameters on X is*

$$\lim_{d\to\infty} \operatorname{Prob}(f_0, f_1, \dots, f_k \textit{ of degree } d \textit{ are parameters on } X) = \begin{cases} 1 & \text{if } k < n, \\ \zeta_X(n+1)^{-1} & \text{if } k = n, \end{cases}$$

where $\zeta_X(s)$ is the arithmetic zeta function of X.

The maximal case $k = n$ follows from the $k = m + 1$ case of Bucur and Kedlaya [2012, Theorem 1.2] (though they assume that X is smooth, their proof does not need that assumption when $k = m + 1$) and is proven using Poonen's closed point sieve. Moreover, the result in both cases could be derived from a slight modification of [Poonen 2013, Proof of Theorem 2.1]. See also [Charles and Poonen 2016, Corollary 1.4] for a similar result.

The main results in our paper stem from a deeper investigation of the cases where $k < n$, as the limiting value of 1 is only the beginning of the story. In the following theorem, we use $|Z|$ to denote the number of irreducible components of a scheme Z, and we write $\dim Z \equiv k$ if Z is equidimensional of dimension k.

[1] See [Bruns and Vetter 1988, Theorem 2.5] for a modern statement and proof. That result has a complicated history, discussed in [Bruns and Vetter 1988, Section 2.E], with some cases dating as far back as [Macaulay 1916, Section 53].

Theorem 1.4. *Let $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ be a projective scheme of dimension n. Fix e and let $k < n$. The probability that random polynomials $f_0, f_1, \dots, f_k$ of degree d are parameters on X is*

$$\operatorname{Prob}\left(\begin{array}{l} f_0, f_1, \dots, f_k \text{ of degree } d \\ \text{are parameters on } X \end{array}\right) = 1 - \sum_{\substack{Z \subseteq X \text{ reduced} \\ \dim Z \equiv n-k \\ \deg Z \leq e}} (-1)^{|Z|-1} q^{-(k+1)h^0(Z, \mathcal{O}_Z(d))} + o(q^{-e(k+1)\binom{n-k+d}{n-k}}).$$

Theorem 1.4 illustrates that the probability of finding a sequence $f_0, f_1, \dots, f_k$ of parameters on X is intimately tied to the codimension k geometry of X. Note that, by basic properties of the Hilbert polynomial, as $d \to \infty$ we have

$$h^0(Z, \mathcal{O}_Z(d)) = \frac{\deg(Z)}{(n-k)!} d^{n-k} + o(d^{n-k}) = \deg(Z) \binom{n-k+d}{n-k} + o(d^{n-k}).$$

It follows that the term $q^{-(k+1)h^0(Z, \mathcal{O}_Z(d))}$ lies in $o(q^{-e(k+1)\binom{n-k+d}{n-k}})$ if and only if $\deg(Z) > e$.

For instance, setting $e = 1$, the sum simplifies to $1 - N \cdot q^{-(k+1)\binom{n-k+d}{n-k}} + o(q^{-(k+1)\binom{n-k+d}{n-k}})$, where N is the number of $(n-k)$-dimensional linear subspaces lying in X. It would thus be more difficult to find parameters on a variety X containing lots of linear spaces, as illustrated in Example 8.1. More generally, the probability of finding parameters for $k < n$ depends on a power series that counts the number of $(n-k)$-dimensional subvarieties of varying degrees, in analogue with the appearance of the zeta function in the $k = n$ case.

Our approach to Theorem 1.4 is motivated by a simple observation: $f_0, f_1, \dots, f_k$ fail to be parameters if and only if they all vanish along some $(n-k)$-dimensional subvariety of X. We thus develop an analogue of Poonen's sieve where closed points are replaced by $(n-k)$-dimensional varieties. Sieving over higher dimensional varieties presents new challenges, especially bounding the error. This error depends on the Hilbert function of these varieties, and one key innovation is a uniform lower bound for Hilbert functions given in Lemma 3.1.

This perspective also leads to our second main result: an answer to Questions 1.1.(2) where the bound is in terms of the sum of the degrees of the irreducible components. If $X \subseteq \mathbb{P}^r$ has minimal irreducible components $V_1, V_2, \dots, V_s$ (considered with the reduced scheme structure), then we define $\widehat{\deg}(X) := \sum_{i=1}^s \deg(V_i)$ (see Definition 2.2). We set $\log_q 0 = -\infty$.

Theorem 1.5. *Let $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ where $\dim X = n$. If $\max\{d, \frac{q}{d^n}\} \geq \widehat{\deg}(X)$ and*

$$d > \log_q \widehat{\deg}(X) + \log_q n + n \log_q d$$

then there exist $f_0, f_1, \dots, f_n$ of degree d^{n+1} inducing a finite morphism $\pi : X \to \mathbb{P}^n_{\mathbb{F}_q}$.

The bound is asymptotically optimal in q. Namely, if we fix $\widehat{\deg}(X)$, then as $q \to \infty$, the bound becomes $d = 1$. Thus, a linear Noether normalization exists if $q \gg \widehat{\deg}(X)$. For a fixed q, we expect the bound could be significantly improved. (Even the case $\dim X = 0$ would be interesting, as it is related to Kakeya type problems over finite fields [Ellenberg and Erman 2016; Ellenberg et al. 2010].)

Theorem 1.5 provides the first explicit bound for Noether normalization over a finite field. (One could potentially derive an explicit bound from Nagata's argument [1962, Chapter I.14], though the inductive nature of that construction would at best yield a bound that is multiply exponential in the largest degree of a defining equation of X.)

After computing the probabilities over finite fields, we combine these analyses and characterize the distribution of parameters on projective B-schemes where $B = \mathbb{Z}$ or $\mathbb{F}_q[t]$. We use standard notions of density for a subset of a free B-module; see Definition 7.1.

Corollary 1.6. *Let $B = \mathbb{Z}$ or $\mathbb{F}_q[t]$. If $X \subseteq \mathbb{P}^r_B$ is a closed subscheme whose general fiber over B has dimension n, then*

$$\lim_{d\to\infty} \text{Density}\left\{\begin{array}{l} f_0, f_1, \ldots, f_k \textit{ of degree } d \textit{ that} \\ \textit{restrict to parameters on } X_p \textit{ for all } p \end{array}\right\} = \begin{cases} 1 & \textit{if } k < n, \\ 0 & \textit{if } k = n \textit{ and all } d. \end{cases}$$

The density over B thus equals the product over all the fibers of the asymptotic probabilities over $\mathbb{F}_q$. In the case $B = \mathbb{Z}$, our proof relies on Ekedahl's infinite Chinese remainder theorem [Ekedahl 1991, Theorem 1.2] combined with Proposition 5.1, which illustrates uniform convergence in p for the asymptotic probabilities in Theorem 1.3. In the case $B = \mathbb{F}_q[t]$, we use Poonen's analogue of Ekedahl's result [Poonen 2003, Theorem 3.1].

When $k = n$, an analogue of Corollary 1.6 for smoothness is given by Poonen [2004, Theorem 5.13]. Moreover, while it is unknown if there are any smooth hypersurfaces of degree > 2 over $\mathbb{Z}$ (see for example the discussion in [Poonen 2009]), the density zero subset from Corollary 1.6 turns out to be nonempty for large d. This leads to a new proof of a recent result about uniform Noether normalizations.

Corollary 1.7. *Let $B = \mathbb{Z}$ or $\mathbb{F}_q[t]$. Let $X \subseteq \mathbb{P}^r_B$ be a closed subscheme. If each fiber of X over B has dimension n, then for some d, there exist homogeneous polynomials $f_0, f_1, \ldots, f_n \in B[x_0, x_1, \ldots, x_r]$ of degree d inducing a finite morphism $\pi : X \to \mathbb{P}^n_B$.*

Corollary 1.7 is a special case of a recent result of Chinburg, Moret-Bailly, Pappas and Taylor [2017, Theorem 1.2] and of Gabber, Liu and Lorenzini [2015, Theorem 8.1]. This corollary can fail when B is any of $\mathbb{Q}[t]$ or $\mathbb{Z}[t]$ or $\mathbb{F}_q[s, t]$, as in those cases, the Picard group of a finite cover of Spec B can fail to be torsion. See Section 8 for explicit examples and counterexamples and see [Chinburg et al. 2017; Gabber et al. 2015] for generalizations and applications.

There are a few earlier results related to Noether normalization over the integers. For instance [Moh 1979] shows that Noether normalizations of semigroup rings always exist over $\mathbb{Z}$; and [Nagata 1962, Theorem 14.4] implies that given a family over any base, one can find a Noether normalization over an open subset of the base. Relative Noether normalizations play a key role in [Achinger 2015, Section 5]. There is also the incorrect claim in [Zariski and Samuel 1960, page 124] that Noether normalizations exist over any infinite domain (see [Abhyankar and Kravitz 2007]). Brennan and Epstein [2011] analyze the distribution of systems of parameters from a different perspective, introducing the notion of a generic matroid to relate various different systems of parameters. In addition, after our paper was posted, work of

Charles [2017] on arithmetic Bertini theorems appeared which, under the additional hypothesis that X is integral and flat, implies a stronger version of Corollary 1.6 where one also obtains bounds on the norms of the functions.

This paper is organized as follows. Section 2 gathers background results and Section 3 involves a key lower bound on Hilbert functions. Section 4 contains our geometric analysis of parameters including a proof of Theorem 1.2. Sections 5 and 6 contain the probabilistic analysis of parameters over finite fields: Section 5 proves Theorem 1.3 and Theorem 1.5 while Section 6 gives the more detailed description via an analogue of the zeta function enumerating $(n-k)$-dimensional subvarieties, including the proof of Theorem 1.4. Section 7 contains our analysis over $\mathbb{Z}$ including proofs of Corollaries 1.6 and 1.7 and related corollaries. Section 8 contains examples.

2. Background

In this section, we gather some algebraic and geometric facts that we will cite throughout.

