Journal of Number Theory 130 (2010) 2528–2541

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Fluctuations in the number of points on smooth plane curves over finite fields

Alina Bucur [a,b], Chantal David [c,b], Brooke Feigon [d], Matilde Lalín [e,*]

[a] University of California at San Diego, United States
[b] Institute for Advanced Study, United States
[c] Concordia University, Canada
[d] University of Toronto, Canada
[e] University of Alberta, Canada

ARTICLE INFO

Article history:
Received 16 January 2010
Revised 10 May 2010
Available online xxxx
Communicated by J. Brian Conrey

Keywords:
Plane curves
Finite fields
Number of points

ABSTRACT

In this note, we study the fluctuations in the number of points on smooth projective plane curves over a finite field $\mathbb{F}_q$ as q is fixed and the genus varies. More precisely, we show that these fluctuations are predicted by a natural probabilistic model, in which the points of the projective plane impose independent conditions on the curve. The main tool we use is a geometric sieving process introduced by Poonen (2004) [8].

1. Introduction

Let S_d be the set of homogeneous polynomials $F(X,Y,Z)$ of degree d over $\mathbb{F}_q$, and let $S_d^{\mathrm{ns}} \subseteq S_d$ be the subset of polynomials corresponding to smooth (or nonsingular) curves C_F: $F(X,Y,Z)=0$. The genus of C_F is $(d-1)(d-2)/2$. By running over all polynomials $F \in S_d^{\mathrm{ns}}$, one would expect the average number of points of $C_F(\mathbb{F}_q)$ to be $q+1$. We show that this is true, and that the difference between $\#C_F(\mathbb{F}_q)$ and $q+1$ (properly normalized) tends to a standard Gaussian, $N(0,1)$, when q and d tend to infinity in a certain range. Our main tool is a sieving process due to Poonen [8] which allows us to count the number of polynomials in S_d which give rise to smooth curves C_F, and the number of smooth curves C_F which pass through a fixed set of points of $\mathbb{P}^2(\mathbb{F}_q)$. We denote by p the characteristic of $\mathbb{F}_q$.

* Corresponding author.
E-mail addresses: alina@math.ucsd.edu (A. Bucur), cdavid@mathstat.concordia.ca (C. David), bfeigon@math.toronto.edu (B. Feigon), mlalin@dms.umontreal.ca (M. Lalín).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.05.009

Theorem 1.1. *Let $X_1, \dots, X_{q^2+q+1}$ be q^2+q+1 i.i.d. random variables taking the value 1 with probability $(q+1)/(q^2+q+1)$ and the value 0 with probability $q^2/(q^2+q+1)$. Then, for $0 \leqslant t \leqslant q^2+q+1$,*

$$\frac{\#\{F \in S_d^{\mathrm{ns}}\colon \#C_F(\mathbb{F}_q) = t\}}{\#S_d^{\mathrm{ns}}} = \mathrm{Prob}(X_1 + \cdots + X_{q^2+q+1} = t) \times \Big(1 + O\big(q^t\big(d^{-1/3} + (d-1)^2 q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})} + dq^{-\lfloor \frac{d-1}{p} \rfloor - 1}\big)\big)\Big),$$

where $\lfloor \cdot \rfloor$ denotes the integer part.

We now explain why these random variables model the point count for smooth curves. Intuitively, if F is any polynomial in S_d, then the set of $\mathbb{F}_q$-points of the curve C_F is a subset of $\mathbb{P}^2(\mathbb{F}_q)$, which has q^2+q+1 elements. Heuristically, these points impose independent conditions on F.

Let us look at one of those conditions, say at the point $[0:0:1]$. Put $f(x,y) = F(X,Y,1)$ the dehomogenization of F and write

$$f(x,y) = a_{0,0} + a_{1,0}x + a_{0,1}y + \cdots.$$

Since we insist that C_F is smooth, we cannot have $(a_{0,0}, a_{1,0}, a_{0,1}) = (0,0,0)$, so there are q^3-1 possibilities for this triplet. Of these triplets, the ones that correspond to the case where $[0:0:1]$ is on the curve C_F are those where $a_{0,0} = 0$, of which there are q^2-1. So the probability that $[0:0:1]$ lies on C_F is

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

The argument works the same for any point in the plane, and in particular the expected number of points in $C_F(\mathbb{F}_q)$ is $q+1$. This explains the random variables of Theorem 1.1. Namely, the probability that $X = 1$ (respectively $X = 0$) is the probability that a point $P \in \mathbb{P}^2(\mathbb{F}_q)$ belongs (respectively does not belong) to a smooth curve $F(X,Y,Z) = 0$.

Remark 1.2. One could take the iterated limit $\lim_{q\to\infty}\lim_{d\to\infty}$ in Theorem 1.1. Or we could invert the order and take the $\lim_{d\to\infty}\lim_{q\to\infty}$ provided that d goes to infinity in such a way that $d > q^{3(q^2+q+1)+\varepsilon}$. By studying the moments we can substantially weaken this condition and compute the double limit $\lim_{d,q\to\infty}$ in a larger range. It would be ideal to be able to take the double limit with no conditions on d and q, but at present our error terms are not good enough for that.

The average value of each of the random variables X_i is $(q+1)/(q^2+q+1)$, and the standard deviation is $q\sqrt{q+1}/(q^2+q+1)$. Thus, we have a triangular array of random variables (each row indexed by q), with q^2+q+1 variables in each row that satisfies the Lyapunov condition. It then follows from the Triangular Central Limit Theorem [1] that

$$\frac{(X_1 + \cdots + X_{q^2+q+1}) - (q+1)}{\sqrt{q+1}} \to N(0,1)$$

as q tends to infinity.

