MOST PLANE CURVES OVER FINITE FIELDS ARE NOT BLOCKING

SHAMIL ASGARLI, DRAGOS GHIOCA, AND CHI HOI YIP

ABSTRACT. A plane curve $C \subset \mathbb{P}^2$ of degree d is called *blocking* if every $\mathbb{F}_q$-line in the plane meets C at some $\mathbb{F}_q$-point. We prove that the proportion of blocking curves is $o(1)$ when $d \geq 2q - 1$ and $q \to \infty$. We also show that the same conclusion holds for smooth curves under the somewhat weaker condition $d \geq 3p$ and $d, q \to \infty$. Moreover, the two events in which a random plane curve is smooth and is blocking, respectively, are shown to be asymptotically independent. Extending a classical result on the number of $\mathbb{F}_q$-roots of random polynomials, we find that the limiting distribution of the number of $\mathbb{F}_q$-points in the intersection of a random plane curve and a fixed $\mathbb{F}_q$-line is Poisson with mean 1. We also present an explicit formula for the proportion of blocking curves involving statistics on the number of $\mathbb{F}_q$-points contained in a union of k lines for $k = 1, 2, \ldots, q^2 + q + 1$.

1. INTRODUCTION

We start with the definition of the main combinatorial structure in this paper. As usual, p denotes a prime, q denotes a power of p, and $\mathbb{F}_q$ denotes the finite field with q elements. A set of points $B \subseteq \mathbb{P}^2(\mathbb{F}_q)$ is a *blocking set* if every $\mathbb{F}_q$-line meets B. The simplest example of a blocking set is a union of $q + 1$ distinct $\mathbb{F}_q$-points on a line. A blocking set B is *trivial* if it contains all the $q + 1$ points of a line, and is *nontrivial* if it is not a trivial blocking set.

Given a projective plane curve $C \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$, we say that C is a *blocking curve* if $C(\mathbb{F}_q)$ is a blocking set. Moreover, C is *nontrivially blocking* if $C(\mathbb{F}_q)$ is a nontrivial blocking set. A systematic study of blocking curves was carried out in our previous paper [AGY22]. In particular, we showed that an irreducible plane curve is not blocking whenever its degree is small compared to q [AGY22, Theorem 1.2]. We also constructed a few families of geometrically irreducible or smooth nontrivially blocking curves. Our motivation for studying blocking curves stems from the interesting interplay between finite geometry and algebraic geometry developed in recent years; see the surveys [Sző97b, SS98] for more instances. We refer to [AGY22] for more motivation to study smooth blocking curves, including potential applications in algebraic geometry.

The goal of the present paper is to study blocking curves through the lens of arithmetic statistics. We prove several precise results in this direction. In particular, we show that the property of being blocking is rare whenever the degree is large compared to q.

Theorem 1.1. *There exists a function $\psi(x)$ with $\lim\limits_{x \to \infty} \psi(x) = 0$ such that the following holds. Let $\mathbb{F}_q$ be a fixed finite field, and $d \geq 2q - 1$. Among all plane curves of degree d defined over $\mathbb{F}_q$, the fraction of blocking curves is at most $\psi(q)$. In particular, most plane curves are not blocking.*

We have a similar result for smooth plane curves where the condition on the degree d depends on the characteristic p of the field $\mathbb{F}_q$.

Theorem 1.2. *Almost all smooth plane curves of degree d over $\mathbb{F}_q$ are not blocking when $d, q \to \infty$ satisfying $d \geq \min\{2q, 3p\}$.*

Note that Theorem 1.2 is somewhat weaker than Theorem 1.1 when q is a prime number. However, when q is a proper prime power (that is, of the form p^n with $n \geq 2$), Theorem 1.2 provides a more refined result. For instance, we can deduce that the proportion of blocking curves of degree $d = \lfloor p \log q \rfloor$ over $\mathbb{F}_q$ tends to 0 as $q \to \infty$.

Given a plane curve C defined over $\mathbb{F}_q$, we say that a line L is *skew* to C if $L \cap C$ has no $\mathbb{F}_q$-points. Using this language, a plane curve C is not blocking if and only if C admits a skew $\mathbb{F}_q$-line. Not only we show that most curves are *not* blocking, but we also expect that a plane curve of degree $d \geq q$ has many skew lines. More precisely, we prove the following effective result.