Lemma 2.1. *Let $\boldsymbol{k}$ be a field and let R be a $(k+1)$-dimensional graded $\boldsymbol{k}$-algebra where $R_0 = \boldsymbol{k}$. If $f_0, f_1, \dots, f_k$ are homogeneous elements of degree d and $R/\langle f_0, f_1, \dots, f_k\rangle$ has finite length, then the extension $\boldsymbol{k}[z_0, z_1, \dots, z_k] \to R$ given by $z_i \mapsto f_i$ is a finite extension.*

Proof. See [Bruns and Herzog 1993, Theorem 1.5.17]. □

This lemma implies that if $X \subseteq \mathbb{P}^r_{\boldsymbol{k}}$ has dimension n, and if $f_0, f_1, \dots, f_n$ are parameters on X, then the map $\phi\colon X \to \mathbb{P}^n_{\boldsymbol{k}}$ given by sending $x \mapsto [f_0(x) : f_1(x) : \cdots : f_n(x)]$ is a finite morphism. In particular, if R is the homogeneous coordinate of X, then the ideal $\langle f_0, f_1, \dots, f_n\rangle \subseteq R$ has finite colength, and thus the base locus of ϕ is the empty set. In other words, ϕ defines a genuine morphism. Moreover, the lemma shows that the corresponding map of coordinate rings $\phi^\sharp : R \to \boldsymbol{k}[z_0, z_1, \dots, z_n]$ is finite, and this implies that ϕ is finite.

Definition 2.2. Let $X \subseteq \mathbb{P}^r$ be a projective scheme with minimal irreducible components $V_1, \dots, V_s$ (considered with the reduced scheme structure). We define $\widehat{\deg}(X) := \sum_{i=1}^{s} \deg(V_i)$. For a subscheme $X' \subseteq \mathbb{A}^r$ with projective closure $\overline{X}' \subseteq \mathbb{P}^r$ we define $\widehat{\deg}(X') := \widehat{\deg}(\overline{X}')$.

This provides a notion of degree which ignores nonreduced structure but takes into account components of lower dimension. Similar definitions have appeared in the literature: for instance, in the language of [Bayer and Mumford 1993, Section 3], we would have $\widehat{\deg}(X) = \sum_{j=0}^{\dim X} \text{geom-deg}_j(X)$.

Lemma 2.3. *Let $\boldsymbol{k}$ be any field and let $X \subseteq \mathbb{A}^r_{\boldsymbol{k}}$. Let $f_0, f_1, \dots, f_t$ be polynomials in $\boldsymbol{k}[x_1, \dots, x_r]$. If $X' = X \cap \mathbb{V}(f_0, f_1, \dots, f_t)$, then $\widehat{\deg}(X') \le \widehat{\deg}(X) \cdot \prod_{i=0}^{t} \deg(f_i)$.*

Proof. This follows from the refined version of Bezout's theorem [Fulton 1984, Example 12.3.1]. □

3. A uniform lower bound on Hilbert functions

For a subscheme of $\mathbb{P}^r$, the Hilbert function in degree d is controlled by the Hilbert polynomial, at least if d is very large related to some invariants of the subscheme. We analyze the Hilbert function at the other extreme, where the degree of the subscheme may be much larger than d. The following lemma, which applies to subschemes of arbitrarily high degree, provides uniform lower bounds that are crucial to bounding the error in our sieves.

Lemma 3.1. *Let $\boldsymbol{k}$ be an arbitrary field and fix some $e \geq 0$. Let $V \subseteq \mathbb{P}^r_{\boldsymbol{k}}$ be any closed, m-dimensional subscheme of degree $> e$ with homogeneous coordinate ring R:*

(1) *We have* $\dim R_d \geq h^0(\mathbb{P}^m, \mathcal{O}_{\mathbb{P}^m}(d))$ *for all d.*

(2) *For any $0 < \epsilon < 1$, there exists a constant C depending only on m and ϵ (but not on d or $\boldsymbol{k}$ or R) such that*
$$\dim R_d > (e+\epsilon)\cdot h^0(\mathbb{P}^m, \mathcal{O}_{\mathbb{P}^m}(d))$$
for all $d \geq Ce^{m+1}$.

Proof. If $\boldsymbol{k}'$ is a field extension of $\boldsymbol{k}$, then the Hilbert series of R is the same as the Hilbert series of $R \otimes_{\boldsymbol{k}} \boldsymbol{k}'$. We can thus assume that $\boldsymbol{k}$ is an infinite field. For part (1), we simply take a linear Noether normalization $\boldsymbol{k}[t_0, t_1, \dots, t_m] \subseteq R$ of the ring R [Eisenbud 1995, Theorem 13.3]. This yields $\boldsymbol{k}[t_0, t_1, \dots, t_m]_d \subseteq R_d$, giving the statement about Hilbert functions.

We prove part (2) of the lemma by induction on m. Let $S = \boldsymbol{k}[x_0, x_1, \dots, x_r]$ and let $I_V \subseteq S$ be the saturated, homogeneous ideal defining V. Thus $R = S/I_V$. If $m = 0$, then we have $\dim R_d \geq \min\{d+1, \deg V\} \geq \min\{d+1, e+1\}$ which is at least $e+\epsilon$ for all $d \geq e$. This proves the case $m = 0$, where the constant C can be chosen to be 1.

Now assume the claim holds for all closed subschemes of dimension less than m. Let $V \subset \mathbb{P}^r_{\boldsymbol{k}}$ be a closed subscheme with $\dim V = m \geq 1$. Fix $0 < \epsilon < 1$. Since we are working over an infinite field, [Eisenbud 1995, Lemma 13.2(c)] allows us to choose a linear form ℓ that is a nonzero divisor in R. This yields a short exact sequence $0 \to R(-1) \xrightarrow{\cdot \ell} R \to R/\ell \to 0$. Since $R/\ell = S/(I_V + \langle \ell \rangle)$, this yields the equality
$$\dim R_i = \dim R_{i-1} + \dim(S/(I_V + \langle \ell \rangle))_i. \tag{1}$$

Letting $W = V \cap V(\ell)$ we know that $\dim W = m-1$ and $\deg W = \deg V$. Moreover, if I_V is the saturated ideal defining V and if I_W is the saturated ideal defining W, then since I_W contains $I_V + \langle \ell \rangle$, we have $\dim(S/(I_V + \langle \ell \rangle))_i \geq \dim(S/I_W)_i$. Combining with (1) yields
$$\dim R_i \geq \dim R_{i-1} + \dim(S/I_W)_i. \tag{2}$$

Now, by induction, in the case $m-1$ and $\epsilon' := \frac{1+\epsilon}{2}$, there exists C' depending on ϵ' and $m-1$ (or equivalently depending on ϵ and m) where
$$\dim(S/I_W)_i \geq (e+\epsilon')\binom{m-1+i}{m-1} \tag{3}$$

for all $i \geq C'e^m$. Now let $d \geq C'e^m$. Iteratively applying (2) for $i = d, d-1, d-2, \ldots, \lceil C'e^m \rceil$, we obtain:

$$\dim R_d \geq \dim R_{\lceil C'e^m \rceil - 1} + \sum_{i=\lceil C'e^m \rceil}^{d} \dim(S/I_W)_i.$$

By dropping the $\dim R_{\lceil C'e^m \rceil - 1}$ term and applying (3), we conclude that

$$\dim R_d \geq \sum_{i=\lceil C'e^m \rceil}^{d} (e+\epsilon')\binom{m-1+i}{m-1}.$$

The identity $\sum_{i=a}^{b} \binom{i+k}{k} = \binom{b+k+1}{k+1} - \binom{a+k}{k+1}$ implies that $\sum_{i=\lceil C'e^m \rceil}^{d} (e+\epsilon')\binom{m-1+i}{m-1}$ can be rewritten as $(e+\epsilon')\left(\binom{m+d}{m} - \binom{m-1+\lceil C'e^m \rceil}{m}\right)$. There exists a constant C depending on ϵ and m so that $(\epsilon' - \epsilon)\binom{m+d}{m} = \left(\frac{1}{2} - \frac{\epsilon}{2}\right)\binom{m+d}{m} \geq (e+\epsilon')\binom{m-1+\lceil C'e^m \rceil}{m}$ for all $d \geq \lceil Ce^{m+1} \rceil$. Thus, for all $d \geq \lceil Ce^{m+1} \rceil$ we have

$$\dim R_d \geq (e+\epsilon')\binom{m+d}{m} - (\epsilon' - \epsilon)\binom{m+d}{d} = (e+\epsilon)\binom{m+d}{m}. \qquad \square$$

Remark 3.2. Asymptotically in e, the bound of Ce^2 is the best possible for curves. For instance, let $C \subseteq \mathbb{P}^r$ be a curve of degree $(e+1)$ lying inside some plane $\mathbb{P}^2 \subseteq \mathbb{P}^r$. Let R be the homogeneous coordinate ring of C. If $d \geq e$ then the Hilbert function is given by

$$\dim R_d = (e+1)d - \tfrac{e^2-e}{2}.$$

Thus, if we want $\dim R_d \geq (e+\epsilon)(d+1)$, we will need to let $d \geq (e^2+e+2\epsilon)/(2(1-\epsilon)) \approx \frac{1}{2}e^2$. It would be interesting to know if the bound Ce^{m+1} is the best possible for higher dimensional varieties.

4. Geometric analysis

In this section we analyze the geometric picture for the distribution of parameters on X. The basic idea behind the proof of Theorem 1.2 is that $f_0, f_1, \ldots, f_k$ fail to be parameters on X if and only if they all vanish along some $(n-k)$-dimensional subvariety of X. Since the Hilbert polynomial of a $(n-k)$-dimensional variety grows like d^{n-k}, when we restrict a degree d polynomial f_j to such a subvariety, it can be written in terms of $\approx d^{n-k}$ distinct monomials. The polynomial f_j will all vanish along the subvariety if and only if all of the $\approx d^{n-k}$ coefficients vanish. This rough estimate explains the growth of the codimension of $\mathscr{D}_{k,d}(X)$ as $d \to \infty$.