We can show that this also holds for $\#C_F(\mathbb{F}_q)$ for $F \in S_d^{\mathrm{ns}}$, as q and d tend to infinity with $d > q^{1+\varepsilon}$, by showing that, under these conditions, the integral moments of

$$\frac{\#C_F(\mathbb{F}_q)-(q+1)}{\sqrt{q+1}}$$

converge to the integral moments of $\frac{(X_1+\cdots+X_{q^2+q+1})-(q+1)}{\sqrt{q+1}}$.

Theorem 1.3. *Let k be a positive integer, and let*

$$M_k(q,d)=\frac{1}{\#S_d^{\mathrm{ns}}}\sum_{F\in S_d^{\mathrm{ns}}}\left(\frac{\#C_F(\mathbb{F}_q)-(q+1)}{\sqrt{q+1}}\right)^k.$$

Then,

$$M_k(q,d)=\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\left(\sum_{i=1}^{q^2+q+1}X_i-(q+1)\right)\right)^k\right)\times\left(1+O\left(q^{\min(k,q^2+q+1)}\left(q^{-k}d^{-1/3}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{2})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right)\right)\right).$$

Corollary 1.4. *When q and d tend to infinity and $d>q^{1+\varepsilon}$, the limiting distribution of*

$$\frac{\#C_F(\mathbb{F}_q)-(q+1)}{\sqrt{q+1}}$$

is a standard Gaussian distribution (mean 0, variance 1).

Remark 1.5. The conclusion of Corollary 1.4 holds whenever, for a fixed k, the error term in Theorem 1.3 approaches 0 as both q and d grow. This happens when $d>q^{1+\varepsilon}$, which is the condition in the corollary. But it also holds, for example, when the characteristic of the finite field is bounded. In particular, it holds for a tower of fields $\mathbb{F}_{p^n}$, with p fixed, as $n,d\to\infty$.

Finally, we remark that Theorem 1.1 implies that the average number of points on a smooth plane curve is $q+1$, but this is not true anymore if one looks at all plane curves. Our heuristic above shows that for a random polynomial $F\in S_d$ the probability that a point $P\in\mathbb{P}^2(\mathbb{F}_q)$ actually lies on C_F is $1/q$. This can also be proven easily (see Section 2.1 for the proof); we record the result here.

Proposition 1.6. *Let $Y_1,\dots,Y_{q^2+q+1}$ be i.i.d. random variables taking the value 1 with probability $1/q$ and the value 0 with probability $(q-1)/q$. Then, for $d\geqslant q^2+q$,*

$$\frac{\#\{F\in S_d\colon \#C_F(\mathbb{F}_q)=t\}}{\#S_d}=\mathrm{Prob}(Y_1+\cdots+Y_{q^2+q+1}=t).$$

Proposition 1.6 is an exact result (without an error term) as there is no sieving involved. For smooth curves, one has to sieve over primes of arbitrarily large degree, since a smooth curve is required not to have any singular points over $\overline{\mathbb{F}}_q$, not only over $\mathbb{F}_q$. This introduces the error term. In particular, the average number of points on a plane curve $F(X,Y,Z)=0$ without any smoothness condition is $q+1+\frac{1}{q}$.

Some related work. Brock and Granville [2] calculated the average number of points in families of curves of given genus g over finite fields,

$$N_r(g,q) = \sum_{C/\mathbb{F}_q,\ \mathrm{genus}(C)=g} \frac{N_r(C)}{|\mathrm{Aut}(C/\mathbb{F}_q)|} \Big/ \sum_{C/\mathbb{F}_q,\ \mathrm{genus}(C)=g} \frac{1}{|\mathrm{Aut}(C/\mathbb{F}_q)|}$$

where $N_r(C)$ denotes the number of $\mathbb{F}_{q^r}$-rational points of C. It turns out that, depending on the value of r, $N_r(g,q)$ shows very different behavior as $q \to \infty$. Indeed, $N_r(g,q) = q^r + o(q^{r/2})$ unless r is even and $r \leqslant 2g$, in which case $N_r(g,q) = q^r + q^{r/2} + o(q^{r/2})$. This "excess" phenomenon has a natural explanation in terms of Deligne's equidistribution theorem for Frobenius conjugacy classes of the ℓ-adic sheaf naturally attached to this family, as pointed out by Katz [5]. Using Deligne's theorem, Katz showed that as $q \to \infty$, $N_r(g,q)$ can be expressed in terms of the integral $I_r(G) = \int_G \mathrm{tr}(A^r)\,dA$, where G ($= \mathrm{USp}(2g)$ in this case) is a compact form of the geometric monodromy group of that sheaf; the occurrence of the excess phenomenon depends on the values of $I_r(G)$, which are computed using the representation theory of G. This approach, which is described in a more general form in [6], has the advantage of being applicable to other situations in which the geometric monodromy group has been identified, for instance, when calculating the average number of points in the family of smooth degree d hypersurfaces in $\mathbb{P}^n$ over finite fields. In particular, for $n = 2$, one obtains the average number of points of smooth plane curves of degree d, which are the subject of the present investigation, but from a different point of view.

Namely, while both [2,5] are concerned with curves of fixed genus as the number of points in the base field varies, we consider the complementary situation of working over a fixed field and allowing the genus to vary. We also consider the question of the double limit as both the genus and the number of points in the base field grow. Similar questions were investigated in [7] for hyperelliptic curves, and in [3,4,9] for cyclic trigonal curves and general cyclic p-covers.

2. Poonen's sieve

We will adapt the results from Section 2 of [8] to our case, which is simpler as we take $n = 2$ and $X = \mathbb{P}^2 \subset \mathbb{P}^2$. But, unlike Poonen, we need to keep track of the error terms.

First let us do this in general in his setup, namely take $Z \subset X$ a finite subscheme. Then $U = \mathbb{P}^2 \setminus Z$ will automatically be smooth and of dimension 2. We will need to choose Z and a subset $T \subset H^0(Z, \mathcal{O}_Z)$ in a way that imposes the appropriate local conditions for our curves at finitely many points.