Theorem 1.3. *Let $C \subset \mathbb{P}^2$ be a plane curve of degree d defined over $\mathbb{F}_q$ satisfying $d \geq q$. Then the expected number of skew $\mathbb{F}_q$-lines for C is*

$$\frac{q^2}{e} - \frac{q}{2e} - \frac{5}{24e} + O\left(\frac{1}{q}\right).$$

In other words, we expect roughly 36.7879% of all lines defined over $\mathbb{F}_q$ to be skew to C.

More generally, Poisson distribution can be used to predict the number of skew lines to a random plane curve; see Section 3.2. As we will explain later in Remark 3.7, there is also a connection between Theorem 1.3 and Entin's work on the Chebotarev density theorem [Ent21].

Let S_d be the set of homogeneous polynomials $F(X, Y, Z)$ of degree d over $\mathbb{F}_q$ including $0 \in S_d$ in order to make S_d into a vector space, and let $S_d^{\mathrm{ns}} \subseteq S_d$ be the subset of polynomials corresponding to smooth (**ns** stands for non-singular) curves $C_F : F(X, Y, Z) = 0$. Define

$$\mathrm{nb}(q) = \lim_{d \to \infty} \frac{\#\{F \in S_d : C_F \text{ is not blocking}\}}{\#S_d}.$$

We find an explicit lower and upper bound for $\mathrm{nb}(q)$.

Theorem 1.4. *Given a finite field $\mathbb{F}_q$, define*

$$\lambda_q(x) = x\left(1 - (1 - x^q)^{q+1}\right) + x \sum_{j=1}^{q} (1 - x)^j \left(1 - (1 - x^q)^q\right).$$

We have

$$\lambda_q\left(1 - \frac{1}{q}\right) \leq \mathrm{nb}(q) \leq 1 - \lambda_q\left(\frac{1}{q}\right).$$

In fact, the conclusion of Theorem 1.4 holds even if $\mathrm{nb}(q)$ is replaced with the density of non-blocking curves of fixed degree d as long as $d \geq 2q - 1$; see Proposition 4.3.

Note that the sequence $\lambda_q\left(1 - \frac{1}{q}\right)$ is increasing in q. Thus, Theorem 1.4 implies

$$\mathrm{nb}(q) \geq \lambda_q\left(1 - \frac{1}{11}\right) > 0.994$$

for each $q \geq 11$. We conclude that a random plane curve of large degree over $\mathbb{F}_q$ does *not* give rise to a blocking set with probability at least 0.99, provided that $q \geq 11$.

2

Similarly, we can define the analogous constant for smooth curves:

$$\mathrm{nb}^{\mathrm{ns}}(q) = \lim_{d \to \infty} \frac{\#\{F \in S_d^{\mathrm{ns}} : C_F \text{ is not blocking}\}}{\#S_d^{\mathrm{ns}}}.$$

Note that Theorem 1.1 and Theorem 1.2 provide effective estimates on the above two densities. In particular, we have $\lim_{q \to \infty} \mathrm{nb}(q) = 1$ and $\lim_{q \to \infty} \mathrm{nb}^{\mathrm{ns}}(q) = 1$, that is, almost all curves are not blocking, and the statement remains true when we restrict to smooth curves. It follows immediately that $\lim_{q \to \infty} \frac{\mathrm{nb}^{\mathrm{ns}}(q)}{\mathrm{nb}(q)} = 1$. However, it is not clear whether the following limit

$$\lim_{q \to \infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)}$$

exists and has any meaningful value. We will show that the limit above also approaches 1.

Theorem 1.5. *We have*

$$\lim_{q \to \infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} = 1.$$

In particular, the events of being smooth and being blocking are asymptotically independent.

It is necessary to take the limit as $q \to \infty$ in the previous theorem. Indeed, as we will see in Theorem 6.1, the value of the fraction $\frac{1-\mathrm{nb}^{\mathrm{ns}}(q)}{1-\mathrm{nb}(q)}$ is strictly less than 1 when q is large.

Related work. Our broad focus is elucidating the interaction between arithmetic statistics and finite geometry. We briefly mention a few recent related works in this area. Let C be a geometrically irreducible plane curve over $\mathbb{F}_q$ with degree d. Fix an integer $0 \le k \le d$. Makhul, Schicho, and Gallet [MSG20] studied the probability for a random line in $\mathbb{P}^2(\mathbb{F}_{q^N})$ to intersect C with exactly k points, as $N \to \infty$. Yet another research avenue is arithmetic statistics of plane curves satisfying (or not satisfying) Bertini's theorem. Recently, Asgarli and Freidin [AF21] computed upper and lower bounds for the density of plane curves over $\mathbb{F}_q$ which admit no transverse line over $\mathbb{F}_q$. One can also study probabilistic questions about random algebraic varieties over p-adic fields; see [AL20] and [KL21] for recent papers on this topic.