We begin by constructing the schemes $\mathscr{D}_{k,d}(X)$. Fix $X \subseteq \mathbb{P}^r_{\boldsymbol{k}}$ a closed subscheme of dimension n over a field $\boldsymbol{k}$. Given $k < n$ and $d > 0$, let $\mathscr{A}_{k,d}$ be the affine space $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(d))^{\oplus k+1}$ and $\boldsymbol{k}[c_{0,1}, \ldots, c_{k,\binom{r+d}{d}}]$ be the corresponding polynomial ring. We enumerate the monomials in $H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(d))$ as $m_1, \ldots, m_{\binom{r+d}{d}}$, and then define the universal polynomial

$$F_i := \sum_{j=1}^{\binom{r+d}{d}} c_{i,j} m_j \in \boldsymbol{k}[c_{0,1}, \ldots, c_{k,\binom{r+d}{d}}] \otimes_{\boldsymbol{k}} \boldsymbol{k}[x_0, x_1, \ldots, x_r].$$

Given a closed point $c \in \mathscr{A}_{k,d}$ we can specialize $F_0, F_1, \dots, F_k$ and obtain polynomials $f_0, f_1, \dots, f_k \in \kappa(c)[x_0, x_1, \dots, x_r]$, where $\kappa(c)$ is the residue field of c. We will thus identify each element of $\mathscr{A}_{k,d}(\boldsymbol{k})$ with a collection of polynomials $\boldsymbol{f} = (f_0, f_1, \dots, f_k) \in \boldsymbol{k}[x_0, x_1, \dots, x_r]$.

Now define $\Sigma_{k,d}(X) \subseteq X \times \mathscr{A}_{k,d}$ via the equations $F_0, F_1, \dots, F_k$. Consider the second projection $p_2 \colon \Sigma_{k,d}(X) \to \mathscr{A}_{k,d}$. Given a point $\boldsymbol{f} = (f_0, f_1, \dots, f_k) \in \mathscr{A}_{k,d}$, the fiber $p_2^{-1}(\boldsymbol{f}) \subseteq X$ can be identified with the points lying in $X \cap \mathbb{V}(f_0, f_1, \dots, f_k)$. For generic choices of $\boldsymbol{f}$ (after passing to an infinite field if necessary) the polynomials $f_0, f_1, \dots, f_k$ will define an ideal of codimension $k+1$, and thus the fiber $p_2^{-1}(\boldsymbol{f})$ will have dimension $n-k-1$.

There is a closed sublocus $\mathscr{D}_{k,d}(X) \subsetneq \mathscr{A}_{k,d}$ where the dimension of the fiber is at least $n-k$, and we give $\mathscr{D}_{k,d}(X)$ the reduced scheme structure. It follows that $\mathscr{D}_{k,d}(X)$ parametrizes collections $\boldsymbol{f} = (f_0, f_1, \dots, f_k)$ of degree d polynomials which fail to be parameters on X.

Remark 4.1. If we fix $X_{\mathbb{Z}} \subseteq \mathbb{P}^r_{\mathbb{Z}}$, then we can follow the same construction to obtain a scheme $\mathscr{D}_{k,d}(X_{\mathbb{Z}}) \subseteq \mathscr{A}_{k,d}$. Writing $X_{\boldsymbol{k}}$ as the pullback $X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\boldsymbol{k}$, we observe that the equations defining $\Sigma_{k,d}(X_{\boldsymbol{k}})$ are obtained by pulling back the equations defining $\Sigma_{k,d}(X_{\mathbb{Z}})$. It follows that $\mathscr{D}_{k,d}(X_{\mathbb{Z}}) \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}(\boldsymbol{k})$ has the same set-theoretic support as $\mathscr{D}_{k,d}(X_{\boldsymbol{k}})$.

Definition 4.2. We let $\mathscr{D}^{\text{bad}}_{k,d}(X)$ be the locus of points in $\mathscr{D}_{k,d}(X)$ where $f_0, f_1, \dots, f_{k-1}$ already fail to be parameters on X and let $\mathscr{D}^{\text{good}}_{k,d}(X) := \mathscr{D}_{k,d}(X) \setminus \mathscr{D}^{\text{bad}}_{k,d}(X)$. We set $\mathscr{D}^{\text{bad}}_{0,d}(X) = \varnothing$.

Remark 4.3. We have a factorization:

$$\begin{aligned} \mathscr{A}_{k,d} &\to \mathscr{A}_{k-1,d} \times \mathscr{A}_{0,d} \\ (f_0, f_1, \dots, f_k) &\mapsto ((f_0, f_1, \dots, f_{k-1}), f_k). \end{aligned}$$

We let $\pi : \mathscr{D}_{k,d}(X) \to \mathscr{A}_{k-1,d}$ be the induced projection, which will we use to work inductively.

Proof of Theorem 1.2. First consider the case $k = n$. There is a natural rational map from $\mathscr{A}_{n,d}$ to the Grassmanian $\operatorname{Gr}(n+1, S_d)$ given by sending the point $(f_0, f_1, \dots, f_n) \in \mathscr{A}_{n,d}$ to the linear space that those polynomials span. Inside of the Grassmanian, the locus of choices of $(f_0, f_1, \dots, f_n)$ that all vanish on a point of X is a divisor in the Grassmanian defined by the Chow form; see [Gelfand et al. 1994, 3.2.B]. The preimage of this hypersurface in $\mathscr{A}_{n,d}$ is a hypersurface contained in $\mathscr{D}_{n,d}(X)$, and thus $\mathscr{D}_{n,d}(X)$ has codimension 1.

For $k < n$, we will induct on k. Let $k = 0$. A polynomial f_0 will fail to be a parameter on X if and only if $\dim X = \dim(X \cap \mathbb{V}(f_0))$. This happens if and only if f_0 is a zero divisor on a top-dimensional component of X. Let V be the reduced subscheme of some top-dimensional irreducible component of X and let $\mathcal{I}_V$ be the defining ideal sheaf of V. Then the set of zero divisors of degree d on V will form a linear subspace in $\mathscr{A}_{0,d}$ corresponding to the elements of the vector subspace $H^0(\mathcal{I}_V(d))$. The codimension of $H^0(\mathcal{I}_V(d)) \subseteq S_d$ is precisely given by the Hilbert function of the homogeneous coordinate ring of V in degree d. By applying Lemma 3.1(1), we conclude that for all d this linear space has codimension at least $\binom{n+d}{d}$. Since $\mathscr{D}_{0,d}(X)$ is the union of these linear spaces over all top-dimensional components of X, this proves that $\operatorname{codim} \mathscr{D}_{0,d}(X) \geq \binom{n+d}{d}$.

Take the induction hypothesis that we have proven the statement for $\mathscr{D}_{j,d}(X')$ for all $X' \subseteq \mathbb{P}^r$ and all $j \leq k-1$. We separate $\mathscr{D}_{k,d}(X) = \mathscr{D}_{k,d}^{\text{bad}}(X) \sqcup \mathscr{D}_{k,d}^{\text{good}}(X)$ and will show that each locus has sufficiently large codimension. We begin with $\mathscr{D}_{k,d}^{\text{bad}}(X)$. By using the factorization from Remark 4.3, we can realize $\mathscr{D}_{k,d}^{\text{bad}}(X) \subseteq \mathscr{A}_{k,d} \cong \mathscr{A}_{k-1,d} \times \mathscr{A}_{0,d}$. By definition of $\mathscr{D}_{k,d}^{\text{bad}}(X)$, the image of $\mathscr{D}_{k,d}^{\text{bad}}(X)$ in $\mathscr{A}_{k-1,d} \times \mathscr{A}_{0,d}$ is $\mathscr{D}_{k-1,d}(X) \times \mathscr{A}_{0,d}$. It follows that

$$\operatorname{codim}(\mathscr{D}_{k,d}^{\text{bad}}(X), \mathscr{A}_{k,d}) = \operatorname{codim}(\mathscr{D}_{k-1,d}(X), \mathscr{A}_{k-1,d}) \geq \binom{n-k+1+d}{n-k+1} \geq \binom{n-k+d}{n-k},$$

where the middle inequality follows by induction.

Now consider an arbitrary point $\boldsymbol{f} = (f_0, f_1, \ldots, f_k)$ in $\mathscr{D}_{k,d}^{\text{good}}(X)$. By definition, $f_0, f_1, \ldots, f_{k-1}$ are parameters on X, and thus $\pi(\boldsymbol{f}) \in \mathscr{A}_{k-1,d} \setminus \mathscr{D}_{k-1,d}(X)$. Using the splitting of Remark 4.3, the fiber of $\mathscr{D}_{k,d}^{\text{good}}(X)$ over $\boldsymbol{f}$ can be identified with $\mathscr{D}_{0,d}(X')$ where $X' := X \cap \mathbb{V}(f_0, f_1, \ldots, f_{k-1})$. Since $(f_0, f_1, \ldots, f_{k-1}) \notin \mathscr{D}_{k-1,d}(X)$, we have that $\dim X' = n-k$. The inductive hypothesis thus guarantees that $\operatorname{codim} \mathscr{D}_{0,d}(X') \geq \binom{\dim X'+d}{d} = \binom{n-k+d}{d}$. □

5. Probabilistic analysis, I: Proof of Theorem 1.3

The main result of this section is Proposition 5.1 which provides an effective bound for finding parameters, and which we will use to prove Theorem 1.5. We also use this to give a new proof of Theorem 1.3 for $k < n$. Throughout this section, we let $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ be a projective scheme of dimension n over a finite field $\mathbb{F}_q$. Recall that $S_d = H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(d))$. We define

$$\operatorname{Par}_{d,k} = \{f_0, f_1, \ldots, f_k \text{ that are parameters on } X\} \subset S_d^{k+1}.$$

In Theorem 1.3, we compute the following limit (which a priori might not exist):

$$\lim_{d\to\infty} \operatorname{Prob}(f_0, f_1, \ldots, f_k \text{ of degree } d \text{ are parameters on } X) := \lim_{d\to\infty} \frac{\#\operatorname{Par}_{d,k}}{\#S_d^{k+1}}.$$

Proposition 5.1. *If $k < n$ then*

$$\operatorname{Prob}(f_0, f_1, \ldots, f_k \textit{ of degree } d \textit{ are parameters on } X) \geq 1 - \widehat{\deg}(X)(1 + d + d^2 + \cdots + d^k) q^{-\binom{n-k+d}{n-k}}.$$

Proof. We induct on k and largely follow the structure of the proof of Theorem 1.2. First, let $k = 0$. A polynomial f_0 will fail to be a parameter on X if and only if it is a zero divisor on a top-dimensional component V of X. There are at most $\widehat{\deg}(X)$ many such components. As argued in the proof of Theorem 1.2, the set of zero divisors on V corresponds to the elements of $H^0(\mathbb{P}^r, \mathcal{I}_V(d))$ which has codimension at least $\binom{n+d}{d}$ in S_d. It follows that

$$\operatorname{Prob}(f_0 \text{ of degree } d \text{ is not a parameter on } X) \leq \widehat{\deg}(X) q^{-\binom{n+d}{d}}.$$