The strategy is to check the smoothness separately at points of low, medium, and high degree, and then combine the conditions at the end. The main term will come from imposing conditions on the values taken by both a random polynomial $F \in S_d$ and its first order derivatives at the points in U of relatively small degree (for d large enough). The error term will come from smoothness conditions at primes P of medium and large degree (compared to d).

Following Poonen, denote $A = \mathbb{F}_q[x_1, x_2]$ and $A_{\leqslant d}$ the set of polynomials in A of degree at most d. Denote by $U_{<r}$ the closed points of U of degree $< r$ and by $U_{>r}$ the closed points of U of degree $> r$. Set

$$\mathcal{P}_{d,r} = \{F \in S_d\colon\ C_F \cap U \text{ is smooth of dimension 1 at all } P \in U_{<r},\ F|_Z \in T\},$$

$$\mathcal{Q}_{d,r} = \{F \in S_d\colon\ \exists P \in U \text{ s.t. } r \leqslant \deg P \leqslant d/3,\ C_F \cap U \text{ is not smooth of dimension 1 at } P\},$$

$$\mathcal{Q}_d^{high} = \{F \in S_d\colon\ \exists P \in U_{>d/3} \text{ s.t. } C_F \cap U \text{ is not smooth of dimension 1 at } P\}.$$

2.1. Points of low degree

All the results of this section depend on the following lemma proven in [8] using classical results from algebraic geometry.

Lemma 2.1. *For any subscheme $Y \subset \mathbb{P}^2$, the map $\phi_d\colon\ S_d = H^0(\mathbb{P}^2, \mathcal{O}_{\mathbb{P}^2}(d)) \to H^0(Y, \mathcal{O}_Y(d))$ is surjective for $d \geqslant \dim H^0(Y, \mathcal{O}_Y) - 1$.*

Proof. Take $n = 2$ in Lemma 2.1 in [8]. □

Lemma 2.2. *Let $U_{<r} = \{P_1, \dots, P_s\}$. Then for $d \geqslant 3rs + \dim H^0(Z, \mathcal{O}_Z) - 1$, we have*

$$\frac{\#\mathcal{P}_{d,r}}{\#S_d} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} \prod_{i=1}^{s} \bigl(1 - q^{-3\deg P_i}\bigr).$$

Proof. The result follows from Lemma 2.2 in [8], as long as we ensure that $d+1$ is bigger than the dimension of $H^0(Z, \mathcal{O}_Z) \times \prod_{i=1}^{s} H^0(Y_i, \mathcal{O}_{Y_i})$, where Y_i is the closed subscheme corresponding to P_i in the manner described by Poonen. Namely, if $\mathfrak{m}_i$ denotes the ideal sheaf of P_i on U, then Y_i is the subscheme of U corresponding to the ideal sheaf $\mathfrak{m}_i^2 \subseteq \mathcal{O}_U$. Thus $\dim H^0(Y_i, \mathcal{O}_{Y_i}) = 3\deg P_i < 3r$. □

Proof of Proposition 1.6. We can use this last result to compute the average number of points on the curves C_F associated to the polynomials $F \in S_d$ without any smoothness condition. We pick $P_1, \dots, P_{q^2+q+1}$ an enumeration of the points of $\mathbb{P}^2(\mathbb{F}_q)$, and we take Z to be an $\mathfrak{m}_P$-neighborhood for each point $P \in \mathbb{P}^2(\mathbb{F}_q)$ (this means that we look at the value of F at that point; for smoothness, we will also look at the value of its first order derivatives). Thus

$$H^0(Z, \mathcal{O}_Z) = \prod_{P \in \mathbb{P}^2(\mathbb{F}_q)} \mathcal{O}_P/\mathfrak{m}_P. \tag{1}$$

Each space has dimension 1, so we can identify

$$H^0(Z, \mathcal{O}_Z) \cong \bigoplus_{i=1}^{q^2+q+1} \mathbb{F}_q. \tag{2}$$

Therefore, $\dim H^0(Z, \mathcal{O}_Z) = q^2 + q + 1$ and $\#H^0(Z, \mathcal{O}_Z) = q^{q^2+q+1}$. Let $0 \leqslant t \leqslant q^2 + q + 1$. We want to count all curves C_F such that $P_1, \dots, P_t \in C_F(\mathbb{F}_q)$ and $P_{t+1}, \dots, P_{q^2+q+1} \notin C_F(\mathbb{F}_q)$. We then choose, via the identification (2),

$$T \cong \bigl\{(a_i)_{1 \leqslant i \leqslant q^2+q+1} \colon a_1, \dots, a_t = 0,\ a_{t+1}, \dots, a_{q^2+q+1} \in \mathbb{F}_q^{\times}\bigr\},$$

and $\#T = (q-1)^{q^2+q+1-t}$. It follows by taking $r = 0$ in Lemma 2.2 that, when $d \geqslant q^2 + q$,

$$\begin{aligned} &\frac{\#\{F \in S_d \colon P_1, \dots, P_t \in C_F(\mathbb{F}_q),\ P_{t+1}, \dots, P_{q^2+q+1} \notin C_F(\mathbb{F}_q)\}}{\#S_d} \\ &= \frac{\#\mathcal{P}_{d,0}}{\#S_d} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} = \frac{(q-1)^{q^2+q+1-t}}{q^{q^2+q+1}} = \left(\frac{1}{q}\right)^t \left(\frac{q-1}{q}\right)^{q^2+q+1-t}. \end{aligned}$$

Then, summing over all possible choices of t points,

$$\begin{aligned} \operatorname{Prob}\bigl(\#C_F(\mathbb{F}_q) = t\bigr) &= \sum_{\substack{\varepsilon_1, \dots, \varepsilon_{q^2+q+1} \in \{0,1\} \\ \varepsilon_1 + \cdots + \varepsilon_{q^2+q+1} = t}} \left(\frac{1}{q}\right)^t \left(\frac{q-1}{q}\right)^{q^2+q+1-t} \\ &= \operatorname{Prob}(Y_1 + \cdots + Y_{q^2+q+1} = t), \end{aligned}$$

and this proves Proposition 1.6. □

Now we want to use Lemma 2.2 to sieve out nonsmooth curves. We remark that Lemma 2.2 gives an exact formula without error term, but we need to choose r as a function of d and the product will contribute to the error term. In addition, s itself depends on r.

