Undergraduate Senior Thesis

Ziquan Yang

April 16, 2016

Contents

1 Introduction

Let X be a non-singular closed subvariety of $\mathbb{P}^N$ of dimension m over a ground field κ . The classical Bertini theorem states that if κ is algebraically closed, then for almost all hyperplanes H, $H \cap X$ is non-singular. More precisely, the set of all hyperplanes with this property forms an open dense subset of the complete linear system $|\mathcal{O}_{\mathbb{P}^N}(1)|$, considered as a projective space.

The classical Bertini theorem is known to fail for finite fields, as Poonen demonstrated in [4]. However, he used the closed point sieve to show that the asymptotic density of degree d hypersurfaces that intersect X transversely as

$d \to \infty$ is $\zeta_X(m+1)^{-1}$. More precisely, if $\mathcal{S} \subseteq \bigcup_d H^0(\mathbb{P}^n, \mathcal{O}(d))$, the asymptotic density of $\mathcal{S}$, denoted by $\mu(\mathcal{S})$, is defined by

$$\mu(\mathcal{S}) := \lim_{d\to\infty} \frac{\#\mathcal{S} \cap H^0(\mathbb{P}^n, \mathcal{O}(d))}{\#H^0(\mathbb{P}^n, \mathcal{O}(d))}$$

if it exists, and Poonen proved the following theorem:

Theorem 1.1. *Let X be a smooth quasi-projective subscheme of $\mathbb{P}^n$ of dimension $m \geq 0$ over $\mathbb{F}_q$. Define*

$$\mathcal{P} := \{f \in \bigcup_{d\geq 0} H^0(\mathbb{P}^n, \mathcal{O}(d)) : \{f = 0\} \cap X \text{ is smooth of dimension } m-1\}$$

Then $\mu(\mathcal{P}) = \zeta_X(m+1)^{-1}$.

Poonen employed an analogue of the sieve method in number theory, which he called the "closed point sieve", in the proof of the theorem. We may explain the main idea of his proof here. The condition that $\{f = 0\} \cap X$ is singular at a closed point $Q \in X$ amounts to $m+1$ linear conditions on the coefficients of f, since if we dehomogenize f in an affine chart of $\mathbb{P}^n$ that contains Q to obtain a regular function in the neighborhood of Q, then all partial derivatives of this function have to vanish. These linear conditions are over the residue field of Q. When d is large enough, f has more than $d+1$ coefficients, the density of f such that $f = 0$ intersects X transversely at Q is $(1 - q^{-(m+1)\deg Q})$. In fact, let $\mathcal{P}_e$ denote the set $\bigcup_d \{f \in H^0(\mathbb{P}^n, \mathcal{O}(d)) : \{f = 0\} \cap X \text{ is smooth at all } Q \text{ with } \deg Q \leq e\}$, it is not hard to prove that

$$\mu(\mathcal{P}_e) = \prod_{Q\in X : \deg Q \leq e} (1 - q^{-(m+1)\deg Q})$$

We may guess that $\mu(\mathcal{P}) = \lim_{d\to\infty} \mu(\mathcal{P}_e) = \zeta_X(m+1)^{-1}$. Indeed, essentially what we need to do is to justify a change of the order of two limits

$$\lim_{d\to\infty} \frac{\#\cap_{e=1}^{\infty} \mathcal{P}_e \cap H^0(\mathbb{P}^n, \mathcal{O}(d))}{\#H^0(\mathbb{P}^n, \mathcal{O}(d))} = \lim_{e\to\infty} \lim_{d\to\infty} \frac{\#\mathcal{P}_e \cap H^0(\mathbb{P}^n, \mathcal{O}(d))}{\#H^0(\mathbb{P}^n, \mathcal{O}(d))}$$

Therefore, the only thing left is to bound the tail terms, and indeed this is the most technical part of the proof. Poonen used a very clever decoupling idea to control the error that arises from ignoring the conditions from points of high degree.

In fact, Poonen proved a more general version of the theorem, with which he demonstrated many new results. He used it to construct counterexamples to the original hyperplane Bertini theorem when the base field is finite. He could also construct examples of space-filling and space-avoiding varieties. For example, he proved the following:

Theorem 1.2. *Let X be a smooth, projective, geometrically integral variety of dimension $m \geq 1$ over $\mathbb{F}_q$, and let E be a finite extension of $\mathbb{F}_q$. Then there exists a smooth, projective, geometrically integral curve $Y \subseteq X$ such that $Y(E) = X(E)$.*

Poonen's theorem 1.1 has been generalized by Erman and Wood to semi-ample divisors in [3].

Theorem 1.3. *Let X be a smooth projective variety over $\mathbb{F}_q$, with a very ample divisor A and a globally generated divisor E. Let π be the map given by the complete linear series on E.*

$$\pi : X \stackrel{|E|}{\to} \mathbb{P}^M$$

There exists an n_0, depending only on $\dim X$ and $\operatorname{char} \mathbb{F}_q$, such that for $n \geq n_0$, the probability of smoothness for a random $D \in |nA + dE|$ as $d \to \infty$ is given by the product of local probabilities taken over the fibers of π:

$$\operatorname{Prob}(D \textit{ is smooth}) = \prod_{P \in \mathbb{P}^M} \operatorname{Prob}(D \textit{ is smooth at all points of } \pi^{-1}(P)).$$

The product on the right converges, is zero only if some factor is zero, and is always non-zero for n sufficiently large.

By "probability", they mean an asymptotic probability, which is defined in the same way that Poonen defined the asymptotic density.

This thesis studies non-singular hypersurfaces of bidegree $(3, d)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2 \times \mathbb{P}^1$ over a finite field $\mathbb{F}_q$. Via the second projection to $\mathbb{P}^1$, these hypersurfaces can viewed as $\mathbb{P}^1$-families of three collinear points and plane cubics respectively. Due to topological constraints, these families will inevitably contain some singular fibers. We may ask for the density of those families whose fibers have at worst the simplest type of singularity. We borrow techniques from [3] to show that we can express this density as an infinite product taken over all closed points in $\mathbb{P}^1$. However, we need to make some nontrivial adjustments to the sieve method to bound the error terms in our case. In particular, in the study of hypersurfaces of bidegree $(3, d)$ in $\mathbb{P}^2 \times \mathbb{P}^1$, we employ the basic idea of *linearization*.

In [1], Poonen proposed a principle that "If an existence result about polynomials or n-tuples of polynomials over an infinite field can be proved by dimension counting, then a corresponding result over finite fields can be proved by the closed point sieve." Both our results conform to this principle. The author hopes that these results will be of some use to inspire the formulation of some meta-theorems that make this principle precise.

2 Simply Ramified Curves in $\mathbb{P}^1 \times \mathbb{P}^1$

2.1 Introduction

Among other things, Erman and Wood showed that for fixed $n \geq 3$, over a finite field $\kappa = \mathbb{F}_q$, the asymptotic probability for a randomly chosen curve in $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree (n, d) to be non-singular is $\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-1}\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(3)^{-1}$ as $d \to \infty$ [[3], Theorem 9.5]. In this section, we attempt to study ramifications of these curves with respect to the second projection $\pi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$. When $n \geq 2, d > 1$, a non-singular curve C of bidegree (n, d) has genus $nd-n-d+1 > 0$ [[5], Chapter III Exercise 5.6 (c)], and hence by Riemann-Hurwitz theorem, $\pi : C \to \mathbb{P}^1$ is necessarily ramified. In other words, if we view the curve C as a $\mathbb{P}^1$-family of three collinear points via π, then C necessarily contains singular fibers.

Nonetheless we can show that if the ground field κ is algebraically closed, then for a sufficiently general choice of C, the ramification of $\pi : C \to \mathbb{P}^1$ is simple. Moreover, the set of the curves with this property forms a dense subset of $|\mathcal{O}_{\mathbb{P}^1\times\mathbb{P}^1}(n, d)|$, viewed as a projective space. Then we borrow techniques from papers [4] and [3] to show that when $\kappa = \mathbb{F}_q$ with $p = \operatorname{char} \mathbb{F}_q > 2$ and $n = 3$, the asymptotic probability for a randomly chosen curve in the divisor class $|\mathcal{O}_{\mathbb{P}^1\times\mathbb{P}^1}(3, d)|$ to be simply ramified with respect to π is $\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-2}$ as $d \to \infty$.

Notation Let X be $\mathbb{P}^1 \times \mathbb{P}^1$ over a ground field κ. We label its coordinates as $((s_0, s_1), (t_0, t_1))$. $\pi : X \to \mathbb{P}^1$ is the second projection. If $W \subset \mathbb{P}^1$ is a finite subscheme, the fiber $\pi^{-1}(W) \subset X$ is denoted by X_W. Let $R_{n,d} \subseteq \kappa[s_0, s_1, t_0, t_1]$ be the set of bihomogeneous polynomials that are of degree n in s_0, s_1 and d in t_0, t_1. $R_{n,d}$ can be naturally identified with $H^0(\mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(n, d))$. For a section $f \in R_{n,d}$, the curve in X cut out by f is denoted by H_f. The fiber of H_f over $P \in \mathbb{P}^1$ is denoted by $(H_f)_P$. If $Q \in X$ is a closed point and $C \subseteq X$ is a curve that is non-singular at Q, then $e_Q(C)$ denotes the ramification degree of C with respect to π. When $\kappa = \mathbb{F}_q$ is finite, for a subset $\mathcal{P} \subseteq \bigcup_d R_{n,d}$, we define

$$\operatorname{Prob}(f \in \mathcal{P}) := \lim_{d\to\infty} \operatorname{Prob}(f_d \in \mathcal{P}) = \lim_{d\to\infty} \frac{\#\mathcal{P} \cap R_{n,d}}{\#R_{n,d}}$$

where f and f_d are randomly chosen from $\bigcup_d R_{n,d}$ and $R_{n,d}$ respectively.

In general, if Y is a scheme and Q is a closed point in Y, we use $Q^{(2)}$ to denote the first-order infinitesimal neighborhood of Q in Y. The residue field of Q is denoted by $\kappa(Q)$.

2.2 A Density Result over Finite Fields

Theorem 2.1. *Suppose $p = \mathrm{char}\mathbb{F}_q > 2$. Let $\mathcal{D} \subset \bigcup_d R_{3,d}$ be the subset of sections f such that H_f is simply ramified with respect to π. Then*

$$\mathrm{Prob}(f \in \mathcal{D}) = \zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-2}$$

Furthermore, the conditional probability for a randomly chosen non-singular curve of bidegree $(3,d)$ to be simply ramified is $\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(3)/\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)$ as $d \to \infty$.