Now consider the induction step. We will separately compute the probability that $\boldsymbol{f} = (f_0, f_1, \ldots, f_k)$ lies in $\mathscr{D}_{k,d}^{\text{bad}}(X)$ and the probability that $\boldsymbol{f}$ lies in $\mathscr{D}_{k,d}^{\text{good}}(X)$. By definition, the projection π maps $\mathscr{D}_{k,d}^{\text{bad}}(X)$

onto $\mathscr{D}_{k-1,d}(X)$, and by induction

$$\begin{aligned}\operatorname{Prob}(\pi(\boldsymbol{f}) \in \mathscr{P}_{k-1,d}(X)(\mathbb{F}_q)) &\le \widehat{\deg}(X)(1+d+d^2+\cdots+d^{k-1})q^{-\binom{n-k+1+d}{n-k+1}} \\ &\le \widehat{\deg}(X)(1+d+d^2+\cdots+d^{k-1})q^{-\binom{n-k+d}{n-k}}.\end{aligned}$$

We now assume $\boldsymbol{f} \notin \mathscr{D}^{\text{bad}}_{k,d}(X)$. We thus have that $f_0, f_1, \dots, f_{k-1}$ are parameters on X. As in the proof of Theorem 1.2, the fiber $\pi^{-1}(\boldsymbol{f})$ can be identified with $\mathscr{D}_{0,d}(X')$ where $X' := X \cap \mathbb{V}(f_0, f_1, \dots, f_{k-1})$. By construction $\dim X' = n-k$ and by Lemma 2.3, $\widehat{\deg}(X') \le \widehat{\deg}(X) \cdot d^k$. Our inductive hypothesis thus implies that

$$\operatorname{Prob}\begin{pmatrix} (f_0, f_1, \dots, f_k) \in \mathscr{D}_{k,d}(X)(\mathbb{F}_q) \text{ given that} \\ (f_0, f_1, \dots, f_{k-1}) \notin \mathscr{D}_{k-1,d}(X)(\mathbb{F}_q) \end{pmatrix} \le \widehat{\deg}(X')q^{-\binom{n-k+d}{n-k}} \le \widehat{\deg}(X)\cdot d^k q^{-\binom{n-k+d}{n-k}}.$$

Combining the estimates for $\mathscr{D}^{\text{bad}}_{k,d}(X)$ and $\mathscr{D}^{\text{good}}_{k,d}(X)$ yields the proposition. □

Proof of Theorem 1.3. If $k < n$, then we apply Proposition 5.1 to obtain

$$\lim_{d\to\infty} \operatorname{Prob}\begin{pmatrix} f_0, f_1, \dots, f_k \text{ of degree } d \\ \text{are parameters on } X \end{pmatrix} \ge \lim_{d\to\infty} 1 - \widehat{\deg}(X)(d^0+d^1+\cdots+d^k)q^{-\binom{n-k+d}{n-k}} = 1.$$

Now let $k = n$. For completeness, we summarize the proof of [Bucur and Kedlaya 2012, Theorem 1.2]. We fix e, which will go to ∞, and separate the argument into low, medium, and high degree cases.

Low degree argument. For a zero dimensional subscheme Y, we have that S_d surjects on $H^0(Y, \mathcal{O}_Y(d))$ when $d \ge \deg Y - 1$ [Poonen 2004, Lemma 2.1]. So if $d > \deg P - 1$, the probability that $f_0, f_1, \dots, f_n$ all vanish at a closed point $P \in X$ is $1 - q^{-(n+1)\deg P}$. If $Y \subseteq X$ is the union of all points of degree $\le e$, and if $d \ge \deg Y - 1$, then the surjection onto $H^0(Y, \mathcal{O}_Y(d))$ implies that the probabilities at the points $P \in Y$ behave independently. This yields:

$$\operatorname{Prob}\begin{pmatrix} f_0, f_1, \dots, f_n \text{ of degree } d \text{ are parameters on } X \\ \text{at all points } P \in X \text{ where } \deg(P) \le e \end{pmatrix} = \prod_{\substack{P\in X \\ \deg(P)\le e}} 1 - q^{-(n+1)\deg P}.$$

Medium degree argument. Our argument is nearly identical to [Poonen 2004, Lemma 2.4], and covers all points whose degree lies in the range $\left[e+1, \frac{d}{n+1}\right]$. For any such point $P \in X$, S_d surjects onto $H^0(P, \mathcal{O}_P(d))$ and thus the probability that $f_0, f_1, \dots, f_n$ all vanish at P is $q^{-\ell(n+1)}$. By [Lang and Weil 1954], $\#X(\mathbb{F}_{q^\ell}) \le Kq^{\ell n}$ for some constant K independent of ℓ. We have

$$\begin{aligned}\operatorname{Prob}\begin{pmatrix} f_0, f_1, \dots, f_n \text{ of degree } d \text{ all vanish} \\ \text{at some } P \in X \text{ where } e < \deg(P) \le \left\lfloor \frac{d}{n+1} \right\rfloor \end{pmatrix} &\le \sum_{\ell=e+1}^{\left\lfloor \frac{d}{n+1} \right\rfloor} \#X(\mathbb{F}_{q^\ell})q^{-\ell(n+1)} \\ &\le \sum_{\ell=e+1}^{\infty} Kq^{\ell n}q^{-(n+1)\ell} \\ &= \frac{Kq^{-e-1}}{1-q^{-1}}.\end{aligned}$$

This tends to 0 as $e \to \infty$, and therefore does not contribute to the asymptotic limit.

High degree argument. By the case when $k = n-1$, we may assume that $f_0, f_1, \dots, f_{n-1}$ form a system of parameters with probability $1 - o(1)$. So we let V be one of the irreducible components of this intersection (over $\mathbb{F}_q$) and we let R be its homogeneous coordinate ring. If $\deg V \leq \frac{d}{n+1}$, then it can be ignored as we considered such points in the low and medium degree cases. Hence, we can assume $\deg V > \frac{d}{n+1}$. Since $\dim R_\ell \geq \min\{\ell+1, \deg R\}$ for all ℓ, the probability that f_n vanishes along V is at most $q^{-\lfloor d/(n+1)\rfloor - 1}$. Hence the probability of vanishing on some high degree point is bounded by $O(d^n q^{-\lfloor d/(n+1)\rfloor-1})$ which is $o(1)$ as $d \to \infty$.

Combining the various parts as $e \to \infty$, we see that the low degree argument converges to $\zeta_X(n+1)^{-1}$ and the contributions from the medium and high degree points go to 0. □

Remark 5.2. It might be interesting to consider variants of Theorem 1.3 that allow imposing conditions along closed subschemes, similar to Poonen's Bertini with Taylor coefficients [Poonen 2004, Theorem 1.2]. For instance, [Kedlaya 2005, Theorem 1] might be provable by such an approach, though this would be more complicated than the original proof.

Proposition 5.1 yields an effective bound on the degree of a full system of parameters over a finite field. Sharper bounds can be obtained if one allows the f_i to have different degrees.

Corollary 5.3. (1) *If d_1 satisfies $d_1^{n-1}q^{-d_1-1} < (n \cdot \widehat{\deg}(X))^{-1}$, then there exist $g_0, g_1, \dots, g_{n-1}$ of degree d_1 that are parameters on X.*

(2) *Let X' be* 0*-dimensional. If* $\max\{d_2+1, q\} \geq \widehat{\deg}(X')$ *then there exists a degree d_2 parameter on X'.*

Proof. Applying Proposition 5.1 in the case $k = n-1$ yields (1). For (2), let f be a random degree d polynomial and let $P \in X'$ be a closed point. Since the dimension of the image of S_d in $H^0(P, \mathcal{O}_P(d))$ is at least $\min\{d+1, \deg P\}$, the probability that f vanishes at P is at worst $q^{-\min\{d+1, \deg P\}}$ which is at least q^{-1}. It follows that the probability that a degree d function vanishes on some point of X' is at worst $\sum_{P\in X'} q^{-1} \leq \widehat{\deg}(X')q^{-1}$. Thus if $q > \widehat{\deg}(X')$, this happens with probability strictly less than 1. On the other hand, if $d+1 \geq \widehat{\deg}(X')$ then polynomials of degree d surject onto $H^0(X', \mathcal{O}_{X'}(d))$ and hence we can find a parameter on X' by choosing a polynomial that restricts to a unit on X'. □

Proof of Theorem 1.5. If $\dim X = 0$, then we can directly apply Corollary 5.3(2) to find a parameter of degree d. So we assume $n := \dim X > 0$. Since $d > \log_q \widehat{\deg}(X) + \log_q n + n \log_q d$ it follows that $(n \cdot \widehat{\deg}(X))^{-1} > q^{-d}d^n > q^{-d-1}d^{n-1}$. Applying Corollary 5.3(1), we find $g_0, g_1, \dots, g_{n-1}$ in degree d that are parameters on X. Let $X' = X \cap V(g_0, g_1, \dots, g_{n-1})$. Since $\max\{d, \frac{q}{d^n}\} \geq \widehat{\deg}(X)$ it follows that $\max\{d^{n+1}, q\} \geq d^n\widehat{\deg}(X) \geq \widehat{\deg}(X')$, and Corollary 5.3(2) yields a parameter g_n of degree d^{n+1} on X'. Thus $g_0^{d^n}, g_1^{d^n}, \dots, g_{n-1}^{d^n}, g_n$ are parameters of degree d^{n+1} on X. □

6. Probabilistic analysis, II: The error term and proof of Theorem 1.4

In this section, we let $k < n$ and we analyze the error terms in Theorem 1.3 more precisely. In particular, we prove Theorem 1.4, which shows that the probabilities are controlled by the probability of vanishing along an $(n-k)$-dimensional subvariety, with varieties of lowest degree contributing the most.

Our proof of Theorem 1.4 adapts Poonen's sieve in a couple of key ways. The first big difference is that instead of sieving over closed points, we will sieve over $(n-k)$-dimensional subvarieties of X; this is because polynomials $f_0, f_1, \dots, f_k$ will fail to be parameters on X only if they all vanish along some $(n-k)$-dimensional subvariety.

The second difference is that the resulting probability formula will not be a product of local factors. This is because the values of a function can never be totally independent along two higher dimensional varieties with a nontrivial intersection. For instance, Lemma 6.1 shows that the probability that a degree d polynomial vanishes along a line is $q^{-(d+1)}$, but the probability of vanishing along two lines that intersect in a point is $q^{-(2d+1)} > (q^{-(d+1)})^2$.