As the number of closed points of degree e in U is bounded by the number of closed points of degree e in $\mathbb{P}^2$, which is $q^{2e}+q^e+1<2q^{2e}$, the product

$$\prod_{P \text{ closed point of } U} \left(1-q^{-z\deg P}\right)^{-1} = \zeta_U(z)$$

converges for $\Re(z)>2$. For the same reason, we get that

$$\prod_{i=1}^{s}\left(1-q^{-3\deg P_i}\right) = \zeta_U(3)^{-1}\left(1+O\left(\frac{q^{-r}}{1-q^{-1}-2q^{-r}}\right)\right). \tag{3}$$

Indeed, in order to show (3), we write

$$\prod_{i=1}^{s}\left(1-q^{-3\deg P_i}\right) = \zeta_U(3)^{-1}\prod_{\deg P\geqslant r}\left(1-q^{-3\deg P}\right)^{-1}.$$

For any sequence of numbers $\{x_i\colon\ 0\leqslant x_i<1\}$, we know that

$$1\leqslant\prod_{i=1}^{\infty}(1-x_i)^{-1}\leqslant\frac{1}{1-\sum x_i}.$$

Taking the sequence in question to be $\{q^{-3\deg P}\}_{\deg P\geqslant r}$, it means that we need an upper bound for

$$\sum_{\deg P\geqslant r} q^{-3\deg P} = \sum_{j=r}^{\infty} q^{-3j}\#\{\text{closed points of } U \text{ of degree } j\}.$$

All the P's until now have been closed points of U, but U is a subset of $\mathbb{P}^2$, so it has at most $\#\mathbb{P}^2(\mathbb{F}_{q^j})=q^{2j}+q^j+1\leqslant 2q^{2j}$ closed points of degree j. Hence

$$\sum_{\deg P\geqslant r} q^{-3\deg P}\leqslant 2\sum_{j=r}^{\infty}q^{-j}=\frac{2q^{-r}}{1-q^{-1}},$$

and now we get

$$1\leqslant\prod_{\deg P\geqslant r}\left(1-q^{-3\deg P}\right)^{-1}\leqslant\frac{1}{1-\frac{2q^{-r}}{1-q^{-1}}},$$

which proves (3). Substituting (3) in Lemma 2.2, we obtain

$$\frac{\#\mathcal{P}_{d,r}}{\#S_d} = \zeta_U(3)^{-1}\frac{\#T}{\#H^0(Z,\mathcal{O}_Z)}\left(1+O\left(\frac{q^{-r}}{1-q^{-1}-2q^{-r}}\right)\right). \tag{4}$$

2.2. Points of medium degree

Lemma 2.3. *For a closed point $P \in U$ of degree $e \leqslant d/3$, we have*

$$\frac{\#\{F \in S_d\colon C_F \cap U \text{ is not smooth of dimension 1 at } P\}}{\#S_d} = q^{-3e}.$$

Proof. Take $m = 2$ in Lemma 2.3 of [8]. This also follows from Lemma 2.2 by taking $r = 0$ and Z to be an $\mathfrak{m}_P^2$-neighborhood of P (which means that we look at F and its first order derivatives). Then,

$$H^0(Z, \mathcal{O}_Z) = \mathcal{O}_P/\mathfrak{m}_P^2,$$

and $\dim H^0(Z, \mathcal{O}_Z) = q^{3\deg P}$. We also choose $T = \{(0,0,0)\}$, as we want F and its first order derivatives to vanish at P. Then,

$$\frac{\#\{F \in S_d\colon C_F \cap U \text{ is not smooth of dimension 1 at } P\}}{\#S_d} = \frac{\#T}{\#H^0(Z, \mathcal{O}_Z)} = q^{-3\deg P}. \qquad \square$$

Lemma 2.4.

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leqslant 2\frac{q^{-r}}{1-q^{-1}}.$$

Proof. We follow the proof of Lemma 2.4 of [8]. We have that

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leqslant \sum_{\substack{P \in U \\ \deg P = r}}^{d/3} \frac{\#\{F \in S_d\colon C_F \cap U \text{ is not smooth of dimension 1 at } P\}}{\#S_d},$$

and $\#U(\mathbb{F}_{q^e}) \leqslant \#\mathbb{P}^2(\mathbb{F}_{q^e}) = q^{2e} + q^e + 1 \leqslant 2q^{2e}$. Then, using Lemma 2.3, we have

$$\frac{\#\mathcal{Q}_{d,r}}{\#S_d} \leqslant 2\sum_{e=r}^{d/3} q^{-e} \leqslant 2\sum_{e=r}^{\infty} q^{-e} = 2\frac{q^{-r}}{1-q^{-1}}. \qquad \square$$

2.3. Points of high degree

Lemma 2.5. *For $P \in \mathbb{A}^2(\mathbb{F}_q)$ of degree e, we have*

$$\frac{\#\{f \in A_{\leqslant d}\colon f(P) = 0\}}{\#A_{\leqslant d}} \leqslant q^{-\min(d+1,e)}.$$

Proof. Take $n = 2$ in Lemma 2.5 of [8]. $\square$

Lemma 2.6.

$$\frac{\#\mathcal{Q}_d^{high}}{\#S_d} \leqslant 3(d-1)^2 q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})} + 3dq^{-\lfloor \frac{d-1}{p} \rfloor - 1}.$$

Proof. If we get a bound for all affine $U \subset \mathbb{A}^2$, the same bound multiplied by 3 will hold for any $U \subset \mathbb{P}^2$, since it can be covered by three affine charts. So we can reduce the problem to affine sets. We follow the proof of Lemma 2.6 of [8], while keeping track of the constants appearing in the error terms, which is not done in [8] as only the main term is needed for his application. In our case the coordinates are simply x_1 and x_2, which have degree 1 and $D_i = \frac{\partial}{\partial x_i}$, $i = 1, 2$ are already global derivations. This allows us to work globally on the set U and there is no need to work locally as in [8]. Now we can work with dehomogenizations of polynomials in S_d, so we need to find the polynomials $f \in A_{\leqslant d}$ for which $C_f \cap U$ fails to be smooth at some $P \in U$. This happens if and only if $f(P) = (D_1 f)(P) = (D_2 f)(P) = 0$.