For convenience, we say $f \in R_{n,d}$ is "good" at $Q \in X$, if H_f is non-singular at Q and $e_Q(H_f) \leq 2$. If $Q \notin H_f$, then by default f is good at Q. Otherwise we say that f is bad at Q. For a fixed $e_0 \in \mathbb{N}$, we define

$$\mathcal{P}^{\mathrm{low}}_{e_0} = \bigcup_{d\geq 0}\{f \in R_{3,d} : f \textit{ is good at all } Q \in X, \deg \pi(Q) < e_0\}$$
$$\mathcal{Q}^{\mathrm{med}}_{e_0} = \bigcup_{d\geq 0}\{f \in R_{3,d} : f \textit{ is bad at some } Q, \deg \pi(Q) \in [e_0, \lfloor d/p \rfloor]\}$$
$$\mathcal{Q}^{\mathrm{high}} = \bigcup_{d\geq 0}\{f \in R_{3,d} : f \textit{ is bad at some } Q, \deg \pi(Q) > d/p\}$$

2.2.1 Points of Low and Medium Degree

We first do some local analysis on a fiber. Let $P \in \mathbb{P}^1 = \mathrm{Proj}\ \mathbb{F}_q[t_0, t_1]$ be a closed point. Without loss of generality, we assume $t_1 \neq 0$ at P and P lies in $\mathbb{A}^1 = \mathrm{Spec}\,\mathbb{F}_q[t]$ where $t = t_0/t_1$. Let $\mathfrak{m} = (r(t)) \subseteq \mathbb{F}_q[t]$ be the maximal ideal corresponding to P, so that $\kappa(P) = \mathbb{F}_q[t]/\mathfrak{m}$, $P^{(2)} = \mathrm{Spec}\,\mathbb{F}_q[t]/\mathfrak{m}^2$ and $X_P = \mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}} \subset X$. Denote the reduction map $\mathbb{F}_q[t]/\mathfrak{m}^2 \to \mathbb{F}_q[t]/\mathfrak{m}$ by $g \mapsto \overline{g}$. We extend it to a map

$$H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}, \mathcal{O}(3)) \to H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}}, \mathcal{O}(3))$$

by applying $\mathbb{F}_q[t]/\mathfrak{m}^2 \to \mathbb{F}_q[t]/\mathfrak{m}$ to coefficients of cubic polynomials. Let

$$\varphi_P : R_{3,d} \to H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}, \mathcal{O}(3))$$

be the restriction map. H_f is non-singular at a point $Q \in X_P$ if and only if $\varphi_P(f)$ does not vanish at $Q^{(2)} \in \mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}$. If H_f is non-singular at Q, then $e_Q(H_f) < 3$ if and only if $\overline{\varphi_P(f)} \in H^0(\mathbb{P}^1_{\mathbb{F}[t]/\mathfrak{m}}, \mathcal{O}(3))$ does not have a zero of multiplicity ≥ 3 at Q . Therefore we can determine if f is good at all points in $(H_f)_P$ by looking at the image of f in $H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}, \mathcal{O}(3))$. This observation yields an independence result across fibers. More precisely, we have

Lemma 2.2. *If $\{P_1, P_2, \cdots, P_s\}$ is a set of finitely many closed points in $\mathbb{P}^1$, then for f randomly chosen from $\bigcup_d R_{3,d}$,*

$$\mathrm{Prob}(f \text{ is good at all } Q \in \coprod X_{P_i}) = \prod_{i=1}^{s} \mathrm{Prob}(f \text{ is good at all points } Q \in (H_f)_{P_i})$$

In particular, we have

$$\mathrm{Prob}(f \in \mathcal{P}_{e_0}^{\mathrm{low}}) = \prod_{\deg(P) < e_0} \mathrm{Prob}(f \text{ is good at all points } Q \in (H_f)_P)$$

since there are only finitely many points with degree $< e_0$.

Proof. Let $W := \coprod P_i^{(2)}$ and $\delta := \deg W = \sum_{i=1}^{s} 2\deg P_i$. Then we have an exact sequence

$$0 \to \mathcal{O}_X(3, d-\delta) \to \mathcal{O}_X(3,d) \to \mathcal{O}_X(3,d)|_{X_W} \to 0$$

which induces an exact sequence

$$H^0(X, \mathcal{O}_X(3,d)) \to H^0(X_W, \mathcal{O}_X(3,d)|_{X_W}) \to H^1(X, \mathcal{O}_X(3, d-\delta))$$

That $H^1(X, \mathcal{O}_X(3, d-\delta)) = 0$ when $d \geq \delta$ follows from the isomorphism $H^1(X, \mathcal{O}(a,b)) \cong H^1(X, \mathcal{O}_X(-2-a, -2-b))$ given by Serre duality and the fact that $H^1(X, \mathcal{O}_X(a,b)) = 0$ when $a, b < 0$ [[5], Chapter III Exercise 5.6 (a)]. Therefore the restriction map

$$R_{3,d} = H^0(\mathbb{P}^1 \times \mathbb{P}^1, \mathcal{O}(3,d)) \to H^0(X_W, \mathcal{O}_X(3,d)|_{X_W}) \cong \prod_{i=1}^{s} H^0(X_{P_i^{(2)}}, \mathcal{O}(3))$$

is surjective for $d \geq \sum_i 2\deg P_i$. This surjectivity, together with our observation that whether f is good at all $Q \in (H_f)_{P_i}$ is completely determined by $\varphi_{P_i}(f) \in H^0(\mathbb{P}^1_{P_i^{(2)}}, \mathcal{O}(3))$, implies that when $d \geq \delta$, we have

$$\frac{\#R_{3,d} \cap \mathcal{P}_{e_0}^{\mathrm{low}}}{\#R_{3,d}} = \prod_{i=1}^{s} \frac{\#\varphi_{P_i}(\{f \in R_{3,d} : f \text{ is good at all } Q \in X_{P_i}\})}{\#H^0(X_{P_i^{(2)}}, \mathcal{O}(3))}$$

The lemma follows by taking $d \to \infty$ on both sides. □

Before proceeding we make the following convention: A pair $(F_1, F_2) \in H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}}, \mathcal{O}(3))^2$ is said to be *bad* if it falls in one of the following 3 types:

1. F_1 has a root of multiplicity ≥ 2 at a point where F_2 also vanishes.
2. F_1 has a root of multiplicity 3 at a point where F_2 does not vanish.

3. $F_1 \equiv 0$.

Otherwise, the pair is said to be *good*. Let $\widetilde{\ }: \mathbb{F}_q[t]/\mathfrak{m} \to \mathbb{F}_q[t]/\mathfrak{m}^2$ be a $\mathbb{F}_q$-linear map that is a section to the previously defined reduction map $\mathbb{F}_q[t]/\mathfrak{m}^2 \to \mathbb{F}_q[t]/\mathfrak{m}$. We extend it to a map $H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}, \mathcal{O}(3)) \to H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}}, \mathcal{O}(3))$ in the same way we extended the reduction map. Then we have the following:

Lemma 2.3. *The $\mathbb{F}_q$-linear map*

$$H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}}, \mathcal{O}(3))^2 \to H^0(\mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}^2}, \mathcal{O}(3))$$

given by $(F_1, F_2) \mapsto \widetilde{F_1} + r(t)F_2$ is a bijection. Moreover, $f \in R_{3,d}$ is "good" at all points $Q \in \pi^{-1}(P)$ if and only if $\varphi_P(f)$ corresponds to a good pair.

Proof. The map $F \mapsto (\overline{F}, (F - \widetilde{\overline{F}})/r(t))$ is an inverse to the map given in the lemma. Let (F_1, F_2) be the pair corresponding to $\varphi_P(f)$. $\varphi_P(f)$ vanishes on $Q^{(2)}$, i.e. H_f is singular at Q, if and only if Q is a double root of F_1 and a root to F_2. Similarly, if H_f is non-singular at Q, then $e_Q(H_f) \geq 3$ if and only if Q is root to F_1 of multiplicity ≥ 3. □

Lemma 2.4. *Let $e := \deg P$. The density of good pairs in $H^0(\mathbb{P}^1_{\kappa(P)}, \mathcal{O}(3))^2$ is*

$$(1 - q^{-2e})^2$$

Proof. We first count type 1 pairs. Let $Q \in \mathbb{P}^1_{\mathbb{F}_q[t]/\mathfrak{m}} = \mathbb{P}^1_{\mathbb{F}_{q^e}}$ be the point that is a double root to F_1 and a root to F_2. Note that $\deg Q = 1$. F_1 is fixed up to rescaling by $\mathbb{F}^*_{q^e}$ after we choose a third root, which can be any point of degree 1. Therefore there are $(q^e + 1)(q^e - 1)$ choices for F_1, where $(q^e + 1)$ is the number of all possible choices for the third root. The probability that F_2 vanishes at Q as well is q^{-e}, so we have $q^{4e}q^{-e} = q^{3e}$ choices for F_2. Since we have $(q^e + 1)$ choices for Q, there are $q^{3e}(q^e + 1)^2(q^e - 1)$ type 1 pairs.

To count type 2 pairs, let $Q \in \mathbb{P}^1_{\mathbb{F}_{q^e}}$ be the triple root to F_1. Again there are $q^e + 1$ choices. At each Q, there are $(q^e - 1)$ homogeneous polynomials of degree 3 which have Q as a triple root, since the leading coefficient will uniquely determine such a polynomial. We have $q^{4e} - q^{3e}$ choices for F_2. In total there are $(q^e + 1)(q^e - 1)(q^{4e} - q^{3e})$ pairs of type 2.

Finally when $F_1 = 0$, F_2 can be anything, so we have q^{4e} type 3 pairs. Therefore the density of good pairs is

$$1 - q^{-8e}(q^{3e}(q^e + 1)^2(q^e - 1) + (q^e + 1)(q^e - 1)(q^{4e} - q^{3e}) + q^{4e}) = (1 - q^{-2e})^2$$

□

Lemma 2.5.

$$\lim_{e_0 \to \infty} \mathrm{Prob}(f \in \mathcal{Q}^{\mathrm{med}}_{e_0}) = 0$$

Proof. By definition,

$$\mathrm{Prob}(f \in \mathcal{Q}_{e_0}^{\mathrm{med}}) = \lim_{d\to\infty} \mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}})$$

for f_d randomly chosen from $R_{3,d}$. It suffices to show that $\mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}})$ is universally bounded by $O(q^{-e_0})$, where the implied constant is independent of d or e_0.