The following result characterizes the individual probabilities arising in our sieve.

Lemma 6.1. *If $Z \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ is a reduced, projective scheme over a finite field $\mathbb{F}_q$ with homogeneous coordinate ring R then*

$$\mathrm{Prob}(f_0, f_1, \dots, f_k \textit{ of degree } d \textit{ all vanish along } Z) = \left(\frac{1}{\#R_d}\right)^{k+1}.$$

If d is at least the Castelnuovo–Mumford regularity of the ideal sheaf of Z, then

$$\mathrm{Prob}(f_0, f_1, \dots, f_k \textit{ of degree } d \textit{ all vanish along } Z) = q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))}.$$

Proof. Let $I \subseteq S$ be the homogeneous ideal defining Z, so that $R = S/I$. An element $h \in S_d$ vanishes along Z if and only if it restricts to 0 in R_d i.e., if and only if it lies in I_d. Since we have an exact sequence of $\mathbb{F}_q$-vector spaces:

$$0 \to I_d \to S_d \to R_d \to 0$$

we obtain

$$\mathrm{Prob}(h \text{ vanishes on } Z) = \frac{\#I_d}{\#S_d} = \frac{1}{\#R_d}.$$

For $k+1$ elements of S_d, the probabilities of vanishing along Z are independent and this yields the first statement of the lemma.

We write $\tilde{I}$ for the ideal sheaf of Z. If d is at least the regularity of $\tilde{I}$, then $H^1(\mathbb{P}^r_{\mathbb{F}_q}, \tilde{I}(d)) = 0$. Hence there is a natural isomorphism between R_d and $H^0(Z, \mathcal{O}_Z(d))$. Thus, we have

$$\frac{1}{\#R_d} = q^{-h^0(Z,\mathcal{O}_Z(d))},$$

yielding the second statement. □

Proof of Theorem 1.4. Throughout the proof, we set $\epsilon_{e,k}$ to be the error term for a given e and k, namely $\epsilon_{e,k} := q^{-e(k+1)\binom{n-k+d}{n-k}}$. We also set:

$$\begin{aligned}
\mathrm{Par}_{d,k} &:= \{f_0, f_1, \ldots, f_k \text{ are parameters on } X\}\\
\mathrm{Low}_{d,k,e} &:= \left\{\begin{array}{l} f_0, f_1, \ldots, f_k \text{ all vanish along a variety } Z\\ \text{where } \dim Z = (n-k) \text{ and } \deg(Z) \le e \end{array}\right\}\\
\mathrm{Med}_{d,k,e} &:= \left\{\begin{array}{l} (f_0, f_1, \ldots, f_k) \notin \mathrm{Low}_{d,k,e} \text{ which all vanish along a variety } Z\\ \text{where } \dim Z = (n-k) \text{ and } e < \deg(Z) \le e(k+1) \end{array}\right\}\\
\mathrm{High}_{d,k,e} &:= \left\{\begin{array}{l} (f_0, f_1, \ldots, f_k) \notin \mathrm{Low}_{d,ke} \cup \mathrm{Med}_{d,k,e} \text{ which all vanish along}\\ \text{a variety } Z \text{ where } \dim Z = (n-k) \text{ and } e(k+1) < \deg(Z) \end{array}\right\}.
\end{aligned}$$

Note that if $f_0, f_1, \ldots, f_k$ all vanish along a variety of dimension $> n-k$ then they will also all vanish along a high degree variety, and hence we do not need to count this case separately. For $\boldsymbol{f} = f_0, f_1, \ldots, f_k \in S_d^{k+1}$, we thus have

$$\begin{aligned}
\mathrm{Prob}(\boldsymbol{f} \in \mathrm{Par}_{d,k}) &= 1 - \mathrm{Prob}(\boldsymbol{f} \in \mathrm{Low}_{d,k,e} \cup \mathrm{Med}_{d,k,e} \cup \mathrm{High}_{d,k,e})\\
&= 1 - \mathrm{Prob}(\boldsymbol{f} \in \mathrm{Low}_{d,k,e}) - \mathrm{Prob}(\boldsymbol{f} \in \mathrm{Med}_{d,k,e}) - \mathrm{Prob}(\boldsymbol{f} \in \mathrm{High}_{d,k,e}).
\end{aligned}$$

It thus suffices to show that

$$\mathrm{Prob}(\boldsymbol{f} \in \mathrm{Low}_{d,k,e}) = \sum_{\substack{Z \subseteq X \text{reduced}\\ \dim Z \equiv n-k\\ \deg Z \le e}} (-1)^{|Z|-1} q^{-(k+1)h^0(Z,\mathcal{O}_Z(d))} + o(\epsilon_{e,k})$$

and that $\mathrm{Prob}(\boldsymbol{f} \in \mathrm{Med}_{d,k,e})$ and $\mathrm{Prob}(\boldsymbol{f} \in \mathrm{High}_{d,k,e})$ are each in $o(\epsilon_{e,k})$.

We proceed by induction on k. When $k = 0$ the condition that f_0 is a parameter on X is equivalent to f_0 not vanishing along a top-dimensional component of X. Thus, combining Lemma 6.1 with an inclusion/exclusion argument implies the exact result:

$$\mathrm{Prob}(f_0 \in \mathrm{Par}_{d,0}) = 1 - \sum_{\substack{Z \subseteq X \text{reduced}\\ \dim Z \equiv n-k}} (-1)^{|Z|-1} q^{-h^0(Z,\mathcal{O}_Z(d))}.$$

By basic properties of the Hilbert polynomial, as $d \to \infty$ we have

$$h^0(Z, \mathcal{O}_Z(d)) = \frac{\deg(Z)}{n!} d^n + o(d^n) = \deg(Z)\binom{n+d}{d} + o(d^n).$$

Hence for the fixed degree bound e, we obtain

$$\begin{aligned}\operatorname{Prob}(f \in \operatorname{Par}_{d,0}) &= 1 - \sum_{\substack{Z\subseteq X \text{reduced} \\ \dim Z \equiv n-k \\ \deg Z \le e}} (-1)^{|Z|-1} q^{-h^0(Z,\mathcal{O}_Z(d))} - \sum_{\substack{Z\subseteq X \text{reduced} \\ \dim Z \equiv n-k \\ \deg Z > e}} (-1)^{|Z|-1} q^{-h^0(Z,\mathcal{O}_Z(d))} \\ &= 1 - \sum_{\substack{Z\subseteq X \text{reduced} \\ \dim Z \equiv n-k \\ \deg Z \le e}} (-1)^{|Z|-1} q^{-h^0(Z,\mathcal{O}_Z(d))} + o(\epsilon_{e,0}).\end{aligned}$$

We now consider the induction step. Let $\boldsymbol{f} = (f_0, f_1, \dots, f_k)$ drawn randomly from S_d^{k+1}. Here we separate into low, medium, and high degree cases.

Low degree argument. Let $\boldsymbol{V}_{k,e}$ denote the set of integral projective varieties $V \subseteq X$ of dimension $n-k$ and degree $\le e$. We have $\boldsymbol{f} \in \operatorname{Low}_{d,k,e}$ if and only if $\boldsymbol{f}$ vanishes on some $V \in \boldsymbol{V}_{k,e}$. Since $\boldsymbol{V}_{k,e}$ is a finite set, we may use an inclusion-exclusion argument to get

$$\operatorname{Prob}(\boldsymbol{f} \in \operatorname{Low}_{d,k,e}) = \sum_{\substack{Z\subseteq X \text{ a union of} \\ V\in \boldsymbol{V}_{k,e}}} (-1)^{|Z|-1} \operatorname{Prob}(f_0, f_1, \dots, f_k \text{ of degree } d \text{ all vanish along } Z).$$

If $\deg Z > e$ then Lemma 6.1 implies that those terms can be absorbed into the error term $o(\epsilon_{e,k})$. Moreover, assuming that Z is a union of $V \in \boldsymbol{V}_{k,e}$ satisfying $\deg(Z) \le e$ is equivalent to assuming Z is reduced and equidimensional of dimensional $n-k$. We thus have

$$= \sum_{\substack{Z\subseteq X \text{ reduced} \\ \dim Z \equiv n-k \\ \deg Z \le e}} (-1)^{|Z|-1} \operatorname{Prob}(f_0, f_1, \dots, f_k \text{ of degree } d \text{ all vanish along } Z) + o(\epsilon_{e,k}).$$

Medium degree argument. We know that $\operatorname{Prob}(\boldsymbol{f} \in \operatorname{Med}_{d,k,e})$ is bounded by the sum of the probabilities that f vanishes along some irreducible variety V in $\boldsymbol{V}_{k,e(k+1)} \setminus \boldsymbol{V}_{k,e}$.

$$\operatorname{Prob}(\boldsymbol{f} \in \operatorname{Med}_{d,k,e}) \le \sum_{Z\in \boldsymbol{V}_{k,e(k+1)} \setminus \boldsymbol{V}_{k,e}} \operatorname{Prob}(f_0, f_1, \dots, f_k \text{ of degree } d \text{ all vanish along } Z).$$

Lemma 6.1 implies that each summand on the right-hand side lies in $o(\epsilon_{e,k})$. This sum is finite and thus $\operatorname{Prob}(\boldsymbol{f} \in \operatorname{Med}_{d,k,e})$ is in $o(\epsilon_{e,k})$.

High degree argument. Proposition 5.1 implies that $f_0, f_1, \dots, f_{k-1}$ are parameters on X with probability $1 - o(q^{-\binom{n-k+1+d}{d}}) \ge 1 - o(\epsilon_{e,k})$ for any e. Hence we may restrict our attention to the case where $f_0, f_1, \dots, f_{k-1}$ are parameters on X.

Let $V_1, V_2, \dots, V_s$ be the irreducible components of $X' := X \cap \mathbb{V}(f_0, f_1, \dots, f_{k-1})$ that have dimension $n-k$. We have that $f_0, f_1 \dots, f_k$ fail to be parameters on X if and only if f_k vanishes on some V_i. We can assume that f_k does not vanish on any V_i where $\deg V_i \le e(k+1)$ as we have already accounted for this possibility in the low and medium degree cases. After possibly relabeling the components, we let $V_1, V_2, \dots, V_t$ be the components of degree $> e(k+1)$ and $X'' = V_1 \cup V_2 \cup \dots \cup V_t$. Using Lemma 2.3, we compute $\widehat{\deg}(X'') \le \widehat{\deg}(X') = \widehat{\deg}(X) \cdot d^k$. It follows that X'' has at most $\widehat{\deg}(X) d^k/(e(k+1))$ irreducible components.