Poonen's "trick" is based on the observation that any polynomial $f \in A_{\leqslant d}$ can be written as

$$f = g_0 + g_1^p x_1 + g_2^p x_2 + h^p$$

with $g_0 \in A_{\leqslant d}$, $g_1, g_2 \in A_{\leqslant \gamma}$ and $h \in A_{\leqslant \eta}$, where $\gamma = \lfloor \frac{d-1}{p} \rfloor$ and $\eta = \lfloor \frac{d}{p} \rfloor$. This representation is *not* unique, but selecting f uniformly at random amounts to selecting g_0, g_1, g_2 and h independently and uniformly at random. The advantage of this decomposition is that $D_i f = D_i g_0 + g_i^p$, so each derivative depends only on g_0 and one of the g_1, g_2. We will select f_0, g_0, g_1 and h in this order and estimate the probability of making a bad choice at each step. Set

$$W_0 = U, \qquad W_1 = U \cap \{D_1 f = 0\}, \qquad W_2 = U \cap \{D_1 f = D_2 f = 0\}.$$

Claim 1. *For $i = 0, 1$ and for each choice of $g_0, \dots, g_i$, such that* $\dim W_i \leqslant 2 - i$,

$$\frac{\#\{(g_{i+1}, \dots, g_2, h)\colon \dim W_{i+1} > 1 - i\}}{\#\{(g_{i+1}, \dots, g_2, h)\}} \leqslant (d-1)^i q^{-\lfloor \frac{d-1}{p} \rfloor - 1}.$$

Bézout's theorem tells us that the number of $(2-i)$-dimensional components of $(W_i)_{\mathbf{red}}$ is bounded above by $(d-1)^i$, since $\deg D_i f \leqslant d-1$, for each i, and $\deg \overline{U} = 1$. Pick a component V. It has dimension at least 1 and it is a subscheme of $\mathbb{A}^2$, therefore the projection in one of the coordinates, say x_1, will be a 1-dimensional subscheme of $\mathbb{A}^1$. Therefore no nonzero polynomial in $\mathbb{F}_q[x_1]$ can vanish on V, since that would mean that it vanishes on $\mathbb{A}^1$.

The set of choices of g_{i+1} for which $W_{i+1} \supset V$ is a coset of the subspace of functions in $A_{\leqslant \gamma}$ that vanish on V. By the previous paragraph, this subspace is complementary to the space of polynomials in x_1 of degree at most γ. Hence its codimension is at least $\gamma + 1$, and the claim follows.

Claim 2. *For any choice of g_0, g_1, g_2 such that* $\dim W_2 = 0$,

$$\frac{\#\{h\colon C_f \cap W_2 \cap U_{>d/3}\}}{\#\{\text{all } h\}} \leqslant (d-1)^2 q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})}.$$

This follows from the fact that $\#W_2 \leqslant (d-1)^2$ (from Bézout's theorem as before).

For a given $P \in W_2$, the set of bad h's at P (i.e. the set of $h \in A_{\leqslant \eta}$ for which C_f passes through P) is either empty or a coset of $\ker(\mathrm{ev}_P : A_{\leqslant \eta} \to \kappa(P))$, where $\kappa(P)$ is the residue field at P. Since $\deg P > d/3$, it follows from Lemma 2.5 that the set of bad h's has density at most $q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})}$ in the set of all h, and the claim follows.

To finish the proof of the lemma, we put the two claims together and we get that

$$\frac{\#\mathcal{Q}_d^{high}}{\#S_d} \leqslant 3(d-1)^2 q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})} + 3d q^{-\lfloor \frac{d-1}{p} \rfloor - 1}. \qquad \square$$

Combining the points of small, medium, and high degree, we get that, for any Z a finite subscheme of $\mathbb{P}^2$, $U = \mathbb{P}^2 \setminus Z$ and any $T \subset H^0(Z, \mathcal{O}_Z)$,

$$\begin{aligned}&\{F \in S_d\colon C_F \cap U \text{ is smooth of dimension 1 and } F|_Z \in T\}\\ &\quad= \frac{\#T}{\zeta_U(3)\#H^0(Z,\mathcal{O}_Z)}\left(1 + O\left(\frac{q^{-r}}{1-q^{-1}-2q^{-r}}\right)\right)\\ &\qquad+ O\left(\frac{q^{-r}}{1-q^{-1}} + (d-1)^2 q^{-\min(\lfloor \frac{d}{p}\rfloor+1, \frac{d}{3})} + dq^{-\lfloor \frac{d-1}{p}\rfloor - 1}\right).\end{aligned} \tag{5}$$