Outline of the paper. In Section 2 we review relevant background material from finite geometry and algebraic geometry. We also develop some of the key ingredients necessary for the later sections. Section 3 highlights a linear independence argument, namely Proposition 3.1, with application to the distribution of point counts and skew lines to plane curves. In Section 4, we prove our main Theorem 1.1. This is achieved by proving Theorem 1.4 which gives lower and upper bounds on $\mathrm{nb}(q)$. We apply the existing machinery to deduce Theorem 1.3. In Section 5, we focus on smooth curves and prove Theorem 1.2, and in Section 6, we prove Theorem 1.5. Finally, Section 7 is devoted to finding the exact natural density of blocking plane curves over $\mathbb{F}_q$ when $q = 2, 3, 4$.

2. Preliminaries

2.1. **Collection of known results on blocking sets.** Understanding the possible sizes of blocking sets is an important problem in finite geometry. This topic has been studied extensively, and the following theorem summarizes some of the best known lower bounds on the size of a nontrivial blocking set. Recall that if q is a square, a *Baer subplane* in $\mathbb{P}^2(\mathbb{F}_q)$ is a subplane with size $q + \sqrt{q} + 1$. It is known that a Baer subplane is a blocking set. As a result, the lower bound $q + \sqrt{q} + 1$ on B is achieved by Baer subplanes, and in fact only by Baer subplanes [Bru70, Bru71]. Moreover, the lower bound can be improved significantly if B avoids any Baer subplane [BSS99].

Theorem 2.1. *Let $q = p^r$. Let $c_2 = c_3 = 2^{-1/3}$ and $c_p = 1$ for $p > 3$. Let B be a non-trivial blocking set in $\mathbb{P}^2(\mathbb{F}_q)$. Then the following lower bounds on $|B|$ hold:*

- *(Bruen [Bru70, Bru71]) $|B| \geq q + \sqrt{q} + 1$. Moreover, the equality holds if and only if q is a square and B is a Baer subplane.*
- *(Blokhuis [Blo94]) If $r = 1$ and $p > 2$, then $|B| \geq 3(q + 1)/2$, where the lower bound is sharp by considering a projective triangle.*
- *(Szőnyi [Sző97a, Theorem 5.7]) If $p > 2$, $r = 2$, and B does not contain a Baer subplane, then $|B| \geq 3(q+1)/2$, where the lower bound is sharp by considering a projective triangle.*
- *(Blokhuis, Storme, and Szőnyi [BSS99, Theorem 1.1]) If r is odd, then $|B| \geq q+1+c_p q^{2/3}$.*
- *(Blokhuis, Storme, and Szőnyi [BSS99, Theorem 1.1]) If r is even, $q > 16$ and B does not contain a Baer subplane. Then $|B| \geq q + 1 + c_p q^{2/3}$.*

In Section 5, we will use the exponent $2/3$ in [BSS99, Theorem 1.1] in a crucial way.

2.2. Statistics on the number of rational points of smooth curves.

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 curves $C_F : F(X, Y, Z) = 0$. The celebrated Hasse-Weil bound asserts that

$$q + 1 - (d - 1)(d - 2)\sqrt{q} \leq \#C_F(\mathbb{F}_q) \leq q + 1 + (d - 1)(d - 2)\sqrt{q}$$

for each $F \in S_d^{\mathrm{ns}}$. Note that the Hasse-Weil bound already eliminates the possibility of a low degree curve being blocking in view of Theorem 2.1; we refer to [AGY22, Section 3] for stronger statements. However, in this paper, we mainly work on the case when the degree is large, and so relying on Hasse-Weil bound alone is not sufficient.

From a probabilistic point of view, one anticipates that the expectation of $\#C_F(\mathbb{F}_q)$ is $q + 1$ and the variance of $\#C_F(\mathbb{F}_q)$ is small. Note that Hasse-Weil bound gives the window for the possibility on the number of $\mathbb{F}_q$-points where $q + 1$ is the center of the interval. It is reasonable to expect that half of the curves should lie on one side of the interval. Note that this heuristic immediately implies that at least half of smooth curves are not nontrivially blocking in view of Theorem 2.1. Bucur, David, Feigon, and Lalín [BDFL10] proved a much stronger statement: when the degree d is sufficiently large compared to q, the number of rational points tends to the standard normal distribution up to some normalization.