Let P be a point of degree $e \leq \lfloor d/p \rfloor$ on $\mathbb{P}^1$. By the proof of Lemma 2.2, the restriction map $R_{3,d} \to H^0(X_{P^{(2)}}, \mathcal{O}(3))$ is surjective since $p > 2$ and $e < \lfloor d/p \rfloor < d/2$. Lemma 2.3 and Lemma 2.4 hence imply that probability that f_d is "bad" at some point in the fiber X_P is $1 - (1 - q^{-2e})^2 < 2q^{-2e}$.

$$\begin{aligned}\mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}}) &\leq \sum_{e=e_0}^{\lfloor d/p \rfloor} (\text{number of points of degree } e \text{ in } \mathbb{P}^1)(2q^{-2e}) \\ &\leq 2\sum_{e=e_0}^{\lfloor d/p \rfloor} (q^e + 1)q^{-2e} = O(\frac{q^{-e_0}}{1-q^{-1}}) = O(q^{-e_0})\end{aligned}$$

□

2.2.2 Points of High Degree

Lemma 2.6. *Let $W \subseteq \mathbb{A}^M \times \mathbb{A}^1$ be a closed subscheme. Let t be the coordinate for $\mathbb{A}^1$. Denote by $A_{0,d} = \mathbb{F}_q[t]_{\leq d}$ the set of polynomials that are of degree $\leq d$ in t. Let $\pi : \mathbb{A}^M \times \mathbb{A}^1 \to \mathbb{A}^1$ be the second projection. Consider the restriction map*

$$\varphi_W : A_{0,d} \to H^0(W, \mathcal{O}_W)$$

If W contains a closed point Q such that $\deg \pi(Q) \geq j$, then $\#\{\mathrm{Im}\, \varphi_W\} \geq q^{\min(d+1,j)}$.

Proof. If $\dim \pi(W) = 1$, then t, and hence any nonzero polynomial in t, does not vanish identically on W. Therefore φ_W is injective, and $\#\{\mathrm{Im}\, \varphi_W\} = q^{d+1}$. Now suppose $\dim \pi(W) = 0$. Note that φ_W factors as

$$A_{0,d} = \mathbb{F}_q[t]_{\leq d} \overset{\psi_W}{\to} H^0(\pi(W), \mathcal{O}_{\pi(W)}) \overset{\pi^\#}{\to} H^0(W, \mathcal{O}_W)$$

Since the pull back map $\pi^\#$ is injective, it suffices to bound $\#\{\mathrm{Im}\, \psi_W\}$. Let $P = \pi(Q)$. Suppose $P = \mathrm{Spec}\, \mathbb{F}_q[t]/(r(t)) \subset \mathbb{A}^1$. Note that $\deg r(t) \geq j$ since by assumption $\deg P \geq j$. The composition

$$\mathbb{F}_q[t]_{\leq d} \to H^0(\pi(W), \mathcal{O}_{\pi(W)}) \to \kappa(P)$$

is nothing but the natural map $\mathbb{F}_q[t]_{\leq d} \to \mathbb{F}_q[t]/r(t)$. Therefore

$$\#\{\mathrm{Im}\, (\mathbb{F}_q[t]_{\leq d} \to \kappa(P))\} = q^{\min(d+1,j)} \leq \#\{\mathrm{Im}\, \psi_W\}$$

□

We use the following lemma to bound the probability that a randomly chosen $f \in R_{3,d}$ is bad at some point Q when $\pi(Q)$ has high degree ($> \lfloor d/p \rfloor$). Therefore the following lemma is to be applied with $j = \lfloor d/p \rfloor$.

Lemma 2.7. *Let $j > 2$ be an integer and $U \subseteq X$ be an open subscheme. For a randomly chosen $f \in R_{3,d}$, the probability that there exists a point $Q \in U$ with $\deg \pi(Q) \geq j$ such that H_f is non-singular at Q but $e_Q(H_f) \geq 3$ or H_f is singular at Q is at most*

$$O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

Proof. Among all U, the lemma is clearly strongest when $U = X$. Since $\mathbb{P}^1 \times \mathbb{P}^1$ can be covered by 4 affine charts $\mathbb{A}^1 \times \mathbb{A}^1$, we reduce to proving the lemma for all $\mathbb{A}^1 \times \mathbb{A}^1$.

Without loss of generality, we may assume $s_1 \neq 0, t_1 \neq 0$ on $U = \mathbb{A}^1 \times \mathbb{A}^1$ and work with coordinates $s = s_0/s_1, t = t_0/t_1$. Let $A_{n,d} \subseteq \mathbb{F}_q[s,t] = H^0(U, \mathcal{O}_U)$ be the polynomials that are of degree $\leq n$ in s and $\leq d$ in t. Clearly by dehomogenizing sections in $R_{3,d}$, we have a natural identification $R_{3,d} = A_{3,d}$. Accordingly, we replace H_f by $H_f \cap \mathbb{A}^1 \times \mathbb{A}^1$. We call a closed point $Q \in \mathbb{A}^1 \times \mathbb{A}^1$ *admissible* if $\deg \pi(Q) \geq j$ and a subscheme $W \subseteq \mathbb{A}^1 \times \mathbb{A}^1$ *admissible* if it contains an admissible point. By $(W)_{\mathrm{ad}}$ we denote the union of admissible irreducible components of $(W)_{\mathrm{red}}$.

We first deal with the probability that for a randomly chosen $f \in A_{3,d}$, $e_Q(H_f) \geq 3$ at some admissible $Q \in \mathbb{A}^1 \times \mathbb{A}^1$, which happens only if

$$f(Q) = f_s(Q) = f_{ss}(Q) = 0 \tag{2.8}$$

Define subschemes $W_2 = \{f_{ss} = 0\}, W_1 = W_2 \cap \{f_s = 0\}$ and $W_0 = W_1 \cap \{f = 0\}$ in $\mathbb{A}^1 \times \mathbb{A}^1$. We reduce the problem to bounding the probability that for a randomly chosen $f \in A_{3,d}$, W_0 contains an admissible point.

Following Poonen's idea [[4], Proof of Lemma 2.6], we write f in such a way so that the first and second order partial derivatives with respect to s are largely independent. If $f_0 \in A_{3,d}$ and $g_1, g_2, h \in A_{0,\lfloor d/p \rfloor}$ are selected uniformly and independently at random, then the distribution of

$$f = f_0 + g_1^p s^2 + g_2^p s + h^p$$

is uniform over $A_{3,d}$. Direct computation shows that

$$\begin{aligned} f_s &= f_{0,s} + 2g_1^p s + g_2^p \\ f_{ss} &= f_{0,ss} + 2g_1^p \end{aligned}$$

Note that W_2 depends only on the choice of f_0, g_1 and W_1 only on f_0, g_1, g_2. Let E denote the event that

a. $\dim (W_1)_{\mathrm{ad}} = 0$

b. f does not vanish identically on any irreducible component of $(W_1)_{\mathrm{ad}}$.

Clearly if E holds for f, then W_0 does not contain any admissible point. Therefore it suffices to show that for a randomly chosen $f \in A_{3,d}$,

$$\mathrm{Prob}(E) = 1 - O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

as $d \to \infty$. Now we bound $\mathrm{Prob}(E)$ in three steps:

Step 1: Conditioned on a choice of f_0, the probability that $\dim W_2 = 2$ is at most $q^{-(\lfloor d/p \rfloor + 1)}$, since $\dim W_2 = 2$ if and only if $g_1^p = -f_{0,ss}/2$, for which there is at most one choice of g_1.

Step 2: Conditioned on a choice of f_0 and g_1 such that $\dim W_2 = 1$, the probability that $\dim (W_1)_{\mathrm{ad}} = 1$ is at most $O(dq^{-\min(\lfloor d/p \rfloor + 1, j)})$. Let $V_1, \cdots, V_\ell$ be all the irreducible component of $(W_2)_{\mathrm{red}}$. Viewing $\mathbb{P}^1 \times \mathbb{P}^1$ as a subscheme of $\mathbb{P}^3$ via the Segre embedding, we may apply Bézout's theorem to obtain that $\ell = O(d)$. $\dim (W_1)_{\mathrm{ad}} = 1$ if and only if f_s vanishes identically on V_i for some i. We need to bound the set

$$G_i^{\mathrm{bad}} = \{g_2 \in A_{0,\lfloor d/p \rfloor} : f_{0,s} + 2g_1^p s + g_2^p \textit{ vanishes identically on } V_i\}$$

If $g, g' \in G_i^{\mathrm{bad}}$, then $g - g'$ vanishes identically on V_i. Therefore G_i^{bad} is a coset of $\ker \varphi_i$, where φ_i is the $\mathbb{F}_q$-linear restriction map $A_{0,\lfloor d/p \rfloor} \to H^0(V_i, \mathcal{O}_{V_i})$. Now we apply Lemma 2.6 to obtain that $\#\{\mathrm{Im}\, \varphi_i\} \geq q^{\min(\lfloor d/p \rfloor + 1, j)}$. This means the probability that f_s vanishes identically on V_i is

$$\mathrm{Prob}(g_2 \in G_i^{\mathrm{bad}}) = \frac{\# G_i^{\mathrm{bad}}}{\# A_{0,\lfloor d/p \rfloor}} \leq q^{-\min(\lfloor d/p \rfloor + 1, j)}$$

Since there are $\ell = O(d)$ many V_i's, the probability that f_s vanishes identically on any of them is bounded by $O(dq^{-\min(\lfloor d/p \rfloor + 1, j)})$ as claimed.

Step 3: Conditioned on a choice of f_0, g_1 and g_2 such that $\dim (W_1)_{\mathrm{ad}} = 0$, the probability that $(W_0)_{\mathrm{ad}} \neq \emptyset$ is at most $O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})$. Let $Q_1, Q_2, \cdots, Q_{\ell'}$ be all irreducible components of $(W_1)_{\mathrm{ad}}$. Since W_1 is cut out by f_s and f_{ss}, again by considering the Segre embedding $\mathbb{P}^1 \times \mathbb{P}^1 \hookrightarrow \mathbb{P}^3$, we obtain from Bézout's theorem $\ell' = O(d^2)$. Since $\pi(Q_i) \geq j$ by assumption, we may apply Lemma 2.6 again obtaining that for each Q_i, $\mathrm{Im}\, (A_{0,\lfloor d/p \rfloor} \to H^0(Q_i, \mathcal{O}_{Q_i})) \geq q^{\min(\lfloor d/p \rfloor + 1, j)}$. This implies that the probability that f vanishes at Q_i is bounded above by $q^{-\min(\lfloor d/p \rfloor + 1, j)}$. Since there are at most $O(d^2)$ of Q_i's, we obtain the desired conclusion of this step.