We need to choose an appropriate value for r. According to Lemma 2.2, we must have $d \geqslant 3rs + \dim H^0(Z,\mathcal{O}_Z) - 1$ and $\frac{1}{r-1}(q^{2r-2} + q^{r-1} + 1) \leqslant s < q^{2r} + q^r + 1$. When using Eq. (5) in Sections 3 and 4, we will always have $Z \subset \mathbb{P}^2(\mathbb{F}_q)$, thus $\dim H^0(Z,\mathcal{O}_Z) < 6q^2$. Fix $B \geqslant 0$ which will be chosen later. We take

$$r = \frac{3B + \log_q d}{3}. \tag{6}$$

The error term of (5) coming from points of medium and high degree is therefore

$$O\left(\frac{q^{-B}d^{-1/3}}{1-q^{-1}} + (d-1)^2 q^{-\min(\lfloor \frac{d}{p}\rfloor+1, \frac{d}{3})} + dq^{-\lfloor \frac{d-1}{p}\rfloor - 1}\right). \tag{7}$$

3. Number of points

We apply the results in Section 2 twice. The first time to evaluate the fraction of homogeneous polynomials of degree d that define smooth plane curves, and the second time to evaluate the fraction of homogeneous polynomials of degree d that define smooth plane curves with predetermined $\mathbb{F}_q$-points. By taking the quotient we then obtain an asymptotic formula for the fraction of smooth plane curves that have predetermined $\mathbb{F}_q$-points.

For the first evaluation, we take $B = 0$ in (6), $Z = \emptyset$ and $T = \{0\}$ in Eq. (5) to get

$$\begin{aligned}\frac{\#\{F \in S_d^{\mathrm{ns}}\}}{\#S_d} &= \zeta_{\mathbb{P}^2}(3)^{-1}\left(1 + O\left(\frac{d^{-1/3}}{1-q^{-1}-2d^{-1/3}}\right)\right)\\ &\quad+ O\left(\frac{d^{-1/3}}{1-q^{-1}} + (d-1)^2 q^{-\min(\lfloor \frac{d}{p}\rfloor+1, \frac{d}{3})} + dq^{-\lfloor \frac{d-1}{p}\rfloor - 1}\right).\end{aligned} \tag{8}$$

Pick $P_1, \ldots, P_{q^2+q+1}$ an enumeration of the points of $\mathbb{P}^2(\mathbb{F}_q)$, and let $0 \leqslant t \leqslant q^2 + q + 1$. We want to compute

$$\frac{\#\{F \in S_d^{\mathrm{ns}}\colon P_1, \ldots, P_t \in C_F(\mathbb{F}_q),\ P_{t+1}, \ldots, P_{q^2+q+1} \notin C_F(\mathbb{F}_q)\}}{\#S_d}.$$

This is achieved by taking Z to be an $\mathfrak{m}_P^2$-neighborhood for each point $P \in \mathbb{P}^2(\mathbb{F}_q)$ (this means that we look at the value of F and its first order derivatives at each point). Thus

$$H^0(Z,\mathcal{O}_Z) = \prod_{P \in \mathbb{P}^2(\mathbb{F}_q)} \mathcal{O}_P/\mathfrak{m}_P^2. \tag{9}$$

Each space has dimension 3, so we can identify

$$H^0(Z,\mathcal{O}_Z)\cong\bigoplus_{i=1}^{q^2+q+1}\mathbb{F}_q^3, \tag{10}$$

and $\dim H^0(Z,\mathcal{O}_Z)=3(q^2+q+1)$, while $\#H^0(Z,\mathcal{O}_Z)=q^{3(q^2+q+1)}$.

Then we want T to be, via the identification (10), the set of $((a_i,b_i,c_i))_{1\leqslant i\leqslant q^2+q+1}$ such that $a_1,\dots,a_t=0$, $a_{t+1},\dots,a_{q^2+q+1}\in\mathbb{F}_q^\times$, and $(a_i,b_i,c_i)\neq(0,0,0)$ for $1\leqslant i\leqslant q^2+q+1$. This implies that

$$\#T=\left(q^2-1\right)^t(q-1)^{q^2+q+1-t}q^{2(q^2+q+1-t)}.$$

Using (5) with this choice of Z and T, we obtain

$$\begin{aligned}
&\frac{\#\{F\in S_d^{\mathrm{ns}}\colon P_1,\dots,P_t\in C_F(\mathbb{F}_q),\ P_{t+1},\dots,P_{q^2+q+1}\notin C_F(\mathbb{F}_q)\}}{\#S_d}\\
&\quad=\zeta_U(3)^{-1}\frac{(q^2-1)^t(q-1)^{q^2+q+1-t}q^{2(q^2+q+1-t)}}{q^{3(q^2+q+1)}}\left(1+O\left(\frac{d^{-1/3}}{1-q^{-1}-2d^{-1/3}}\right)\right)\\
&\qquad+O\left(\frac{d^{-1/3}}{1-q^{-1}}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right).
\end{aligned}\tag{11}$$

Here, by multiplicativity of zeta functions,

$$\frac{\zeta_{\mathbb{P}^2}(z)}{\zeta_U(z)}=\zeta_Z(z)=\left(\frac{1}{1-q^{-z}}\right)^{q^2+q+1}\quad\text{for } U=\mathbb{P}^2\setminus Z.$$

Then, by taking the quotient of (11) and (8), we get that

$$\begin{aligned}
&\frac{\#\{F\in S_d^{\mathrm{ns}}\colon P_1,\dots,P_t\in C_F(\mathbb{F}_q),\ P_{t+1},\dots,P_{q^2+q+1}\notin C_F(\mathbb{F}_q)\}}{\#S_d^{\mathrm{ns}}}\\
&\quad=\left(\frac{q^3}{q^3-1}\right)^{q^2+q+1}\frac{(q^2-1)^t(q-1)^{q^2+q+1-t}q^{2(q^2+q+1-t)}}{q^{3(q^2+q+1)}}\\
&\qquad\times\left(1+O\left(q^t\left(d^{-1/3}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right)\right)\right)\\
&\quad=\left(\frac{q+1}{q^2+q+1}\right)^t\left(\frac{q^2}{q^2+q+1}\right)^{q^2+q+1-t}\\
&\qquad\times\left(1+O\left(q^t\left(d^{-1/3}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right)\right)\right).
\end{aligned}$$