Now for the key point: since the value of d is not necessarily larger than the Castelnuovo–Mumford regularity of V_i, we cannot use a Hilbert polynomial computation to bound the probability that f_k vanishes along V_i. Instead, we use the lower bound for Hilbert functions obtained in Lemma 3.1. Let $\epsilon = \frac{1}{2}$, though any choice of ϵ would work. We write $R(V_i)$ for the homogeneous coordinate ring of V_i. For any $1 \le i \le t$, Lemmas 3.1 and 6.1 yield

$$\text{Prob}(f_k \text{ of degree } d \text{ vanishes along } V_i) = q^{-\dim R(V_i)_d} \le q^{-(e(k+1)+\epsilon)\binom{n-k+d}{n-k}}$$

whenever $d \ge Ce^{k+1}$. Combining this with our bound on the number of irreducible components of X'' gives $\text{Prob}(\boldsymbol{f} \in \text{High}_{d,k,e}) \le \frac{1}{e(k+1)} \widehat{\deg} X d^k q^{-(e(k+1)+\epsilon)\binom{n-k+d}{n-k}}$ which is in $o(\epsilon_{e,k})$. □

Corollary 6.2. *Let $X \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ be an n-dimensional closed subscheme and let $k < n$. Then*

$$\lim_{d\to\infty} q^{(k+1)\binom{n-k+d}{n-k}} \,\text{Prob}\left(\begin{matrix} f_0, f_1, \dots, f_k \textit{ of degree } d \\ \textit{are } \underline{\textit{not}} \textit{ parameters on } X \end{matrix}\right) = \#\{(n-k)\textit{-planes } L \subseteq \mathbb{P}^r_{\mathbb{F}_q} \textit{ such that } L \subseteq X\}.$$

Proof. Let N denote the number of $(n-k)$-planes $L \subseteq \mathbb{P}^r_{\mathbb{F}_q}$ such that $L \subseteq X$. Choosing $e = 1$ in Theorem 1.4, we compute that

$$\text{Prob}(f_0, f_1, \dots, f_k \text{ of degree } d \text{ are parameters on } X) = 1 - Nq^{-(k+1)\binom{n-k+d}{n-k}} + o(q^{-(k+1)\binom{n-k+d}{n-k}}).$$

It follows that

$$\text{Prob}(f_0, f_1, \dots, f_k \text{ of degree } d \text{ are } \underline{\text{not}} \text{ parameters on } X) = Nq^{-(k+1)\binom{n-k+d}{n-k}} + o(q^{-(k+1)\binom{n-k+d}{n-k}}).$$

Dividing both sides by $q^{-(k+1)\binom{n-k+d}{n-k}}$ and taking the limit as $d \to \infty$ yields the corollary. □

7. Passing to $\mathbb{Z}$ and $\mathbb{F}_q[t]$

In this section we prove Corollaries 1.6 and 1.7.

Definition 7.1. Let $B = \mathbb{Z}$ or $\mathbb{F}_q[t]$ and fix a finitely generated, free B-module B^s and a subset $\mathcal{S} \subseteq B^s$. Given $a \in B^s$ we write $a = (a_1, a_2, \dots, a_s)$. The *density* of $\mathcal{S} \subseteq B^s$ is

$$\text{Density}(\mathcal{S}) := \begin{cases} \lim_{N\to\infty} \frac{\#\{a \in \mathcal{S} \mid \max\{|a_i|\} \le N\}}{\#\{a \in \mathbb{Z}^s \mid \max\{|a_i|\} \le N\}} & \text{if } B = \mathbb{Z}, \\ \lim_{N\to\infty} \frac{\#\{a \in \mathcal{S} \mid \max\{\deg a_i\} \le N\}}{\#\{a \in \mathbb{F}_q[t]^s \mid \max\{\deg a_i\} \le N\}} & \text{if } B = \mathbb{F}_q[t]. \end{cases}$$

Proof of Corollary 1.6. For clarity, we will prove the result over $\mathbb{Z}$ in detail and at the end, mention the necessary adaptations for $\mathbb{F}_q[t]$.

We first let $k < n$. Given degree d polynomials $f_0, f_1, \dots, f_k$ with integer coefficients and a prime p, let $\overline{f}_0, \overline{f}_1, \dots, \overline{f}_k$ be the reduction of these polynomials mod p. Then $\overline{f}_0, \overline{f}_1, \dots, \overline{f}_k$ will be parameters on X_p if and only if the point $\overline{\boldsymbol{f}} = (\overline{f}_0, \overline{f}_1, \dots, \overline{f}_k)$ lies $\mathcal{D}_{d,k}(X_{\mathbb{F}_p})$. As noted in Remark 4.1, this is equivalent to asking that $\overline{f}$ is an $\mathbb{F}_p$-point of $\mathscr{D}_{k,d}(X_{\mathbb{Z}})$. Thus, we may apply [Ekedahl 1991, Theorem 1.2] to $\mathscr{D}_{d,k}(X_{\mathbb{Z}}) \subseteq \mathscr{A}_{k,d}$ (using $M = 1$) to conclude that

$$\text{Density}\left\{\begin{array}{l} f_0, f_1, \dots, f_k \text{ of degree } d \\ \text{that restrict to parameters on } X_p \text{ for all } p \end{array}\right\} = \prod_p \text{Prob}\left(\begin{array}{l} f_0, f_1, \dots, f_k \text{ of degree } d \\ \text{restrict to parameters on } X_p \end{array}\right).$$

Applying Proposition 5.1 to estimate the individual factors; we have:

$$\begin{aligned}\text{Density}\left\{\begin{array}{l} f_0, f_1, \dots, f_k \text{ of degree } d \text{ that} \\ \text{restrict to parameters on } X_p \text{ for all } p \end{array}\right\} &= \lim_{d\to\infty} \prod_p \text{Prob}\left(\begin{array}{l} f_0, f_1, \dots, f_k \text{ of degree } d \\ \text{restrict to parameters on } X_p \end{array}\right) \\ &\geq \lim_{d\to\infty} \prod_p \left(1 - \widehat{\deg}(X_p)(1+d+\cdots+d^k)p^{-\binom{n-k+d}{n-k}}\right).\end{aligned}$$

Lemma 7.2 shows that there is an integer D where $D \geq \widehat{\deg}(X_p)$ for all p. Moreover, $1+d+\cdots+d^k \leq kd^k$ for all d, and hence:

$$\geq \lim_{d\to\infty} \prod_p \left(1 - Dkd^k p^{-\binom{n-k+d}{n-k}}\right).$$

For $d \gg 0$ we can make $Dkd^k p^{-\binom{n-k+d}{n-k}} \leq p^{-d/2}$ for all p simultaneously. Using $\zeta(n)$ for the Riemann zeta function, we get:

$$\geq \lim_{d\to\infty} \prod_p (1 - p^{-d/2}) \geq \lim_{d\to\infty} \zeta(d/2)^{-1} = 1.$$

We now consider the case $k = n$. This follows by a "low degree argument" exactly analogous to [Poonen 2004, Theorem 5.13]. Fix a large integer N and let Y be the union of all closed points $P \in X$ whose residue field $\kappa(P)$ has cardinality at most N. Since Y is a finite union of closed points, we see that for $d \gg 0$, there is a surjection

$$H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(d)) \to H^0(Y, \mathcal{O}_Y(d)) \cong \bigoplus_{\substack{P\in X \\ \#\kappa(P)\leq N}} H^0(P, \mathcal{O}_P(d)) \to 0.$$

It follows that we have a product formula

$$\text{Density}\left\{\begin{array}{l} f_0, f_1, \dots, f_n \text{ of degree } d \text{ do not all} \\ \text{vanish on a point } P \text{ with } \#\kappa(P) \leq N \end{array}\right\} = \prod_{P\in X, \#\kappa(P)\leq N} \left(1 - \frac{1}{\#\kappa(P)^{n+1}}\right)$$

This is certainly an upper bound on the density of $f_0, f_1, \dots, f_n$ that are parameters on X_p for all p. As $N \to \infty$ the right-hand side approaches $\zeta_X(n+1)^{-1}$. However, since the dimension of X is $n+1$, this zeta function has a pole at $s = n+1$ [Serre 1965, Theorems 1 and 3(a)]. Hence this asymptotic density equals 0. This completes the proof over $\mathbb{Z}$.

Over $\mathbb{F}_q[t]$, the key adaptation is to use [Poonen 2003, Theorem 3.1] in place of Ekedahl's result. Poonen's result is stated for a pair of polynomials, but it applies equally well to n-tuples of polynomials such as the n-tuples defining $\mathscr{D}_{k,d}(X)$. In particular, one immediately reduces to proving an analogue of

[Poonen 2003, Lemma 5.1], for n-tuples of polynomials which are irreducible over $\mathbb{F}_q(t)$ and which have gcd equal to 1; but the $n = 2$ version of the lemma then implies the $n \geq 2$ versions of the lemma.[2] The rest of our argument over $\mathbb{Z}$ works over $\mathbb{F}_q[t]$. □

Lemma 7.2. *Let $X \subseteq \mathbb{P}^r_B$ be any closed subscheme. There is an integer D where $D \geq \widehat{\deg}(X_s)$ for all $s \in \operatorname{Spec} B$.*

Proof. First we take a flattening stratification for X over B [EGA IV$_4$ 1967, Corollaire 6.9.3]. Within each stratum, the maximal degree of a minimal generator is semicontinuous, and we can thus find a degree e where X_s is generated in degree e for all $s \in \operatorname{Spec} B$. By [Bayer and Mumford 1993, Proposition 3.5], we then obtain that $\widehat{\deg}(X) \leq \sum_{j=0}^{n} e^{r-j}$. In particular defining $D := re^r$ will suffice. □

To prove Corollary 1.7, we use Corollary 1.6 to find a submaximal collection $f_0, f_1, \dots, f_{n-1}$ which restrict to parameters on X_s for all $s \in \operatorname{Spec} B$. This cuts X down to a scheme $X' = X \cap \mathbb{V}(f_0, f_1, \dots, f_{n-1})$ with 0-dimensional fibers over each point s. When $B = \mathbb{Z}$, such a scheme is essentially a union of orders in number fields, and we find the last element f_n by applying classical arithmetic results about the Picard groups of rings of integers of number fields. When $B = \mathbb{F}_q[t]$, we use similar facts about Picard groups of affine curves over $\mathbb{F}_q$.