Finally *Step 1* and *2* combine to give that

$$\begin{aligned}\mathrm{Prob}(\dim (W_1)_{\mathrm{ad}} = 0) &\geq (1 - q^{-(\lfloor d/p \rfloor + 1)})(1 - q^{-\min(\lfloor d/p \rfloor + 1, j)}) \\ &= 1 - O(dq^{-\min(\lfloor d/p \rfloor + 1, j)})\end{aligned}$$

And *Step 3* gives

$$\begin{aligned}\mathrm{Prob}(E) &\geq \mathrm{Prob}(\dim (W_1)_{\mathrm{ad}} = 0)(1 - O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})) \\ &= 1 - O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})\end{aligned}$$

Now we deal with the probability that H_f is singular at Q for some $Q \in \mathbb{A}^1 \times \mathbb{A}^1$, which happens if and only if $f(Q) = f_s(Q) = f_t(Q) = 0$. Again we choose $f_0 \in A_{3,d}$ $g_1, g_2, h \in A_{0,\lfloor d/p \rfloor}$ uniformly at random, but this time we put

$$f = f_0 + g_1^p t + g_2^p s + h^p$$

The distribution of f is uniform over $A_{3,d}$. The rest of the proof is rather analogous to what we did before, so we only give a sketch. Define $W_2' = \{f_t = 0\}, W_1' = W_2' \cap \{f_s = 0\}$ and $W_0' = W_1' \cap \{f = 0\}$. W_2' depends only on the choices of f_0, g_1 and W_1' only on f_0, g_1, g_2. By applying the same arguments as in *Step 1* and *2*, we may show that

$$\mathrm{Prob}(\dim (W_1')_{\mathrm{ad}} = 0) = 1 - O(dq^{-\min(\lfloor d/p \rfloor + 1, j)})$$

By applying the same arguments as in *Step 3*, we may bound the probability that f does not vanish at any of the irreducible components of $(W_1')_{\mathrm{ad}}$ given that $\dim (W_1')_{\mathrm{ad}} = 0$, so that

$$\mathrm{Prob}((W_0')_{\mathrm{ad}} = \emptyset) \geq 1 - O(d^2 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

Now the proof of the lemma is complete. □

Lemma 2.9.

$$\mathrm{Prob}(f \in \mathcal{Q}^{\mathrm{high}}) = 0$$

Proof. Apply Lemma 2.7 with $U = X$ and $j = \lfloor d/p \rfloor$. Then we take the limit as $d \to \infty$. □

Now we have gathered all the ingredients needed to prove Theorem 2.1.
Proof of Theorem 2.1. For each e_0, we have that

$$\mathcal{P}_{e_0}^{\mathrm{low}} \subseteq \mathcal{D} \subseteq \mathcal{P}_{e_0}^{\mathrm{low}} \cup \mathcal{Q}_{e_0}^{\mathrm{med}} \cup \mathcal{Q}^{\mathrm{high}}$$

Therefore

$$\mathrm{Prob}(f \in \mathcal{P}_{e_0}^{\mathrm{low}}) \leq \mathrm{Prob}(f \in \mathcal{D}) \leq \mathrm{Prob}(f \in \mathcal{P}_{e_0}^{\mathrm{low}} \cup \mathcal{Q}_{e_0}^{\mathrm{med}} \cup \mathcal{Q}^{\mathrm{high}})$$

Now take $e_0 \to \infty$, Lemma 2.2, 2.4, 2.5, and 2.9 combine to give that

$$\begin{aligned}\mathrm{Prob}(f \in \mathcal{D}) &= \lim_{e_0 \to \infty} \mathrm{Prob}(f \in \mathcal{P}_{e_0}^{\mathrm{low}}) \\ &= \prod_{P \in \mathbb{P}^1} \mathrm{Prob}(f \textit{ is good at all points } Q \in (H_f)_P) \\ &= \prod_{P \in \mathbb{P}^1} (1 - q^{-2\deg P})^2 \\ &= \zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-2}\end{aligned}$$

The statement on the conditional probability in Theorem 2.1 now follows directly from Erman and Wood's result [[3], Theorem 9.5] that the asymptotic probability for a randomly chosen curve of bidegree $(3, d)$ to be non-singular is $\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-1}\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(3)^{-1}$. □

3 Elliptic Surfaces in $\mathbb{P}^2 \times \mathbb{P}^1$

3.1 Introduction

In this section we study non-singular hypersurfaces in $\mathbb{P}^2 \times \mathbb{P}^1$ given by sections in $H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d))$. Such a surface can be viewed as a $\mathbb{P}^1$-family of plane cubics that may contain degenerate (singular) fibers.

We first discuss some geometric properties. In the space $\mathbb{P}H^0(\mathbb{P}^2, \mathcal{O}(3))$ which parametrizes plane cubics, curves with worse than nodal singularities (reducible or cuspidal) comprise a closed subset of codimension 2. A $\mathbb{P}^1$-family of plane cubics corresponds to a morphism $\mathbb{P}^1 \to \mathbb{P}H^0(\mathbb{P}^2, \mathcal{O}(3))$. A Bertini type argument shows that those non-singular hypersurfaces whose fibers have at most nodal singularities comprise an open dense subset of the parameter space $\mathbb{P}H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d)) \simeq \mathbb{P}^9$. We say these hypersurfaces are *"good"*. When the base field κ is infinite, we see that the density of good hypersurfaces is 1.

However, when $\kappa = \mathbb{F}_q$ is a finite field, $H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3, d))$ is a finite set, so sections that do not give good hypersurfaces may have a nonzero density. *In the rest of this section, we assume that* $\mathrm{char}\,\mathbb{F}_q > 3$. In a similar vein to section 2, we may show that as $d \to \infty$, this density converges to an infinite product over $\mathbb{P}^1$. We may explicitly compute the terms in this infinite product and then show that this infinite product converges. Before introducing the result, we first introduce some notations.

Notation Let us label the coordinates of $\mathbb{P}^2 \times \mathbb{P}^1$ as $((X_0 : X_1 : X_2), (T_0 : T_1))$ and let $S_{3,d} \subseteq \mathbb{F}_q[X_0, X_1, X_2, T_0, T_1]$ be the set of bi-homogeneous polynomials

of degree 3 in X_i's and d in T_j's. Then $S_{3,d}$ can be identified with $H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3,d))$ in the natural way. If $\mathcal{B} \subseteq \bigcup_d S_{3,d}$ is a subset, then we define the *asymptotic probability* for a randomly chosen $f \in S_{3,d}$ to belong to $\mathcal{B}$, or simply *probability*, as

$$\mathrm{Prob}(f \in \mathcal{B}) = \lim_{d\to\infty} \frac{\#\mathcal{B} \cap S_{3,d}}{\#S_{3,d}}$$

if it exists. Given a section $f \in S_{3,d}$, we denote the corresponding hypersurface defined by the vanishing of f as H_f. Let $P \in \mathbb{P}^1_{\mathbb{F}_q}$ be a point. We say that a hypersurface H_f, or sometimes f, is *good* at the point P if H_f is non-singular at all points $Q \in \pi^{-1}(P)$, and the fiber $(H_f)_P \subseteq \mathbb{P}^2_{\kappa(P)}$ is either a non-singular or a nodal curve. Otherwise, we say H_f, or f, is *bad* at P. Of course, a hypersurface is good if and only if it is good at every $P \in \mathbb{P}^1_{\mathbb{F}_q}$. Define

$$\mathcal{S} = \bigcup_d \{f \in S_{3,d} : H_f \textit{ is good}\}$$
$$\text{and for } P \in \mathbb{P}^1_{\mathbb{F}_q}, \mathcal{S}_P = \bigcup_d \{f \in S_{3,d} : H_f \textit{ is good at } P\}$$

We will show that

Lemma 3.1. *Let $e = \deg P$. Then*

$$\mathrm{Prob}(f \in \mathcal{S}_P) = (1+q^{-2e})(1-2q^{-2e}-q^{-4e}+q^{-5e}-2q^{-6e}-q^{-7e})$$

In particular, we have inequalities

$$(1-q^{-2e})(1-q^{-3e/2}) < \mathrm{Prob}(f \in \mathcal{S}_P) < (1-q^{-2e})(1-2q^{-2e}+q^{-4e}) = (1-q^{-2e})^3$$

Now we may state our main theorem for elliptic surfaces over finite fields:

Theorem 3.2. *Assume* $\mathrm{char}\mathbb{F}_q > 3$. *The density of good hypersurfaces of bidegree $(3,d)$ in $\mathbb{P}^2 \times \mathbb{P}^1$ over $\mathbb{F}_q$ converges to a number in $(0,1)$ as $d \to \infty$. More precisely,*

$$\mathrm{Prob}(f \in \mathcal{S}) = \prod_{P \in \mathbb{P}^1_{\mathbb{F}_q}} \mathrm{Prob}(f \in \mathcal{S}_P)$$

Combined with the previous lemma, we obtain a bound for $\mathrm{Prob}(\mathcal{S})$ *in terms of Zeta functions:*

$$\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-1}\zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(3/2)^{-1} < \mathrm{Prob}(f \in \mathcal{S}) < \zeta_{\mathbb{P}^1_{\mathbb{F}_q}}(2)^{-3}$$

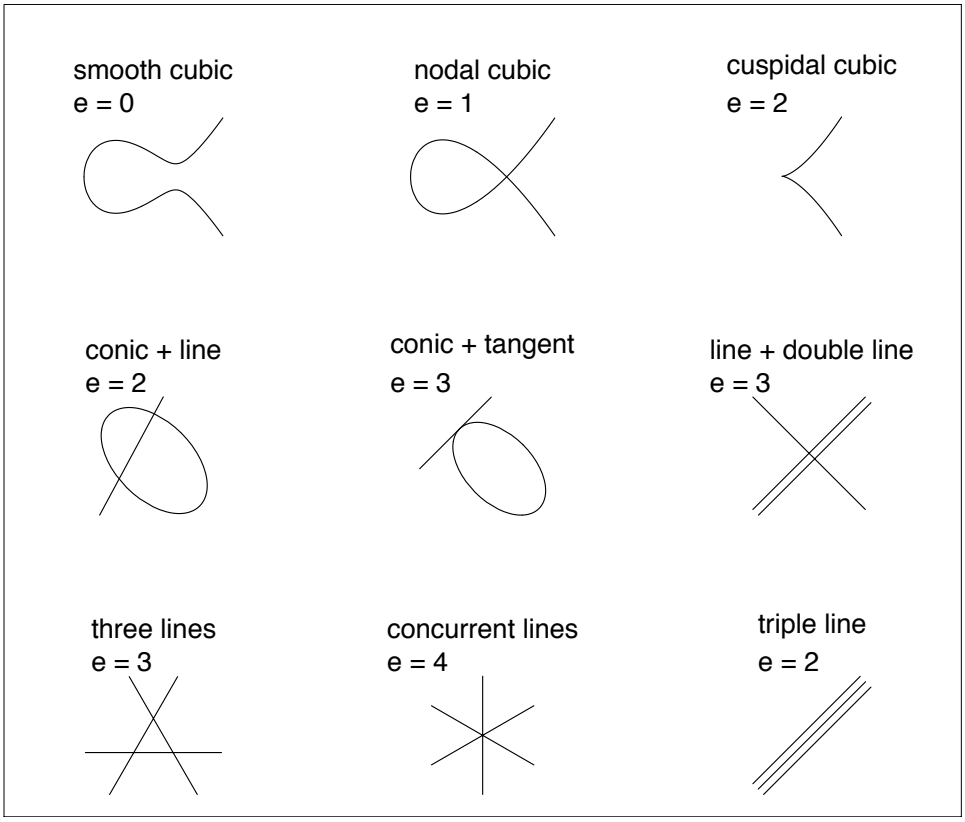


Figure 1: Cubic plane curves and their Euler characteristics [2]

3.2 Plane Cubics

3.2.1 Classification

We first make some easy observations on plane cubics. The following is a table made by B. Poonen that classifies all plane cubics. For convenience we are going to use the same terminology.