Theorem 1.1 follows by noting that for any $\varepsilon_1,\dots,\varepsilon_{q^2+q+1}\in\{0,1\}$ with $\varepsilon_1+\cdots+\varepsilon_{q^2+q+1}=t$,

$$\mathrm{Prob}(X_1=\varepsilon_1,\dots,X_{q^2+q+1}=\varepsilon_{q^2+q+1})=\left(\frac{q+1}{q^2+q+1}\right)^t\left(\frac{q^2}{(q^2+q+1)}\right)^{q^2+q+1-t}.$$

4. Moments

By Theorem 1.1 the number of points of smooth plane curves over $\mathbb{F}_q$ is distributed as $X_1 + \cdots + X_{q^2+q+1}$, and the trace of the Frobenius as $X_1 + \cdots + X_{q^2+q+1} - (q+1)$. (The mean of $X_1 + \cdots + X_{q^2+q+1}$ is $q+1$.) Applying the triangular central limit theorem to the random variables $X_1, \ldots, X_{q^2+q+1}$, we have that $(X_1 + \cdots + X_{q^2+q+1} - (q+1))/\sqrt{q+1}$ is distributed as $N(0,1)$ when $q \to \infty$.

We would like to say the same thing about the distribution of the trace of Frobenius in our family when d and q go to infinity, which amounts to the computation of the moments.

We will first compute

$$N_k(q,d) = \frac{1}{\#S_d^{\mathrm{ns}}} \sum_{F \in S_d^{\mathrm{ns}}} \left(\frac{\#C_F(\mathbb{F}_q)}{\sqrt{q+1}} \right)^k,$$

and then deduce the result for $M_k(q,d)$.

We can write

$$N_k(q,d) = \frac{1}{\#S_d^{\mathrm{ns}}} \left(\frac{1}{\sqrt{q+1}} \right)^k \sum_{F \in S_d^{\mathrm{ns}}} \left(\sum_{P \in \mathbb{P}^2(\mathbb{F}_q)} S\big(F(P)\big) \right)^k,$$

where the function

$$S(a) = \begin{cases} 1, & a = 0, \\ 0, & a \neq 0 \end{cases}$$

allows us to count the number of points in the curve. Thus, expanding the k-th power,

$$\begin{aligned} N_k(q,d) &= \frac{1}{\#S_d^{\mathrm{ns}}} \left(\frac{1}{\sqrt{q+1}} \right)^k \sum_{P_1, \ldots, P_k \in \mathbb{P}^2(\mathbb{F}_q)} \sum_{F \in S_d^{\mathrm{ns}}} S\big(F(P_1)\big) \ldots S\big(F(P_k)\big) \\ &= \frac{1}{\#S_d^{\mathrm{ns}}} \frac{1}{(q+1)^{k/2}} \sum_{\ell=1}^{\min(k, q^2+q+1)} h(\ell,k) \sum_{(\mathbf{P},\mathbf{b}) \in P_{\ell,k}} \sum_{F \in S_d^{\mathrm{ns}}} S\big(F(P_1)\big)^{b_1} \ldots S\big(F(P_\ell)\big)^{b_\ell}, \end{aligned}$$

where

$$\begin{aligned} P_{\ell,k} = \big\{ (\mathbf{P}, \mathbf{b}) \colon\ & \mathbf{P} = (P_1, \ldots, P_\ell) \text{ with } P_i \text{ distinct points of } \mathbb{P}^2(\mathbb{F}_q), \\ & \mathbf{b} = (b_1, \ldots, b_\ell) \text{ with } b_i \text{ positive integers such that } b_1 + \cdots + b_\ell = k \big\}. \end{aligned}$$

Notice that the coefficients $h(\ell,k)$ satisfy

$$\sum_{\ell=1}^{k} h(\ell,k) \sum_{(\mathbf{P},\mathbf{b}) \in P_{\ell,k}} 1 = \big(q^2+q+1\big)^k.$$

Now let us fix $(\mathbf{P}, \mathbf{b}) \in P_{\ell,k}$. Then,

$$\frac{1}{\#S_d^{\mathrm{ns}}} \sum_{F \in S_d^{\mathrm{ns}}} S\big(F(P_1)\big)^{b_1} \dots S\big(F(P_\ell)\big)^{b_\ell} = \sum_{a_1,\dots,a_\ell \in \mathbb{F}_q} \frac{1}{\#S_d^{\mathrm{ns}}} \sum_{\substack{F \in S_d^{\mathrm{ns}} \\ F(P_j)=a_j}} \prod_{j=1}^{\ell} S(a_j)^{b_j}.$$

Since the b_j's are positive integers, they have no influence on the result and we obtain nonzero terms only when $a_j = 0$ for $1 \leqslant j \leqslant \ell$, and in this case

$$\frac{1}{\#S_d^{\mathrm{ns}}} \sum_{F \in S_d^{\mathrm{ns}}} S\big(F(P_1)\big)^{b_1} \dots S\big(F(P_\ell)\big)^{b_\ell} = \frac{\#\{F \in S_d^{\mathrm{ns}}\colon\ F(P_i) = 0 \text{ for } 1 \leqslant i \leqslant \ell\}}{\#S_d^{\mathrm{ns}}}. \tag{12}$$