An example illustrates this approach. Let $X = \mathbb{P}^1_{\mathbb{Z}} = \operatorname{Proj}(\mathbb{Z}[x, y])$. A polynomial of degree d will be a parameter on X as long as the $d + 1$ coefficients are relatively prime. Thus as $d \to \infty$, the density of these choices will go to 1. However, once we have fixed one such parameter, say $5x - 3y$, it is much harder to find an element that will restrict to a parameter on $\mathbb{Z}[x, y]/(5x - 3y)$ modulo p for all p. In fact, the only possible choices are the elements which restrict to units on $\operatorname{Proj}(\mathbb{Z}[x, y]/(5x - 3y))$. Among the linear forms, these are

$$\pm(7x - 4y) + c(5x - 3y) \text{ for any } c \in \mathbb{Z}.$$

Hence, these elements arise with density zero, and yet they form a nonempty subset.

Lemmas 7.3 and 7.4 below are well-known to experts, but we sketch the proofs for clarity.

Lemma 7.3. *If $X' \subseteq \mathbb{P}^r_{\mathbb{Z}}$ is closed and finite over* $\operatorname{Spec}(\mathbb{Z})$, *then* $\operatorname{Pic}(X')$ *is finite.*

Proof. We first reduce to the case where X' is reduced. Let $\mathcal{N} \subseteq \mathcal{O}_{X'}$ be the nilradical ideal. If X' is nonreduced then there is some integer $m > 1$ for which $\mathcal{N}^m = 0$. Let X'' be the closed subscheme defined by $\mathcal{N}^{m-1}$. We have a short exact sequence $0 \to \mathcal{N}^{m-1} \to \mathcal{O}^*_{X'} \to \mathcal{O}^*_{X''} \to 1$ where the first map sends $f \mapsto 1 + f$. Since X' is affine and noetherian and $\mathcal{N}^{m-1}$ is a coherent ideal sheaf, we have that $H^1(X', \mathcal{N}^{m-1}) = H^2(X', \mathcal{N}^{m-1}) = 0$ [Hartshorne 1977, Theorem III.3.7]. Taking cohomology of the above sequence thus yields an isomorphism $\operatorname{Pic}(X') \cong \operatorname{Pic}(X'')$. Iterating this argument, we may assume X' is reduced.

We now have $X' = \operatorname{Spec}(B)$ where B is a finite, reduced $\mathbb{Z}$-algebra. If Q is a minimal prime of B, then B/Q is either zero dimensional or an order in a number field, and hence has a finite Picard group [Neukirch 1999, Theorem I.12.12]. If B has more than one minimal prime, then we let Q' be the

[2]We thank Bjorn Poonen for pointing out this reduction.

intersection of all of the minimal primes of B except for Q, and we again have an exact sequence in cohomology

$$\cdots \to (B/(Q+Q'))^* \to \mathrm{Pic}(X') \to \mathrm{Pic}(B/Q) \oplus \mathrm{Pic}(B/Q') \to \cdots$$

Since $(B/(Q+Q'))^*$ is a finite set, and since B/Q and B/Q' have fewer minimal primes than B, we may use induction to conclude that $\mathrm{Pic}(X')$ is finite. □

Lemma 7.4. *If C is an affine curve over $\mathbb{F}_q$, then $\mathrm{Pic}(C)$ is finite.*

Proof. If C fails to be integral, then an argument entirely analogous to the proof of Lemma 7.3 reduces us to the case C is integral. We next assume that C is nonsingular and integral, and that $\overline{C}$ is the corresponding nonsingular projective curve. Since C is affine we have $\mathrm{Pic}(C) = \mathrm{Pic}^0(C) \subseteq \mathrm{Pic}^0(\overline{C}) \cong \mathrm{Jac}(\overline{C})(\mathbb{F}_q)$, the last of which is a finite group. If C is singular, then the finiteness of $\mathrm{Pic}(C)$ follows from the nonsingular case by a minor adaptation of the proof of [Neukirch 1999, Proposition I.12.9]. □

Proof of Corollary 1.7. By Corollary 1.6, for $d \gg 0$ we can find polynomials $f_0, f_1, \dots, f_{n-1}$ of degree d that restrict to parameters on X_s for all $s \in \operatorname{Spec} B$. Let $X' := \mathbb{V}(f_0, f_1, \dots, f_{n-1}) \cap X$, which is finite over B by construction. Let A be the finite B-algebra where $\operatorname{Spec} A = X'$. Lemma 7.3 or 7.4 implies that $H^0(X', \mathcal{O}_{X'}(e)) = A$ for some e. We can thus find a polynomial f_n of degree e mapping onto a unit in the B-algebra A. It follows that $\mathbb{V}(f_n) \cap X' = \varnothing$. Replace f_i by f_i^e for $i = 0, \dots, n-1$ and replace f_n by f_n^d. Then we have $f_0, f_1, \dots, f_n$ of degree $d' := de$ and restricting to parameters on X_s for all $s \in \operatorname{Spec}(B)$ simultaneously.

We thus obtain a proper morphism $\pi : X \to \mathbb{P}^n_B$ where $X_s \to \mathbb{P}^n_{\kappa(s)}$ is finite for all s. Since π is quasifinite and proper, it is finite by [EGA IV$_3$ 1966, Théorème 8.11.1]. □

The following generalizes Corollary 1.7 to other graded rings.

Corollary 7.5. *Let $B = \mathbb{Z}$ or $\mathbb{F}_q[t]$ and let R be a graded, finite type B-algebra where $\dim R \otimes_{\mathbb{Z}} \mathbb{F}_p = n+1$ for all p. Then there exist $f_0, f_1, \dots, f_n$ of degree d for some d such that $B[f_0, f_1, \dots, f_n] \subseteq R$ is a finite extension.*

Proof. After replacing R by a high degree Veronese subring R', we may assume that R' is generated in degree one and contains no R'_+-torsion submodule, where $R'_+ \subseteq R'$ is the homogeneous ideal of strictly positive degree elements. Let $r+1$ be the number of generators of R'_1. Then there is a surjection $\phi \colon B[x_0, x_1, \dots, x_r] \to R'$ inducing an embedding of $X := \mathrm{Proj}(R') \subseteq \mathbb{P}^r_B$. Since R' contains no R'_+-torsion submodule, the kernel of ϕ will be saturated with respect to $(x_0, x_1, \dots, x_r)$ and hence R' will equal the homogeneous coordinate ring of X. Choosing $f_0, f_1, \dots, f_n$ as in Corollary 1.7, it follows that $B[f_0, f_1, \dots, f_n] \subseteq R'$ is a finite extension, and thus so is $B[f_0, f_1, \dots, f_n] \subseteq R$. □

8. Examples

Example 8.1. By Corollary 6.2, it is more difficult to randomly find parameters on surfaces that contain lots of lines. Consider $\mathbb{V}(xyz) \subset \mathbb{P}^3$ which contains substantially more lines than $\mathbb{V}(x^2+y^2+z^2) \subset \mathbb{P}^3$.

Using [Macaulay2] to select 1,000,000 random pairs (f_0, f_1) of polynomials of degree two, the proportion that failed to be systems of parameters were

	$\mathbb{V}(xyz)$	$\mathbb{V}(x^2+y^2+z^2)$
$\mathbb{F}_2$	.2638	.1179
$\mathbb{F}_3$	.0552	.0059
$\mathbb{F}_5$	.0063	.0004

Example 8.2. Let $X \subseteq \mathbb{P}^3_{\mathbb{F}_q}$ be a smooth cubic surface. Over the algebraic closure X has 27 lines, but it has between 0 and 27 lines defined over $\mathbb{F}_q$. For example, working over $\mathbb{F}_4$, the Fermat cubic surface X' defined by $x^3+y^3+z^3+w^3$ has 27 lines, while the cubic surface X defined by $x^3+y^3+z^3+aw^3$ where $a \in \mathbb{F}_4 \setminus \mathbb{F}_2$ has no lines defined over $\mathbb{F}_4$ [Debarre et al. 2017, Section 3]. It will thus be more difficult to find parameters on X than on X'. Using [Macaulay2] to select 100,000 random pairs (f_0, f_1) of polynomials of degree two, 0.62% failed to be parameters on X whereas no choices whatsoever failed to be parameters on X'. This is in line with the predictions from Corollary 6.2; for instance, in the case of X, we have $27 \cdot 4^{-2\cdot 3} \approx 0.66\%$.

Example 8.3. Let $X = [1:4] \cup [3:5] \cup [4:5] = \mathbb{V}((4x-y)(5x-3y)(5x-4y)) \subseteq \mathbb{P}^1_{\mathbb{Z}}$ and let R be the homogeneous coordinate ring of X. The fibers are 0-dimensional so finding a Noether normalization $X \to \mathbb{P}^0_{\mathbb{Z}}$ is equivalent to finding a single polynomial f_0 that restricts to a unit on each of the points simultaneously. We can find such an f_0 of degree d if and only if the induced map of free $\mathbb{Z}$-modules $\mathbb{Z}[x, y]_d \to R_d$ is surjective. A computation in [Macaulay2] shows that this happens if and only if d is divisible by 60.

Example 8.4. Let $R = \mathbb{Z}[x]/(3x^2-5x) \cong \mathbb{Z} \oplus \mathbb{Z}\left[\frac{1}{3}\right]$. This is a flat, finite type $\mathbb{Z}$-algebra where every fiber has dimension 0, yet it is not a finite extension of $\mathbb{Z}$. However, if we take the projective closure of $\operatorname{Spec}(R)$ in $\mathbb{P}^1_{\mathbb{Z}}$, then we get $\operatorname{Proj}(\bar{R})$ where $\bar{R} = \mathbb{Z}[x, y]/(3x^2-5xy)$. If we then choose $f_0 := 4x-7y$, we see that $\mathbb{Z}[f_0] \subseteq \bar{R}$ is a finite extension of graded rings.