We may use tangent cones to differentiate the nodal cubics from singular cubics of other types. Suppose we find a singular point Q on a cubic C. We ask two questions:

1. Does the tangent cone of C at Q contain a double line? If yes, then we have found a cuspidal cubic or a reducible cubic of the type conic + tangent, line + double line, or a triple line.

2. Does the tangent cone of C at Q share an irreducible component, which has to be a line, with C? If yes, then we have found a reducible cubic.

If both answers are no, then we have found a nodal cubic. Now we explain how to perform the above tests using partial derivatives.

Let us label the coordinates of $\mathbb{P}^2$ as X_0, X_1, X_2 and let $Q \in \mathbb{P}^2$ be a closed point. Without loss of generality, we assume $X_0(Q) \neq 0$ and dehomogenize a homogeneous cubic polynomial in $\kappa[X_0, X_1, X_2]$ at X_0 to a polynomial g in $x_1 = X_1/X_0, x_2 = X_2/X_0$. The cubic $C = \{g = 0\}$ is singular at Q if and only if

$$g(Q) = \frac{\partial g}{\partial x_1}(Q) = \frac{\partial g}{\partial x_2}(Q) = 0$$

Suppose Q is a singularity. Note that $\deg Q$ has to be 1 since a plane cubic cannot be singular at a point of higher degree. For $m = 2, 3$, we define polynomials

$$T^m g(U_0, U_1) = \sum_{r+s=m} \frac{\partial^m g}{\partial x_1^r x_2^s}(Q) U_0^r U_1^s \in \kappa[U_0, U_1]$$

which are homogeneous in U_0, U_1. If $T^2 g(U_0, U_1) \equiv 0$, then the tangent cone of C at Q must have degree 3, in which case C must be a triple line, a line + double line, concurrent lines, or three lines (see Figure 1). Otherwise, $T^2 g(x_1 - x_1(Q), x_2 - x_2(Q)) = 0$ describes the (affine) tangent cone of C at Q, which we denote by $TC_Q(C)$. $TC_Q(C)$ contains a double line if and only if $T^2 g(U_0, U_1)$ vanishes at a closed point in $\mathbb{P}^1 = \operatorname{Proj} \kappa[\mathrm{U}_0, \mathrm{U}_1]$ with multiplicity ≥ 2. For convenience, we say a triple line contains a double line, and if $T^2 g(U_0, U_1) \equiv 0$, it vanishes at all points in $\operatorname{Proj} \kappa[\mathrm{U}_0, \mathrm{U}_1]$ with ∞ multiplicity. Taylor expansion of g at Q says

$$g = T^2 g(x_1 - x_1(Q), x_2 - x_2(Q)) + T^3 g(x_1 - x_1(Q), x_2 - x_2(Q))$$

we see that the $TC_Q(C)$ shares an irreducible component with C if and only if there $T^2 g(U_0, U_1)$ and $T^3 g(U_0, U_1)$ share a zero on $\operatorname{Proj} \kappa[\mathrm{U}_0, \mathrm{U}_1]$. Therefore if we fix a particular closed point in $\operatorname{Proj} \kappa[\mathrm{U}_0, \mathrm{U}_1]$, then both conditions on $T^m(U_0, U_1)$ become linear in partial derivatives.

We may summarize the above observations into a geometric statement: Let $\mathbb{A}^2 \subseteq \mathbb{P}^2$ be the affine chart as above. Consider two subschemes of $\mathbb{A}^2 \times \operatorname{Proj} \kappa[\mathrm{U}_0, \mathrm{U}_1]$:

$$\mathcal{W}_1 = \{g = \frac{\partial g}{\partial x_1} = \frac{\partial g}{\partial x_2} = T^2 g(U_0, U_1) = 0\}$$
$$\mathcal{W}_2 = \{g = \frac{\partial g}{\partial x_1} = \frac{\partial g}{\partial x_2} = T^2 g(U_0, U_1) = T^3 g(U_0, U_1) = 0\}$$

1. If there does not exist a closed point $Q \in \mathbb{A}^2$ such that the fiber of $\mathcal{W}_1$ over Q is non-reduced, then C cannot be a cuspidal curve with the singularity in this affine chart $\mathbb{A}^2$.

2. If $\mathcal{W}_2 = \emptyset$, then C cannot be a reducible curve with a singularity in this affine chart $\mathbb{A}^2$.

These statements are weaker than our observations, but they suffice for our purposes. We are going to use them in the proof of Lemma 3.10.

3.2.2 Counting Plane Cubics of Different Types

In this section we count the number of reducible, cuspidal and nodal cubics in the projective plane $\mathbb{P}^2$ over a finite field $\mathbb{F}_q$. Plane cubics are given by sections in $S = H^0(\mathbb{P}^2, \mathcal{O}(3))$. We may identify S with the subset of $\mathbb{F}_q[X_0, X_1, X_2]$ consisting of homogeneous polynomials of degree 3. Given $f \in S$, we denote its vanishing locus in $\mathbb{P}^2$ by $Z(f)$. Define

$$R = \{f \in S : Z(f) \textit{ is reducible}\}$$
$$C = \{f \in S : Z(f) \textit{ is cuspidal}\}$$
$$N = \{f \in S : Z(f) \textit{ is nodal}\}$$

Let $H_j \subseteq \mathbb{F}_q[U_0, U_1]$ denote the set of homogeneous polynomials of degree j. Given $g \in H_j$, denote its vanishing locus in $\mathbb{P}^1 = \text{Proj } \mathbb{F}_q[U_0, U_1]$ by $Z(g)$. Note that $\dim_{\mathbb{F}_q} H_j = j + 1$. If $g \in H_j$ and $W \in \mathbb{P}^1$ is a finite subscheme, let $g|_W$ be the element of $H^0(W, \mathcal{O}_W)$ that on each connected component W_i equals the restriction of $U_i^{-j} g$, where i is the smallest index such that $U_i \neq 0$ at W_i.

Lemma 3.3. *If $g_2 \in H_2, g_3 \in H_3$ are randomly chosen, then*

$$\text{Prob}(g_2 \textit{ is coprime to } g_3 \mid g_2 \textit{ is a nonzero square}) = 1 - q^{-1}$$

Proof. Let L be the closed point contained in $Z(g_2)$. g_2 and g_3 are coprime if and only if $L \notin Z(g_3)$. Since $\deg L = 1$, the $\mathbb{F}_q$-linear map $H_3 \to \kappa(L)$ given by $g_3 \mapsto g_3|_L$ is surjective. Therefore the probability that a randomly chosen $g_3 \in H_3$ vanishes at L is $1/\#\kappa(L) = 1/q$. □

Lemma 3.4. *If $g_2 \in H_2, g_3 \in H_3$ are randomly chosen, then*

$$\text{Prob}(g_3 \textit{ is coprime to } g_2 \,|\, g_2 \textit{ is not a square}) = \frac{1}{q^3}(q+1)(q-1)^2$$

Proof. Now we have to divide it into two cases.
Case 1: g_2 is an reducible polynomial, so that $Z(g_2)$ contains two distinct closed points L_1, L_2, both of which have to be of degree 1. g_3 is coprime to g_2 if and only if $L_1, L_2 \notin Z(g_3)$. Since $H_3 \to \kappa(L_1) \oplus \kappa(L_2)$ is surjective, events $\{g_3(L_1) = 0\}$ and $\{g_3(L_2) = 0\}$ are independent. Hence

$$\text{Prob}(g_3 \textit{ is coprime to } g_2 \mid g_2 \textit{ is reducible}) = (1 - q^{-1})^2$$

By counting the number of pairs (L_1, L_2), $L_1 \neq L_2$, we easily see that

$$\#\{g_2 \in H_2 : g_2 \textit{ is reducible with two distinct roots}\} = \frac{1}{2}q(q+1)(q-1)$$

where the factor $q-1$ comes from the fact that g_2 is determined by L_1, L_2 up to scalar multiplication by $\mathbb{F}_q^\times$.
Case 2: g_2 is an irreducible polynomial. Then g_3 fails to be coprime to g_2 if and only if g_2 divides g_3 if and only if g_3 vanishes at $L_2 := Z(g_2)$, which is a closed point of degree 2. Since $H_3 \to \kappa(L_2)$ given by $g_3 \mapsto g_3|_{L_2}$ is surjective,

$$\text{Prob}(g_3 \textit{ is coprime to } g_2 \mid g_2 \textit{ is irreducible}) = 1 - q^{-2}$$

Since there are $(q^2-q)/2$ possible choices for L_2's and g_2 is determined by L_2 up to a nonzero constant in $\mathbb{F}_q$, we see that

$$\#\{g_2 \in H_2 : g_2 \textit{ is irreducible}\} = \frac{1}{2}(q^2-q)(q-1)$$

Therefore the conditional probability in the lemma equals to

$$\frac{q+1}{2q}(1-q^{-1})^2 + \frac{q-1}{2q}(1-q^{-2}) = \frac{1}{q^3}(q+1)(q-1)^2$$

□

Lemma 3.5. *Let $Q \in \mathbb{P}^2$ be a closed point of degree 1, then for a randomly chosen $f \in S$,*

$$\text{Prob}(f \textit{ is a cuspidal curve with a cusp at } Q) = \frac{1}{q^7}(q-1)^2(q+1)$$
$$\text{Prob}(f \textit{ is a nodal curve with a node at } Q) = \frac{1}{q^7}(q-1)^3(q+1)$$

Proof. Without loss of generality, assume that $X_0 \neq 0$ at Q, so that $Q \in \mathbb{A}^2$, on which we may use coordinates $x_1 = X_1/X_0, x_2 = X_2/X_0$. We further assume that $x_1(Q) = x_2(Q) = 0$, i.e. Q is the origin of the affine chart $X_0 \neq 0$. We may identify $f \in S$ with its dehomogenization $f/X_0^3 = g(x_1, x_2)$ on $\mathbb{A}^2$. We may write

$$g = g_0 + g_1 + g_2 + g_3$$

where g_j is the homogeneous part of degree j of g. If the g_j's are chosen uniformly and independently at random, then the distribution of f is uniform over S. $Z(g)$ is a cuspidal curve with a cusp at Q if and only if

i. $g_0 = g_1 = 0$ ($Z(f)$ is singular at Q.)

ii. $g_2 \neq 0$ and g_2 is a square. (The tangent cone of $Z(f)$ at Q is a doubled line.)

iii. g_2 and g_3 are coprime. ($Z(f)$ is irreducible.)