Let $X_1, \ldots, X_{q^2+q+1}$ be $q^2 + q + 1$ independent and identically distributed (henceforth shortened to i.i.d.) random variables taking the value 1 with probability $(q + 1)/(q^2 + q + 1)$ and the value 0 with probability $q^2/(q^2 + q + 1)$. The key ingredient in their proof is the following random model: $\#C_F(\mathbb{F}_q) \approx X_1 + X_2 + \cdots + X_{q^2+q+1}$. In other words, the random model predicts that a random smooth curve will pass through each particular point with probability $(q + 1)/(q^2 + q + 1)$, and all such events are independent. By estimating the corresponding moments, they showed that the random model above portrays the truth with a high level of accuracy.

Theorem 2.2 ([BDFL10, Theorem 1.3]). *Let k be a positive integer, and let*

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

4

Then,

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

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

The next corollary will be useful in the proof of Theorem 1.2.

Corollary 2.3. *When q and d tend to infinity with $d \geq 3p$, we have $M_2(q,d) = o(q^{1/3})$.*

Proof. Since X_i's are i.i.d. random variables, it is straightforward to compute that,

$$\mathbb{E}\left(\left(\frac{1}{\sqrt{q+1}}\left(\sum_{i=1}^{q^2+q+1} X_i - (q+1)\right)\right)^2\right) = 1 + o(1)$$

as $q \to \infty$. Thus, in view of Theorem 2.2, it suffices to show that

$$(d-1)^2 q^{\frac{5}{3}-\min\left(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3}\right)} + dq^{\frac{5}{3}-\lfloor\frac{d-1}{p}\rfloor-1} = o(1) \tag{1}$$

when $q, d \to \infty$ and $d \geq 3p$.

When $p \leq 5000$ and $q \to \infty$, we have $q/p \to \infty$; thus, under the assumption that $d \to \infty$,

$$(d-1)^2 q^{\frac{5}{3}-\min\left(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3}\right)} + dq^{\frac{5}{3}-\lfloor\frac{d-1}{p}\rfloor-1} = o(1).$$

Next we assume $p > 5000$ so that $\min\left(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3}\right) = \lfloor\frac{d}{p}\rfloor+1 \geq 4$ when $d \geq 3p$. Note that

$$\log_q d \leq \frac{\log d}{\log p} = 1 + \frac{\log d/p}{\log p} \leq 1 + \frac{\log d/p}{\log 5000}.$$

When $x \geq 4$, it can be checked that,

$$(\lfloor x \rfloor + 1) - \frac{11}{3} - 2 \cdot \frac{\log x}{\log 5000} \geq x - \frac{11}{3} - 2 \cdot \frac{\log x}{\log 5000} > 0.007.$$

When $3 \leq x < 4$, we have $\lfloor x \rfloor + 1 = 4$ and again,

$$(\lfloor x \rfloor + 1) - \frac{11}{3} - 2 \cdot \frac{\log x}{\log 5000} = \frac{1}{3} - 2 \cdot \frac{\log x}{\log 5000} > 0.007.$$

Thus, it follows that

$$\frac{5}{3} + 2\log_q d - \left(\lfloor\frac{d}{p}\rfloor+1\right) \leq \frac{11}{3} + 2 \cdot \frac{\log d/p}{\log 5000} - \left(\lfloor\frac{d}{p}\rfloor+1\right) < -0.007$$

provided that $d \geq 3p$, which implies that

$$d^2 q^{\frac{5}{3}-\left(\lfloor\frac{d}{p}\rfloor+1\right)} = q^{2\log_q d+\frac{5}{3}-\left(\lfloor\frac{d}{p}\rfloor+1\right)} \leq q^{-0.007} = o(1)$$

when $q \to \infty$. Similarly, when $x \geq 3$, it is easy to verify that

$$x - \frac{8}{3} - \frac{\log x}{\log 5000} > 0.2.$$

It follows that

$$dq^{\frac{5}{3}-d/p} = q^{\log_q d+\frac{5}{3}-d/p} < q^{-0.2} = o(1).$$

5

Combining the ingredients above, we obtain

$$(d-1)^2 q^{\frac{5}{3}-\min\left(\lfloor \frac{d}{p}\rfloor+1,\frac{d}{3}\right)} + dq^{\frac{5}{3}-\lfloor \frac{d-1}{p}\rfloor-1} \le d^2 q^{\frac{5}{3}-\left(\lfloor \frac{d}{p}\rfloor+1\right)} + dq^{\frac{5}{3}-d/p} = o(1)$$

and the conclusion follows. □

Remark 2.4. By adapting the proof of the above corollary, we can show that if q and d tend to infinity such that $d/p \to \infty$, then as C_F runs over smooth plane curves with degree d over $\mathbb{F}_q$, the limiting distribution of