Example 8.5. Let $\boldsymbol{k}$ be a field and let $X = [1:1+t] \cup [1-t:1] = \mathbb{V}((y-(1+t)x)(x-(1-t)y)) \subseteq \mathbb{P}^1_{\boldsymbol{k}[t]}$. Let R be the homogeneous coordinate ring of X. In degree d, we have the map $\phi_d : \boldsymbol{k}[t][x, y]_d \cong \boldsymbol{k}[t]^{d+1} \to R_d \cong \boldsymbol{k}[t]^2$. Choosing the standard basis $x^d, x^{d-1}y, \ldots, y^d$ for the source of ϕ_d, and the two points of X for the target, we can represent ϕ_d by the matrix

$$\begin{pmatrix} 1 & 1+t & (1+t)^2 & \cdots & (1+t)^d \\ (1-t)^d & (1-t)^{d-1} & (1-t)^{d-2} & \cdots & 1 \end{pmatrix}.$$

It follows that $\operatorname{im}\phi_d = \operatorname{im}\left(\begin{smallmatrix} t^2 & (1+t)^d \\ 0 & 1 \end{smallmatrix}\right) = \operatorname{im}\left(\begin{smallmatrix} t^2 & 1+dt \\ 0 & 1 \end{smallmatrix}\right)$. The image of ϕ_d thus contains a unit if and only if the characteristic of $\boldsymbol{k}$ is p and $p \mid d$. In particular, if $\boldsymbol{k} = \mathbb{Q}$, then we cannot find a polynomial f_0 inducing a finite map $X \to \mathbb{P}^0_{\mathbb{Q}[t]}$.

Example 8.6. Let $\boldsymbol{k}$ be any field, let $B = \boldsymbol{k}[s, t]$, and let $X = [s:1] \cup [1:t] = \mathbb{V}((x-sy)(y-tx)) \subseteq \mathbb{P}^1_B$. We claim that for any $d > 0$, there does not exist a polynomial that restricts to a parameter on X_b for each point $b \in B$. Assume for contradiction that we had such an $f = \sum_{i=0}^{d} c_i s^i t^{d-i}$ with $c_i \in B$. After scaling, we obtain

$$f([s:1]) = c_0 s^d + c_1 s^{d-1} + \cdots + c_d = 1 \quad \text{and} \quad f([1:t]) = c_0 + c_1 t + \cdots + c_d t^d = \lambda$$

where $\lambda \in B^* = \boldsymbol{k}^*$. Substituting for c_d we obtain

$$f([1:t]) = c_0 + c_1 t + \cdots + c_{d-1} t^{d-1} + (1 - (c_0 s^d + c_1 s^{d-1} + \cdots + c_{d-1} s))t^d = \lambda,$$

which implies that

$$\begin{aligned} \lambda - t^d &= c_0 + c_1 t + \cdots + c_{d-1} t^{d-1} - (c_0 s^d + c_1 s^{d-1} + \cdots + c_{d-1} s)t^d \\ &= (c_0 - c_0 s^d t^d) + (c_1 t - c_1 s^{d-1} t^d) + \cdots + (c_{d-1} t^{d-1} - c_{d-1} s t^d) \\ &= (1 - st)h(s,t) \end{aligned}$$

where $h(s,t) \in \boldsymbol{k}[s,t]$. This implies that $\lambda - t^d$ is divisible by $(1 - st)$, which is a contradiction.

Acknowledgements

We thank Joe Buhler, Nathan Clement, David Eisenbud, Jordan S. Ellenberg, Benedict Gross, Moisés Herradón Cueto, Craig Huneke, Kiran Kedlaya, Brian Lehmann, Dino Lorenzini, Bjorn Poonen, Anurag Singh, Melanie Matchett Wood, and the anonymous referees for their helpful conversations and comments. The computer algebra system [Macaulay2] provided valuable assistance throughout our work.

References

[Abhyankar and Kravitz 2007] S. S. Abhyankar and B. Kravitz, "Two counterexamples in normalization", *Proc. Amer. Math. Soc.* **135**:11 (2007), 3521–3523. MR Zbl

[Achinger 2015] P. Achinger, "$K(\pi, 1)$-neighborhoods and comparison theorems", *Compos. Math.* **151**:10 (2015), 1945–1964. MR Zbl

[Bayer and Mumford 1993] D. Bayer and D. Mumford, "What can be computed in algebraic geometry?", pp. 1–48 in *Computational algebraic geometry and commutative algebra* (Cortona, Italy, 1991), edited by D. Eisenbud and L. Robbiano, Sympos. Math. **34**, Cambridge Univ. Press, 1993. MR Zbl

[Benoist 2011] O. Benoist, "Le théorème de Bertini en famille", *Bull. Soc. Math. France* **139**:4 (2011), 555–569. MR Zbl

[Brennan and Epstein 2011] J. P. Brennan and N. Epstein, "Noether normalizations, reductions of ideals, and matroids", *Proc. Amer. Math. Soc.* **139**:8 (2011), 2671–2680. MR Zbl

[Bruns and Herzog 1993] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Stud. Adv. Math. **39**, Cambridge Univ. Press, 1993. MR Zbl

[Bruns and Vetter 1988] W. Bruns and U. Vetter, *Determinantal rings*, Monograf. de Mat. **45**, Inst. Matemática Pura e Aplicada, Rio de Janeiro, 1988. MR Zbl

[Bucur and Kedlaya 2012] A. Bucur and K. S. Kedlaya, "The probability that a complete intersection is smooth", *J. Théor. Nombres Bordeaux* **24**:3 (2012), 541–556. MR Zbl

[Charles 2017] F. Charles, "Arithmetic ampleness and an arithmetic Bertini theorem", preprint, 2017. arXiv

[Charles and Poonen 2016] F. Charles and B. Poonen, "Bertini irreducibility theorems over finite fields", *J. Amer. Math. Soc.* **29**:1 (2016), 81–94. MR Zbl

[Chinburg et al. 2017] T. Chinburg, L. Moret-Bailly, G. Pappas, and M. J. Taylor, "Finite morphisms to projective space and capacity theory", *J. Reine Angew. Math.* **727** (2017), 69–84. MR Zbl

[Debarre et al. 2017] O. Debarre, A. Laface, and X. Roulleau, "Lines on cubic hypersurfaces over finite fields", pp. 19–51 in *Geometry over nonclosed fields*, edited by F. Bogomolov et al., Springer, 2017. MR Zbl

[EGA IV_3 1966] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, III", *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 5–255. MR Zbl

[EGA IV_4 1967] A. Grothendieck, "Eléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, IV", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. MR Zbl

[Eisenbud 1995] D. Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Grad. Texts in Math. **150**, Springer, 1995. MR Zbl

[Ekedahl 1991] T. Ekedahl, "An infinite version of the Chinese remainder theorem", *Comment. Math. Univ. St. Paul.* **40**:1 (1991), 53–59. MR Zbl

[Ellenberg and Erman 2016] J. S. Ellenberg and D. Erman, "Furstenberg sets and Furstenberg schemes over finite fields", *Algebra Number Theory* **10**:7 (2016), 1415–1436. MR Zbl

[Ellenberg et al. 2010] J. S. Ellenberg, R. Oberlin, and T. Tao, "The Kakeya set and maximal conjectures for algebraic varieties over finite fields", *Mathematika* **56**:1 (2010), 1–25. MR Zbl

[Fulton 1984] W. Fulton, *Intersection theory*, Ergebnisse der Mathematik (3) **2**, Springer, 1984. MR Zbl

[Gabber et al. 2015] O. Gabber, Q. Liu, and D. Lorenzini, "Hypersurfaces in projective schemes and a moving lemma", *Duke Math. J.* **164**:7 (2015), 1187–1270. 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

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[Kedlaya 2005] K. S. Kedlaya, "More étale covers of affine spaces in positive characteristic", *J. Algebraic Geom.* **14**:1 (2005), 187–192. MR Zbl

[Lang and Weil 1954] S. Lang and A. Weil, "Number of points of varieties in finite fields", *Amer. J. Math.* **76** (1954), 819–827. MR Zbl

[Macaulay 1916] F. S. Macaulay, *The algebraic theory of modular systems*, Cambridge Tracts Math. and Math. Phys. **19**, Cambridge Univ. Press, 1916. Zbl

[Macaulay2] D. R. Grayson and M. E. Stillman, "Macaulay2, a software system for research in algebraic geometry", Available at http://www.math.uiuc.edu/Macaulay2.

[Moh 1979] T. T. Moh, "On a normalization lemma for integers and an application of four colors theorem", *Houston J. Math.* **5**:1 (1979), 119–123. MR Zbl

[Nagata 1962] M. Nagata, *Local rings*, Intersci. Tracts Pure Appl. Math. **13**, Intersci., New York, 1962. MR Zbl

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Math. Wissenschaften **322**, Springer, 1999. MR Zbl

[Poonen 2003] B. Poonen, "Squarefree values of multivariable polynomials", *Duke Math. J.* **118**:2 (2003), 353–373. MR Zbl

[Poonen 2004] B. Poonen, "Bertini theorems over finite fields", *Ann. of Math.* (2) **160**:3 (2004), 1099–1127. MR Zbl

[Poonen 2009] B. Poonen et al., "Smooth proper scheme over $\mathbb{Z}$", 2009, Available at https://mathoverflow.net/questions/9576/smooth-proper-scheme-over-z/9605. Discussion on MathOverflow website.

[Poonen 2013] B. Poonen, "Extending self-maps to projective space over finite fields", *Doc. Math.* **18** (2013), 1039–1044. MR Zbl

[Serre 1965] J.-P. Serre, "Zeta and L functions", pp. 82–92 in *Arithmetical algebraic geometry* (West Lafayette, IN, 1963), edited by O. F. G. Schilling, Harper & Row, New York, 1965. MR Zbl

[Zariski and Samuel 1960] O. Zariski and P. Samuel, *Commutative algebra, II*, Van Nostrand, Princeton, 1960. MR Zbl

Communicated by Kiran S. Kedlaya
Received 2018-05-23 Revised 2018-12-18 Accepted 2019-06-27

juliette.bruce@math.wisc.edu *Department of Mathematics, University of Wisconsin, Madison, WI, United States*

derman@math.wisc.edu *Department of Mathematics, University of Wisconsin, Madison, WI, United States*

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2019 is US $385/year for the electronic version, and $590/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 13 No. 9 2019

1937-0652(2019)13:9;1-4