We easily see that $\text{Prob}(i) = 1/q^3$, $\text{Prob}(ii) = (q^2-1)/q^3$ and Lemma 3.3 gives $\text{Prob}(iii \mid ii)$. Therefore the probability that $Z(f)$ has a cusp at Q is

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

Similarly, $Z(g)$ is a nodal curve with a node at Q if and only if

i. $g_0 = g_1 = 0$ ($Z(f)$ is singular at Q.)

ii. $g_2 \neq 0$ and g_2 is not a square. (The tangent cone of $Z(f)$ at Q is two distinct lines.)

iii. g_2 and g_3 are coprime. ($Z(f)$ is irreducible.)

This time $\text{Prob}(i) = 1/q^3$, $\text{Prob}(ii) = (q^3-q^2)/q^3$ and Lemma 3.4 gives $\text{Prob}(iii \mid ii)$. Therefore the probability that $Z(f)$ has a node at Q is

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

□

Lemma 3.6.

$$\begin{aligned}
\#R &= (q^2+q+1)(q^6-1)\\
\#C &= q^3(q^2+q+1)(q-1)^2(q+1)\\
\#N &= q^3(q^2+q+1)(q-1)^3(q+1)
\end{aligned}$$

Proof. We obtain the number $\#R$ from the obvious $(q-1)$-to-1 surjection

$$(H^0(\mathbb{P}^2,\mathcal{O}(1)) - \{0\}) \times (H^0(\mathbb{P}^2,\mathcal{O}(2)) - \{0\}) \to R \subset H^0(\mathbb{P}^2,\mathcal{O}(3))$$

$\#C$ and $\#N$ follow directly from Lemma 3.5 and the facts that there are (q^2+q+1) closed points of degree 1 in $\mathbb{P}^2$ over $\mathbb{F}_q$ and $\dim_{\mathbb{F}_q} S = 10$. □

3.3 A Density Result over Finite Fields

In a similar vein as in section 2, we are going to work with the following sets: For a fixed $e_0 \in \mathbb{N}$, we define

$$\mathcal{P}_{e_0}^{\text{low}} = \bigcup_{d\geq 0}\{f \in S_{n,d} : H_f \textit{ is good at all } P \in \mathbb{P}^1_{\mathbb{F}_q}, \deg P < e_0\}$$
$$\mathcal{Q}_{e_0}^{\text{med}} = \bigcup_{d\geq 0}\{f \in S_{n,d} : H_f \textit{ is bad at some } P \in \mathbb{P}^1_{\mathbb{F}_q}, \deg P \in [e_0, \lfloor d/p \rfloor]\}$$
$$\mathcal{Q}^{\text{high}} = \bigcup_{d\geq 0}\{f \in S_{n,d} : H_f \textit{ is bad at some } P \in \mathbb{P}^1_{\mathbb{F}_q}, \deg P \in > d/p\}$$

3.3.1 Points of Low and Medium Degree

We first do some local analysis on a fiber. Let $P \in \mathbb{P}^1 = \text{Proj } \mathbb{F}_q[T_0, T_1]$ be a fixed point and let $e = \deg P$. Suppose $T_i \neq 0$ at P, so $P \in \text{Spec } \mathbb{F}_q[T_{1-i}/T_i] \subseteq \text{Proj } \mathbb{F}_q[T_0, T_1]$. Let $t = T_{1-i}/T_i$ and $r(t) \in \mathbb{F}_q[t]$ be an irreducible polynomial such that the second infinitesimal neighborhood $P^{(2)} = \text{Spec } \mathbb{F}_q[t]/r(t)^2$. Let $B := \mathbb{F}_q[t]$ and $\mathfrak{m} := (r(t)) \subseteq B$ be the maximal ideal. Denote the restriction map $B/\mathfrak{m}^2 \to B/\mathfrak{m}$ by $g \mapsto \overline{g}$ and extend it to a map $H^0(\mathbb{P}^2_{B/\mathfrak{m}^2}, \mathcal{O}(3)) \to H^0(\mathbb{P}^2_{B/\mathfrak{m}}, \mathcal{O}(3))$ by applying the reduction map to each coefficient. Similarly we denote a $\mathbb{F}_q$-linear section of the reduction map $B/\mathfrak{m}^2 \to B/\mathfrak{m}$ by $h \to \widetilde{h}$ and extend it to a map $H^0(\mathbb{P}^2_{B/\mathfrak{m}}, \mathcal{O}(3)) \to H^0(\mathbb{P}^2_{B/\mathfrak{m}^2}, \mathcal{O}(3))$. Let $\varphi_P : S_{3,d} \to H^0(\mathbb{P}^2_{B/\mathfrak{m}^2}, \mathcal{O}(3))$ be the restriction map. H_f is non-singular at a point $Q \in \pi^{-1}(P)$ if and only if $\varphi_P(f)$ does not vanish at $Q^{(2)} \in \mathbb{P}^2_{B/\mathfrak{m}^2}$.

Consider the vector space $H^0(\mathbb{P}^2_{\mathbb{F}_{q^e}}, \mathcal{O}(3))^2$, we say that a pair (F_1, F_2) is good if, it satisfies one the following conditions:

1. F_1 describes a non-singular curve in $\mathbb{P}^2_{\mathbb{F}_{q^e}}$.
2. F_1 describes a nodal curve but F_2 does not vanish at the node.

This terminology is explained by the following lemma, which is an analogous statement to Lemma 2.3.

Lemma 3.7. *The map*

$$\psi : H^0(\mathbb{P}^2_{B/\mathfrak{m}}, \mathcal{O}(3))^2 \to H^0(\mathbb{P}^2_{B/\mathfrak{m}^2}, \mathcal{O}(3))$$

defined by

$$(F_1, F_2) \mapsto \widetilde{F_1} + r(t)F_2$$

is an isomorphism of $B/\mathfrak{m}$-vector spaces. Moreover, f is good at P if and only if $\psi^{-1}(\varphi_P(f))$ in $H^0(\mathbb{P}^2_{B/\mathfrak{m}}, \mathcal{O}(3))^2$ is a good pair.

Proof. The above map has an inverse $F \mapsto (\overline{F}, (F - \widetilde{\overline{F}}))/r(t))$. For f to be good at P, we need $\overline{\varphi_P(f)}$ to describe a non-singular or nodal curve. Let $Q \in \mathbb{P}^2_{B/\mathfrak{m}^2}$ be a closed point and suppose $\varphi_P(f)$ corresponds to (F_1, F_2). If F_1 is non-singular at Q, then H_f must also be non-singular at Q. Otherwise, H_f is non-singular at Q if and only if F_2 does not vanish at Q. □

The following lemma assumes the same role as lemma 2.2 in Section 2, and the proof is similar.

Lemma 3.8. *If $\{P_1, P_2, \cdots, P_s\}$ is a set of finitely many closed points in $\mathbb{P}^1$, then for f randomly chosen from $\bigcup_d S_{3,d}$,*

$$\text{Prob}(f \text{ is good at all } P_i) = \prod_{i=1}^{s} \text{Prob}(f \text{ is good at } P_i)$$

In particular, we have

$$\text{Prob}(f \in \mathcal{P}^{\text{low}}_{e_0}) = \prod_{\deg(P) < e_0} \text{Prob}(f \text{ is good at } P)$$

since there are only finitely many points with degree $< e_0$.

Proof. Denote $\mathbb{P}^2 \times \mathbb{P}^1$ by X. Let $W := \coprod P_i^{(2)}$ and $\delta := \deg W = \sum_{i=1}^{s} 2\deg P_i$. Then we have an exact sequence

$$0 \to \mathcal{O}_X(3, d-\delta) \to \mathcal{O}_X(3,d) \to \mathcal{O}_X(3,d)|_{X_W} \to 0$$

which induces an exact sequence

$$H^0(X, \mathcal{O}_X(3,d)) \to H^0(X_W, \mathcal{O}_X(3,d)|_{X_W}) \to H^1(X, \mathcal{O}_X(3, d-\delta))$$

By Künneth formula,

$$H^1(X, \mathcal{O}_X(3, d-\delta)) \simeq \bigoplus_{i+j=1} H^i(\mathbb{P}^2, \mathcal{O}(3)) \otimes_{\mathbb{F}_q} H^j(\mathbb{P}^1, \mathcal{O}(d-\delta))$$

When $d - \delta \geq 0$, Serre Duality implies $H^1(\mathbb{P}^1, \mathcal{O}(d-\delta)) \simeq H^0(\mathbb{P}^1, \mathcal{O}(-2-(d-\delta))) = 0$. We also have $H^1(\mathbb{P}^2, \mathcal{O}(3)) = 0$. Therefore $H^1(X, \mathcal{O}_X(3, d-\delta)) = 0$ and the restriction map

$$S_{3,d} = H^0(\mathbb{P}^2 \times \mathbb{P}^1, \mathcal{O}(3,d)) \to H^0(X_W, \mathcal{O}_X(3,d)|_{X_W}) \cong \prod_{i=1}^{s} H^0(X_{P_i^{(2)}}, \mathcal{O}(3))$$

is surjective for $d \geq \sum_i 2\deg P_i$. This surjectivity, together with our observation that whether f is good at all $Q \in (H_f)_{P_i}$ is completely determined by $\varphi_{P_i}(f) \in H^0(\mathbb{P}^1_{P_i^{(2)}}, \mathcal{O}(3))$, implies that when $d \geq \delta$, we have

$$\frac{\#S_{3,d} \cap \mathcal{P}^{\text{low}}_{e_0}}{\#S_{3,d}} = \prod_{i=1}^{s} \frac{\#\varphi_{P_i}(\{f \in S_{3,d} : f \text{ is good at } P_i\})}{\#H^0(X_{P_i^{(2)}}, \mathcal{O}(3))}$$

The lemma follows by taking $d \to \infty$ on both sides. □

Lemma 3.9. *The fraction of good pairs in* $H^0(\mathbb{P}^2_{\mathbb{F}_{q^e}}, \mathcal{O}(3))^2$ *is*

$$(1+q^{-2e})(1-2q^{-2e}-q^{-4e}+q^{-5e}-2q^{-6e}-q^{-7e})$$

By the previous lemma, if $e = \deg P$*, then this fraction is precisely* $\mathrm{Prob}(f \in \mathcal{S}_P)$*, defined in Section 3.1.*

Proof. A randomly chosen $(F_1, F_2) \in H^0(\mathbb{P}^2_{\mathbb{F}_{q^e}}, \mathcal{O}(3))^2$ fails to be good if and only if one of the following four events happen:

1. F_1 describes a nodal curve, and F_2 vanishes at the node of F_1.
2. F_1 describes a cuspidal curve.
3. F_1 describes a reducible curve.
4. $F_1 \equiv 0$.