The quotient above can be computed in a similar way as in Section 3. We choose $B = k$ in (6), Z as in (9) and T to be, via the identification (10), the set of $((a_i, b_i, c_i))_{1 \leqslant i \leqslant q^2+q+1}$ such that $a_1 = \dots = a_\ell = 0$, $a_{\ell+1}, \dots, a_{q^2+q+1} \in \mathbb{F}_q$ and $(a_i, b_i, c_i) \neq (0,0,0)$ for $1 \leqslant i \leqslant q^2+q+1$. Then,

$$\#T = \big(q^2-1\big)^{\ell} \big(q^3-1\big)^{q^2+q+1-\ell},$$

and

$$\begin{aligned}&\frac{\#\{F \in S_d^{\mathrm{ns}}\colon\ F(P_i) = 0 \text{ for } 1 \leqslant i \leqslant \ell\}}{\#S_d^{\mathrm{ns}}} \\ &= \left(\frac{q+1}{q^2+q+1}\right)^{\ell} \big(1 + O\big(q^{-k} d^{-1/3} q^{\ell} + (d-1)^2 q^{\ell - \min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})} + d q^{\ell - \lfloor \frac{d-1}{p} \rfloor - 1}\big)\big).\end{aligned}$$

Now we sum over all the elements in $P_{\ell,k}$:

$$\begin{aligned}N_k(q,d) = \frac{1}{(q+1)^{k/2}} \sum_{\ell=1}^{\min(k, q^2+q+1)} h(\ell,k) \sum_{(\mathbf{P},\mathbf{b}) \in P_{\ell,k}} \left(\frac{q+1}{q^2+q+1}\right)^{\ell} \\ \times \big(1 + O\big(q^{\min(k, q^2+q+1)} \big(q^{-k} d^{-1/3} + (d-1)^2 q^{-\min(\lfloor \frac{d}{p} \rfloor + 1, \frac{d}{3})} + d q^{-\lfloor \frac{d-1}{p} \rfloor - 1}\big)\big)\big).\end{aligned}$$

On the other hand, we have

$$\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}} \sum_{i=1}^{q^2+q+1} X_i\right)^k\right) = \left(\frac{1}{\sqrt{q+1}}\right)^k \sum_{\ell=1}^{k} h(\ell,k) \sum_{(\mathbf{i},\mathbf{b}) \in A_{\ell,k}} \mathbb{E}\big(X_{i_1}^{b_1} \dots X_{i_\ell}^{b_\ell}\big),$$

where

$$\begin{aligned}A_{\ell,k} = \big\{&(\mathbf{i}, \mathbf{b})\colon\ \mathbf{i} = (i_1, \dots, i_\ell),\ 1 \leqslant i_j \leqslant q^2+q+1 \text{ distinct}, \\ &\mathbf{b} = (b_1, \dots, b_\ell) \text{ with } b_i \text{ positive integers such that } b_1 + \dots + b_\ell = k\big\}.\end{aligned}$$

Since

$$\mathbb{E}\big(X_1^{b_1}\dots X_\ell^{b_\ell}\big)=\left(\frac{q+1}{q^2+q+1}\right)^{\ell}$$

and $\#P_{\ell,k}=\#A_{\ell,k}$, we conclude that

$$N_k(q,d)=\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q^2+q+1}X_i\right)^k\right) \tag{13}$$

$$\times\left(1+O\left(q^{\min(k,q^2+q+1)}\left(q^{-k}d^{-1/3}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right)\right)\right). \tag{14}$$

Now using (13) and the binomial theorem, we get that

$$\begin{aligned}M_k(q,d)&=\sum_{j=0}^{k}\binom{k}{j}N_j(q,d)(-\sqrt{q+1}\,)^{k-j}\\&\sim\sum_{j=0}^{k}\binom{k}{j}\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\sum_{i=1}^{q^2+q+1}X_i\right)^j\right)(-\sqrt{q+1})^{k-j}\\&=\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\left(\sum_{i=1}^{q^2+q+1}X_i-(q+1)\right)\right)^k\right)\end{aligned}$$

with the same error term as (14). This completes the proof of Theorem 1.3.

Acknowledgments

The authors wish to thank Pierre Deligne and Zeév Rudnick for suggesting the problem that we consider in this paper. The authors are grateful to both of them as well as Pär Kurlberg for helpful discussions. Finally, the authors would like to thank the referee for carefully examining the paper and providing several suggestions that have improved the clarity of exposition.

This work was supported by the Natural Sciences and Engineering Research Council of Canada [B.F., Discovery Grant 155635-2008 to C.D., 355412-2008 to M.L.] and the National Science Foundation of U.S. [DMS-0652529 and DMS-0635607 to A.B.]. M.L. is also supported by a Faculty of Science Startup grant from the University of Alberta, and C.D. is also supported by a grant to the Institute for Advanced Study from the Minerva Research Foundation.

References

[1] P. Billingsley, Probability and Measure, third ed., Wiley Ser. Probab. Math. Stat., John Wiley & Sons, Inc., New York, 1995, xiv+593 pp.
[2] B.W. Brock, A. Granville, More points than expected on curves over finite field extensions, Finite Fields Appl. 7 (1) (2001) 70–91.
[3] A. Bucur, C. David, B. Feigon, M. Lalín, Statistics for traces of cyclic trigonal curves over finite fields, Int. Math. Res. Not. (2010) 932–967.
[4] A. Bucur, C. David, B. Feigon, M. Lalín, Biased statistics for traces of cyclic p-fold covers over finite fields, in: Proceedings of Women in Numbers, Fields Institute Communications, in press.
[5] N.M. Katz, Frobenius–Schur indicator and the ubiquity of Brock–Granville quadratic excess, Finite Fields Appl. 7 (1) (2001) 45–69.

[6] N.M. Katz, P. Sarnak, Random Matrices, Frobenius Eigenvalues, and Monodromy, Amer. Math. Soc. Colloq. Publ., vol. 45, Amer. Math. Soc., Providence, RI, 1999, xii+419 pp.
[7] P. Kurlberg, Z. Rudnick, The fluctuations in the number of points on a hyperelliptic curve over a finite field, J. Number Theory 129 (3) (2009) 580–587.
[8] B. Poonen, Bertini theorems over finite fields, Ann. of Math. (2) 160 (3) (2004) 1099–1127.
[9] M. Xiong, The fluctuation in the number of points on a family of curves over a finite field, preprint, 2009.