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

is the standard normal distribution (which is a stronger version of [BDFL10, Corollary 1.4] whose hypothesis $d > q^{1+\epsilon}$ is more stringent). Under this stronger assumption, we can show that for each fixed positive integer k, the error term in Theorem 2.2 is $o(1)$. The desired conclusion then follows from the triangular central limit theorem and the method of moments from probability theory; we refer to [Bil95, Theorem 27.3] and [BDFL10, Remark 1.5] for related discussions.

3. LINEAR INDEPENDENCE, POINT-COUNTING, AND SKEW LINES

The purpose of this section is to apply a linear independence argument in the parameter space of plane curves to obtain results about point-counting and skew lines. The key Proposition 3.1 will be used again in later sections.

3.1. **Linear independence.** In algebraic geometry, we are often interested in understanding the space of degree d hypersurfaces passing through a specified set of points with prescribed multiplicities. Broadly speaking, this is known as the *interpolation problem*. The main difficulty is that when there are too many points relative to the degree d, vanishing at several points may no longer yield independent conditions. However, when the degree d is large, the following proposition guarantees that different points indeed impose linearly independent conditions on the parameter space. While the result is known to the experts (see [Poo04, Lemma 2.1] where the argument is written in a cohomological language), our proof is self-contained and does not need advanced tools.

Proposition 3.1. *Fix a finite field $\mathbb{F}_q$, and consider any k distinct $\mathbb{F}_q$-points $P_1, P_2, \ldots, P_k$ in $\mathbb{P}^2$. If $d \ge \min\{k-1, 2q-1\}$, then passing through $P_1, P_2, \ldots, P_k$ impose linearly independent conditions in the vector space of degree d plane curves.*

Proof. Let V denote the vector space of all plane curves of degree d. Note that $\mathbb{F}_q$-points of V exactly correspond to plane curves of degree d defined over $\mathbb{F}_q$. It is known that $\dim(V) = N = \binom{d+2}{2}$. For each $1 \le i \le k$, let

$$W_i = \{\text{plane curves of degree } d \text{ passing through } P_1, P_2, \ldots, P_i\}.$$

Our goal is to show that W_k has the expected dimension as an $\mathbb{F}_q$-vector space, namely $\dim(W_k) = \dim(V) - k$. It is clear that $W_i \supseteq W_{i+1}$ for each $1 \le i \le k-1$. In particular, we have:

$$\dim(W_1) \ge \dim(W_2) \ge \dim(W_3) \ge \cdots \ge \dim(W_k).$$

Moreover, passing through one additional point imposes *at most* one linear condition, so we have either $\dim(W_{i+1}) = \dim(W_i) - 1$ or $\dim(W_{i+1}) = \dim(W_i)$ for each i. Since $\dim(W_1) = \dim(V) - 1$, we must have $\dim(W_k) \ge \dim(V) - k$.

6

In order to show that $\dim(W_k) = \dim(V) - k$, it therefore suffices to show that the dimension drops by 1 at each step, that is, we want to show that $\dim(W_{i+1}) = \dim(W_i) - 1$ holds for each $1 \le i \le k - 1$. To prove this, it suffices to find an element $f \in W_i$ such that $f \notin W_{i+1}$.

We proceed to show that for $d \ge \min\{k-1, 2q-1\}$, we can find a plane curve $C = \{f = 0\}$ of degree d defined over $\mathbb{F}_q$ such that $f \in W_i$ but $f \notin W_{i+1}$, that is, f passes through $P_1, P_2, \dots, P_i$ but does *not* pass through P_{i+1}.