We denote the above events by E_1, E_2, E_3, E_4 respectively. To simplify notation, we denote q^e by a bold $\boldsymbol{q}$. Our results on the number of cubics of different types readily imply

$$\begin{aligned}\mathrm{Prob}(E_1) &= \mathrm{Prob}(F_1 \textit{ is a nodal curve})\mathrm{Prob}(F_2 \textit{ vanishes at the node of } F_1)\\ &= \frac{1}{\boldsymbol{q}^7}(\boldsymbol{q}^2+\boldsymbol{q}+1)(\boldsymbol{q}-1)^3(\boldsymbol{q}+1)\cdot\frac{1}{\boldsymbol{q}}\\ &= \frac{1}{\boldsymbol{q}^8}(\boldsymbol{q}^2+\boldsymbol{q}+1)(\boldsymbol{q}-1)^3(\boldsymbol{q}+1)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Prob}(E_2) &= \frac{1}{\boldsymbol{q}^7}(\boldsymbol{q}^2+\boldsymbol{q}+1)(\boldsymbol{q}-1)^2(\boldsymbol{q}+1)\\ \mathrm{Prob}(E_3) &= \frac{1}{\boldsymbol{q}^{10}}(\boldsymbol{q}^2+\boldsymbol{q}+1)(\boldsymbol{q}^6-1)\end{aligned}$$

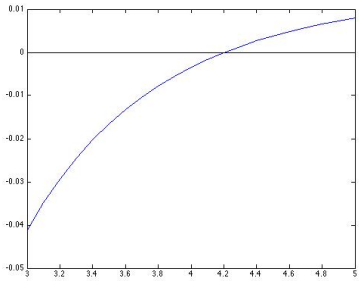
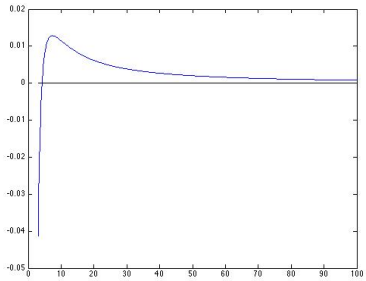
It is clear that $\mathrm{Prob}(E_4) = \boldsymbol{q}^{-10}$. The events E_j's are clearly disjoint, so the fraction of good pairs in the lemma is computed by

$$1-\sum_{j=1}^{4}\mathrm{Prob}(E_j)$$

□

Proof of Lemma 3.1. The first statement is simply Lemma 3.9. The second inequality in the second statement is obvious. For the first equality, we can numerically verify that

$$1-x^{-3/2} < 1-2x^{-2}-x^{-4}+x^{-5}-2x^{-6}-x^{-7}$$

(a) Graph on the domain $[3, 5]$ (b) Graph on the domain $[3, 100]$

holds when $x \geq 5$. Above are two plots of the function $(1-2x^{-2}-x^{-4}+x^{-5}-2x^{-6}-x^{-7})-(1-x^{-3/2})$:

However, we have assumed that $\operatorname{char} \mathbb{F}_q \geq 5$, so the inequality holds in our situation. □

3.3.2 Points of High Degree

We are going to bound the probability that a randomly chosen $f \in S_{3,d}$ is bad at some point P with high degree ($> \lfloor d/p \rfloor$). Therefore the following lemma is to be applied with $j = \lfloor d/p \rfloor$. The main idea used here has been explained in section 3.2.1.

Let $A_{3,d} = \mathbb{F}_q[x, y] \otimes_{\mathbb{F}_q} \mathbb{F}_q[t]$. For each $f \in A_{3,d}$ we define polynomials

$$T^2 f(U_0, U_1, x, y, t) = f_{xx} U_1^2 + 2 f_{xy} U_1 U_0 + f_{yy} U_0^2$$
$$T^3 f(U_0, U_1, x, y, t) = f_{xxx} U_1^3 + 3 f_{x^2y} U_1^2 U_0 + 3 f_{xy^2} U_1 U_0^2 + f_{y^3} U_0^3$$

Lemma 3.10. *Let U be an open subscheme of $\mathbb{P}^2 \times \mathbb{P}^1$ and $j > 2$ be an integer. The probability that for a randomly chosen $f \in S_{3,d}$ there exists a closed point $Q \in U$ that satisfies the following two conditions*

1. *$P := \pi(Q)$ has degree $> j$.*
2. *The fiber $(H_f)_P$ is a cuspidal or reducible cubic with a singularity at Q, or the hypersurface H_f has a singularity at Q.*

is bounded by

$$O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

Proof. It suffices to show the lemma for an affine chart $\mathbb{A}^2 \times \mathbb{A}^1$ since $\mathbb{P}^2 \times \mathbb{P}^1$ can be covered by six such charts. Without loss of generality, assume that $X_0, T_0 \neq 0$ on $U = \mathbb{A}^2 \times \mathbb{A}^1$ and let $x = X_1/X_0, y = X_2/X_0$ and $t = T_1/T_0$, such that $U = \operatorname{Spec} \mathbb{F}_q[x, y] \otimes_{\mathbb{F}_q} \mathbb{F}_q[t]$. Hence we may identify $S_{3,d}$ with $A_{3,d}$. Following the ideas presented in section 3.2.1, we only have to bound the

density of $f \in A_{3,d}$ such that there exists a closed point $Q \in \mathbb{A}^2 \times \mathbb{A}^1$ that satisfies the following three conditions

1. $P := \pi(Q)$ has degree $> j$.
2. $f(Q) = f_x(Q) = f_y(Q) = 0$
3. $T^2 f(U_0, U_1, Q)$ and $T^3 f(U_0, U_1, Q)$ have a common zero on $\operatorname{Proj} \mathbb{F}_q[U_0, U_1]$ (**Type I**), $T^2 f(U_0, U_1, Q)$ vanishes at a point on $\operatorname{Proj} \mathbb{F}_q[U_0, U_1]$ with multiplicity ≥ 2 (**Type II**), or $f_t(Q) = 0$ (**Type III**).

To bound the density of polynomials of Type I or Type II, we are naturally led to consider the scheme $\operatorname{Proj} \mathbb{F}_q[U_0, U_1] \times \mathbb{A}^2 \times \mathbb{A}^1$.

Type I: f is of Type I only if there exists a closed point Q' in the subscheme

$$W_0 := \{f = f_x = f_y = T^2 f = T^3 f = 0\} \subseteq \operatorname{Proj} \mathbb{F}_q[U_0, U_1] \times \mathbb{A}^2 \times \mathbb{A}^1$$

such that $\deg \pi(Q') \geq j$, where we still denote the projection to the last $\mathbb{A}^1$ component by π.

On the affine chart $U' = \operatorname{Spec} \mathbb{F}_q[u] \times \mathbb{A}^2 \times \mathbb{A}^1$ where $u = U_1/U_0$, we dehomogenize $T^2 f, T^3 f$ to:

$$\begin{aligned} T^2 f(u, x, y, t) &= f_{xx} u^2 + 2 f_{xy} u + f_{yy} \\ T^3 f(u, x, y, t) &= f_{xxx} u^3 + 3 f_{x^2 y} u^2 + 3 f_{xy^2} u + f_{yyy} \end{aligned}$$

We call a closed point $Q' \in \operatorname{Proj} \mathbb{F}_q[U_0, U_1] \times \mathbb{A}^2 \times \mathbb{A}^1$ *admissible* if $\deg \pi(Q) \geq j$ and a subscheme $V \subseteq \operatorname{Proj} \mathbb{F}_q[U_0, U_1] \times \mathbb{A}^2 \times \mathbb{A}^1$ *admissible* if it contains an admissible point. We denote the union of admissible irreducible components of $(V)_{\mathrm{red}}$ by V_{ad}, and the collection of its irreducible components by $\operatorname{Irr} V_{\mathrm{ad}}$.

Following Poonen's idea, we write f in a form so that the derivatives involved are largely independent. If $h \in A_{3,d}$, $g_i \in A_{0,\lfloor d/p \rfloor}$ for $0 \leq i \leq 4$ uniformly and independently at random, then the distribution of

$$f = h + g_4^p x^3 + g_3^p y^2 + g_2^p x + g_1^p y + g_0^p$$

is also uniform over $A_{3,d}$. Direct computation shows

$$\begin{aligned} T^3 f &= u^3 (h_{xxx} + 6 g_4^p) + 3 u^2 h_{x^2 y} + 3 u h_{xy^2} + h_{yyy} \\ T^2 f &= u^2 (h_{xx} + 6 x g_4^p) + 2 u h_{xy} + h_{yy} + 2 g_3^p \\ f_x &= h_x + 3 g_4^p x^2 + 2 g_3^p x + g_2^p \\ f_y &= h_y + g_1^p \end{aligned}$$

We define a sequence of subschemes $W_0 \subseteq \cdots \subseteq W_4 \subseteq U$ by

$$W_4 = \{T^3 f = 0\}, W_3 = W_4 \cap \{T^2 f = 0\}$$
$$W_2 = W_3 \cap \{f_x = 0\}, W_1 = W_2 \cap \{f_y = 0\}$$

As the reader may check, we deliberately set up the supscripts so that for each $k = 0, \cdots, 4$, W_k only depends on the choice of $h, g_k, \cdots, g_4$. Let E denote the event that

a. $\dim (W_1)_{\mathrm{ad}} = 0$

b. f does not vanish at any of $\mathrm{Irr}(W_1)_{\mathrm{ad}}$.

Clearly if E holds for f, then W_0 does not contain any admissible point. Therefore it suffices to show that for randomly chosen $h, g_1, \cdots, g_4$,

$$\mathrm{Prob}(E) = 1 - O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

Step 1: Conditioned on a choice of h, the probability that $\dim W_4 = 4$ is at most $q^{-(\lfloor d/p \rfloor + 1)}$.
Proof of Step 1: Indeed, $\dim W_4 = 4$ if only if $T^3 f$ vanish identically on U, which happens only when $T^3 f = 0$ as a polynomial in $\mathbb{F}_q[u, x, y, t]$, and in particular $h_{xxx} + 6g_4^p = 0$. For each h, there is at most one choice for g_4 such that $h_{xxx} + 6g_4^p = 0$ as polynomials, and hence the claim follows.

Step 2: For $k = 3, 2, 1$, conditioned on a choice of $h, g_k, \cdots, g_4$ for which $\dim W_{k+1} \leq k$, the probability that $\dim (W_k)_{\mathrm{ad}} \geq k$ is at most $O(d^{4-k} q^{-\min(\lfloor d/p \rfloor + 1, j)})$.
Proof of Step 2: We only show this for $k = 3$, since the proofs for $k = 2, 1$ are completely analogous. Let $V_1, \cdots, V_\ell$ be all the irreducible components of $(W_4)_{\mathrm{ad}}$, where $\ell = \#\{\mathrm{Irr}(W_4)_{\mathrm{ad}}\}$. By Bèzout's theorem, $\ell = O(d)$. We need to bound the set

$$G_i^{\mathrm{bad}} = \{g_3 \in A_{0, \lfloor d/p \rfloor} : T^2 f \textit{ vanishes identically on } V_i\}$$

If $g, g' \in G_i^{\mathrm{bad}}$, then $g - g'$ vanishes identically on V_i. Hence if $G_i^{\mathrm{bad}} \neq \emptyset$, it is a coset of the kernel of the linear map

$$\varphi_i : A_{0, \lfloor d/p \rfloor} \to H^0(V_i, \mathcal{O}_{V_i})$$

Now we apply Lemma 2.6 by identifying $U' = \mathbb{A}^1 \times \mathbb{A}^2 \times \mathbb{A}^1$ with $\mathbb{A}^3 \times \mathbb{A}^1$ to obtain that $\#\{\mathrm{Im}\, \varphi_i\} \geq q^{\min(\lfloor d/p \rfloor + 1, j)}$. Therefore the probability that a randomly chosen g_3 lies in G_i^{bad} is at most $q^{-\min(\lfloor d/p \rfloor + 1, j)}$. Since there are $O(d)$ such V_i's, the claim follows.

Step 3: Conditioned on choice $h, g_4, \cdots, g_1$ such that $\dim (W_1)_{\mathrm{ad}} = 0$, the probability that $(W_0)_{\mathrm{ad}} \neq \emptyset$ is at most $O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)})$.
Proof of Step 3: By Bézout's theorem again, we see that $\#\{W_0\} = O(d^4)$. For an admissible point $Q \in W_0$, the set H^{bad} of $g_0 \in A_{0,\lfloor d/p \rfloor}$ for which f vanishes at Q forms a coset of the kernel of the map $\varphi_Q : A_{0,\lfloor d/p \rfloor} \to H^0(Q, \mathcal{O}_Q)$. We apply Lemma 2.6 again with $W = Q$ to prove claim 3.
Finally *Step 1* and *2* together give that

$$\begin{aligned}\mathrm{Prob}(\dim (W_1)_{\mathrm{ad}}) = 0) &\geq (1 - q^{-(\lfloor d/p \rfloor + 1)}) \prod_{k=1}^{3} (1 - d^k q^{-\min(\lfloor d/p \rfloor + 1, j)}) \\ &= 1 - O(d^3 q^{-\min(\lfloor d/p \rfloor + 1, j)})\end{aligned}$$

and *Step 3* gives

$$\begin{aligned}\mathrm{Prob}(E) &\geq \mathrm{Prob}(\dim (W_1)_{\mathrm{ad}}) = 0)(1 - O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)}) \\ &= 1 - O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)})\end{aligned}$$

Type II: We can check whether f is of Type II locally. It suffices to bound the density of $f \in A_{3,d}$ such that there exists a closed point $Q' \in U'$ in the subscheme

$$W_0' = \{f = f_x = f_y = T^2 f = (T^2 f)_u = 0\} \subseteq U'$$

with $\deg \pi(Q') \geq j$. The rest of the arguments is rather analogous to what we did before, so we only give a sketch. We define

$$\begin{aligned}W_4' &= \{(T^2 f)_u = 0\}, W_3' = W_4' \cap \{T^2 f = 0\} \\ W_2' &= W_3' \cap \{f_x = 0\}, W_1' = W_2' \cap \{f_y = 0\}\end{aligned}$$

This time we choose $f \in A_{3,d}$ by choosing $h \in A_{3,d}$, $g_i \in A_{0,\lfloor d/p \rfloor}$ for $0 \leq i \leq 4$ uniformly and independently at random and putting

$$f = h + g_4^p xy + g_3^p y^2 + g_2^p x + g_1^p y + g_0^p$$

Direct computation shows

$$\begin{aligned}(T^2 f)_u &= 2u h_{xx} + 2(h_{xy} + g_4^p) \\ T^2 f &= u^2 h_{xx} + 2u(h_{xy} + g_4^p) + h_{yy} + g_3^p \\ f_x &= h_x + g_4^p y + g_2^p \\ f_y &= h_y + g_1^p\end{aligned}$$

By applying the same argument as in *Step 1* and *2* of the Type I case, we may show that

$$\mathrm{Prob}(\dim (W_1')_{\mathrm{ad}} = 0) = 1 - O(d^3 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

By applying the same arguments as in *Step 3*, we may bound the probability that f does not vanish at any of the irreducible components of $(W_2')_{\mathrm{ad}}$ conditioned on $\dim (W_2')_{\mathrm{ad}} = 0$, so that

$$\mathrm{Prob}((W_0')_{\mathrm{ad}} = \emptyset) \geq 1 - O(d^4 q^{-\min(\lfloor d/p \rfloor + 1, j)})$$

Type III: This is the easiest case to deal with. There is no need to involve U_i's. The proof is completely analogous to the second part of the proof of Lemma 2.7, where we treated the case in which the curve H_f has a singularity on $\mathbb{A}^1 \times \mathbb{A}^1$, except that we have $\mathbb{A}^2 \times \mathbb{A}^1$ instead of $\mathbb{A}^1 \times \mathbb{A}^1$ and one more variable in this case.

Now the proof of the lemma is complete. □

3.3.3 Proof of the Main Result

Lemma 3.11.

$$\lim_{e_0 \to \infty} \mathrm{Prob}(f \in \mathcal{Q}_{e_0}^{\mathrm{med}}) = 0$$

Proof. By definition,

$$\mathrm{Prob}(f \in \mathcal{Q}_{e_0}^{\mathrm{med}}) = \lim_{d \to \infty} \mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}})$$

for f_d randomly chosen from $S_{3,d}$. It suffices to show that $\mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}})$ is universally bounded by $O(q^{-e_0})$, where the implied constant is independent of d or e_0.

Let P be a point of degree $e \leq \lfloor d/p \rfloor$ on $\mathbb{P}^1$. By the proof of Lemma 3.8, the restriction map $S_{3,d} \to H^0(X_{P^{(2)}}, \mathcal{O}(3))$ is surjective since $p > 2$ and $e < \lfloor d/p \rfloor < d/2$. By Lemma 2.3 and Lemma 3.1, the probability that f_d is bad at P is $O(q^{-2e})$ as $e \to \infty$.

$$\begin{aligned}
\mathrm{Prob}(f_d \in \mathcal{Q}_{e_0}^{\mathrm{med}}) &\leq \sum_{e=e_0}^{\lfloor d/p \rfloor} (\text{number of points of degree } e \text{ in } \mathbb{P}^1)(2q^{-2e}) \\
&\leq 2 \sum_{e=e_0}^{\lfloor d/p \rfloor} (q^e + 1) q^{-2e} = O(\frac{q^{-e_0}}{1 - q^{-1}}) = O(q^{-e_0})
\end{aligned}$$

□

Lemma 3.12.

$$\mathrm{Prob}(f \in \mathcal{Q}^{\mathrm{high}}) = 0$$

Proof. Apply Lemma 3.10 with $j = \lfloor d/p \rfloor$ and $U = \mathbb{P}^2 \times \mathbb{P}^1$. Then let $d \to \infty$. □

For each e_0, we have

$$\mathcal{P}_{e_0}^{\text{low}} \subseteq \mathcal{S} \subseteq \mathcal{P}_{e_0}^{\text{low}} \cup \mathcal{Q}_{e_0}^{\text{med}} \cup \mathcal{Q}^{\text{high}}$$

As $e_0 \to \infty$, Lemma 3.8, 3.11 and 3.12 combine to give that

$$\text{Prob}(f \in \mathcal{S}) = \prod_{P \in \mathbb{P}^1_{\mathbb{F}_q}} \text{Prob}(f \in \mathcal{S}_P)$$

Finally we would like to make sure that this infinite product converges. Recall the following well known lemma:

Lemma 3.13. *Suppose that $p_e, e = 1, 2, \cdots$ satisfy $0 \leq p_e < 1$ and $\sum p_e < \infty$, then $\prod(1 - p_e) > 0$.*

By Lemma 3.1, the infinite product

$$\prod_{P \in \mathbb{P}^1_{\mathbb{F}_q}} \text{Prob}(f \in \mathcal{S}_P) = \prod_{e=1}^{\infty} \Big(\prod_{\deg P = e} \text{Prob}(f \in \mathcal{S}_P) \Big)$$

converges since

$$1 - \prod_{\deg P = e} \text{Prob}(f \in \mathcal{S}_P) \leq O(q^{-e})$$

References

[1] B. Poonen, *Sieve methods for varieties over finite fields and arithmetic schemes*, J. Thor. Nombres Bordeaux 19 (2007), 221229.

[2] B. Poonen, *An explicit algebraic family of genus-one curves violating the Hasse principle*, available at `http://www-math.mit.edu/~poonen/`,

[3] D. Erman and M.M. Wood, *Semiample Bertini theorems over finite fields*, Duke Mathematical Journal 164(2015), no. 1, 1-38

[4] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) 160 (2004), no. 3, 1099-1127.

[5] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[6] The Stacks Project Authors, *Stacks Project*, `http://stacks.math.columbia.edu`, 2016