First assume that $d \ge k - 1$. For each $j \in \{1, 2, \dots, i\}$, let L_j be an $\mathbb{F}_q$-line which passes through P_j but not P_{i+1}. Then for any $d \ge k - 1$, we can consider the reducible curve C consisting of the lines L_j (for $j = 1, 2, \dots, i$). By repeating some of the lines, we can ensure that C has degree d. This is because $d \ge k - 1$ and the number of lines L_j (for $j = 1, 2, \dots, i$) is at most $i \le k - 1$. By construction, C has degree d, C passes through $P_1, P_2, \dots, P_i$ but C does not pass through P_{i+1}.

Next assume that $d \ge 2q - 1$. In this case, we can instead use a construction due to Homma and Kim (a special case of [HK18, Corollary 2.4]). We can find a polynomial f with degree d that vanishes on all points of $\mathbb{P}^2(\mathbb{F}_q)$ except for P_{i+1} (in particular, $C = \{f = 0\}$ passes through $P_1, P_2, \dots, P_i$ but C does not pass through P_{i+1}). In fact, we can explicitly construct such a polynomial f by noticing that the polynomial

$$x^{d-(2q-2)}(y^{q-1} - x^{q-1})(z^{q-1} - x^{q-1})$$

vanishes on $\mathbb{P}^2(\mathbb{F}_q) \setminus \{[1 : 0 : 0]\}$.

This concludes that proof of the strict inclusion $W_i \supsetneq W_{i+1}$, and the desired result follows. $\qquad\square$

Remark 3.2. When k is close to $q^2 + q + 1$, the degree $2q - 1$ in the statement of Proposition 3.1 is optimal. The paper by Homma and Kim [HK18, Section 3] contains a detailed discussion.

When $d \ge q^2 + q$, the following proposition [BDFL10, Proposition 1.6] describes the explicit distribution of the number of rational points of degree d plane curves over $\mathbb{F}_q$, which consequently implies that the limiting distribution of the number of rational points (up to normalization) is the standard normal distribution (compare to Theorem 2.2 and Remark 2.4). The original proof of [BDFL10, Proposition 1.6] relied on the more general interpolation result developed by Poonen [Poo04, Lemma 2.1]. Lercier et. al. have observed that the construction due to Homma and Kim allows one to weaken the condition $d \ge q^2 + q$ to $d \ge 2q - 1$ in [LRR+19, Proposition 3.1]. Let us explain how Proposition 3.1 leads to a quick proof of this useful result. We present a complete proof below because we will refer to it in later discussions.

Proposition 3.3. *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 each integer $0 \le t \le q^2 + q + 1$ and $d \ge 2q - 1$, we have*

$$\frac{\#\{F \in S_d : \#C_F(\mathbb{F}_q) = t\}}{\#S_d} = \Pr\left(Y_1 + \cdots + Y_{q^2+q+1} = t\right).$$

Proof. Enumerate all the points of $\mathbb{P}^2(\mathbb{F}_q)$ as $P_1, P_2, \dots, P_{q^2+q+1}$. Let C be a random plane curve with degree d. We define the random variables $Z_1, Z_2, \dots, Z_{q^2+q+1}$ as follows: if C passes through P_i, assign Z_i to be 1 and otherwise 0. It suffices to show that for any $\epsilon_1, \epsilon_2, \dots, \epsilon_{q^2+q+1} \in \{0, 1\}$, we have

$$\Pr(Z_i = \epsilon_i \text{ for all } i \le q^2+q+1) = \Pr(Y_i = \epsilon_i \text{ for all } i \le q^2+q+1) = \left(\frac{1}{q}\right)^{|I|}\left(\frac{q-1}{q}\right)^{q^2+q+1-|I|},$$

where $I = \{i : \epsilon_i = 1\}$. Since $d \geq 2q - 1$, Proposition 3.1 implies that for any $J \subset \{1, 2, \ldots, q^2 + q + 1\}$,

$$\Pr(Z_j = 1 \text{ for all } j \in J) = \left(\frac{1}{q}\right)^{|J|}.$$

It follows from the principle of inclusion and exclusion, and the binomial theorem that

$$\Pr(Z_i = \epsilon_i \text{ for all } i \leq q^2 + q + 1) = \sum_{J \supset I} (-1)^{|J|-|I|} \Pr(Z_j = 1 \text{ for all } j \in J)$$

$$= \sum_{J \supset I} (-1)^{|J|-|I|} \left(\frac{1}{q}\right)^{|J|} = \sum_{k=|I|}^{q^2+q+1} \binom{q^2 + q + 1 - |I|}{k - |I|} (-1)^{k-|I|} \left(\frac{1}{q}\right)^k$$

$$= \left(\frac{1}{q}\right)^{|I|} \sum_{k=0}^{q^2+q+1-|I|} \binom{q^2 + q + 1 - |I|}{k} \left(-\frac{1}{q}\right)^k = \left(\frac{1}{q}\right)^{|I|} \left(\frac{q-1}{q}\right)^{q^2+q+1-|I|}$$

leading to the desired result. □

3.2. **Expected number of skew lines.**
In this subsection, we build machinery to calculate the number of skew lines to a random plane curve from a probabilistic perspective (see Corollary 3.6).

Theorem 3.4. *Suppose f is a function with $f(q)/q \to 1$ as $q \to \infty$. Let $P_1, P_2, \ldots, P_{f(q)}$ be distinct points in $\mathbb{P}^2(\mathbb{F}_q)$. For $d \geq f(q) - 1$, consider the space S_d of degree d plane curves defined over $\mathbb{F}_q$. Let X_q be the random variable representing the number of P_i that is contained in a random plane curve $C \in S_d$. As $q \to \infty$, the limiting distribution of X_q is Poisson with mean $\lambda = 1$.*

Proof. We can apply Proposition 3.1, similar to the proof of Proposition 3.3, to deduce that X_q has a binomial distribution $\mathrm{Bin}(f(q), 1/q)$. The conclusion follows from Poisson limit theorem [Bil95, Theorem 23.2] since

$$\lim_{q \to \infty} \mathbb{E}(X_q) = \lim_{q \to \infty} \frac{f(q)}{q} = 1.$$

□

As an application, we will discuss the following question: how many roots in $\mathbb{F}_q$ does a random polynomial in $\mathbb{F}_q[x]$ have? Leont'ev [Leo06] proved the following result which shows that the number of distinct roots is controlled by the Poisson distribution. The original proof is somewhat involved, and uses probability generating functions and some tools from complex analysis. We refer to [LL21] for a different proof of this fact using tools from number theory and generating functions. The proof given below is much shorter.

Corollary 3.5 (Leont'ev). *As $q \to \infty$, the number of distinct $\mathbb{F}_q$-roots of a random polynomial $f \in \mathbb{F}_q[x]$ with degree at most $q - 1$, tends to the Poisson distribution with mean $\lambda = 1$.*

Proof. Let V_{q-1} be the subspace of $\mathbb{F}_q[x]$ consisting of polynomials with degree at most $q - 1$. There is a natural surjective linear map $\pi \colon S_{q-1} \to V_{q-1}$ given by $f(x, y, z) \mapsto f(x, 1, 0)$. Since any two fibers of π are isomorphic, as we pick f uniformly randomly from S_{q-1}, the resulting image polynomials $\pi(f)$ also result in the uniform distribution on V_{q-1}. Moreover, the number of distinct $\mathbb{F}_q$-roots of $\pi(f)$ is equal to the number of $\mathbb{F}_q$-points in the intersection of the curve $\{f = 0\}$ with the affine line $\{z = 0\} - \{[1 : 0 : 0]\} = \{[x : 1 : 0] : x \in \mathbb{F}_q\} \cong \mathbb{A}^1$. The desired result follows from invoking Theorem 3.4 with the q points on this affine line. □

The next corollary is a first step in estimating the number of skew lines to a random plane curve.

Corollary 3.6. *Let L be a fixed $\mathbb{F}_q$-line. For a random plane curve C of degree $d \geq q$, the random variable $\#(C \cap L)(\mathbb{F}_q)$ tends to the Poisson distribution with mean $\lambda = 1$. In particular, the number of skew lines to a random plane curve C is $q^2/e + o(q^2)$.*

Proof. The first assertion follows immediately from Theorem 3.4. In particular, for each line L, the probability that $(C \cap L)(\mathbb{F}_q) = \emptyset$ is $1/e + o(1)$. Since there are $q^2 + q + 1$ lines, the expected number of skew lines to C is $(q^2 + q + 1) \cdot (1/e + o(1)) = q^2/e + o(q^2)$ by the linearity of expectation. $\square$

In Theorem 1.3 we will prove a refined estimate on the expected number of skew lines.

Remark 3.7. The same result on the number of skew lines for different ranges of q and d is obtained by Entin [Ent21]. Let $C \subset \mathbb{P}^2$ be a geometrically irreducible projective plane curve of degree d. Consider the space $Y = (\mathbb{P}^2)^*$ which parametrizes all lines in $\mathbb{P}^2$. We also have the variety X given by:
$$X = \{(P, L) \mid P \in C \cap L\} \subset \mathbb{P}^2 \times (\mathbb{P}^2)^*.$$
Consider the map $f \colon X \to Y$ given by projection to the second coordinate. Note that f is a finite map with $\deg(f) = d$. Suppose that the monodromy group $\mathrm{Mon}(X/Y)$ is equal to the symmetric group $\mathfrak{S}_d$. Having an $\mathbb{F}_q$-point in the fiber $f^{-1}(L)$ for a given $\mathbb{F}_q$-line L is equivalent to a corresponding Frobenius class of the map f at the point L having a fixed point. Applying the Chebotarev density theorem for varieties over finite fields [Ent21, Theorem 3] for each conjugacy class in $\mathfrak{S}_d$ with no fixed points and summing up the contributions, we obtain:
$$\frac{\#\{\text{skew } \mathbb{F}_q\text{-lines to } C\}}{q^2} \approx \frac{\#\text{permutations without fixed points}}{\#\mathfrak{S}_d} = \frac{!d}{d!} = \sum_{i=0}^{d} \frac{(-1)^i}{i}$$
for sufficiently large q. As d gets larger and larger (but fixed), the proportion above will approach $1/e$. When d is fixed, and $q \to \infty$, almost all plane curves are smooth (due to the Lang-Weil bound applied to the discriminant hypersurface) and in particular geometrically irreducible. Therefore, the assumption on the curve made above does not affect the density, if we consider all plane curves of degree d. This limiting proportion $1/e$ is in agreement with our result above. However, the ranges for q and d are different, since we allow d to be large with respect to q.

We can also apply Entin's result in the situation where the conjugacy class has a certain number of fixed points. Furthermore, it is well-known that the number of fixed points of a random permutation on d letters converges to the Poisson distribution with mean 1 as d tends to infinity [Kho07, Example 1.19]. Combining these two ingredients, we get a similar result to Theorem 3.4 but with different ranges for q and d.

4. PROPORTION OF BLOCKING PLANE CURVES

In this section, we will analyze the asymptotic proportion of plane curves of degree d over $\mathbb{F}_q$ which do not form a blocking set. One of the goals of this section is to explain that even a curve of large degree d over a fixed finite field $\mathbb{F}_q$ is not blocking with very high probability.

Let $\mathbb{F}_q$ be a finite field, and $S = \mathbb{F}_q[x, y, z]$. As we saw in Section 2, $S_d \subset S$ denotes the vector subspace of polynomials of degree $d \geq 1$ (including the 0 polynomial). For any subset $A \subset S$, let $\mu_d(A) = \frac{\#(A \cap S_d)}{\#S_d}$. We can define the *upper natural density* and *lower natural density* respectively

as follows,

$$\overline{\mu}(A) = \limsup_{d\to\infty} \mu_d(A) = \limsup_{d\to\infty} \frac{\#(A\cap S_d)}{\#S_d}, \qquad \underline{\mu}(A) = \liminf_{d\to\infty} \mu_d(A) = \liminf_{d\to\infty} \frac{\#(A\cap S_d)}{\#S_d}.$$

If the lower and upper densities agree, then we define the *natural density* of $\mathcal{A}$ by $\mu(A) = \overline{\mu}(A) = \underline{\mu}(A)$ and in this case,

$$\mu(A) = \lim_{d\to\infty} \frac{\#(A\cap S_d)}{\#S_d}.$$

Recall that C_F denotes the plane curve defined by the equation $F = 0$. Let $\mathcal{B} \subset S = \mathbb{F}_q[x, y, z]$ denote the set of homogeneous polynomials F such that the curve C_F is blocking. The primary goal of the present paper is to understand the natural density of $\mathcal{B}$. It turns out that the complement of $\mathcal{B}$ is easier to work with, justifying the following.

Definition 4.1. Let $\mathbb{F}_q$ be a fixed finite field. Define $\mathcal{E}$ as follows:

$$\mathcal{E} = \bigcup_{d\geq 1}\{F \in S_d \mid C_F \text{ is not blocking}\}.$$

To gain insight about the natural density $\mu(\mathcal{E})$, we first stratify the space $\mathcal{E}$ by different $\mathbb{F}_q$-lines and understand the corresponding natural density $\mu(\mathcal{E}_L)$.

Proposition 4.2. *Let L be a fixed $\mathbb{F}_q$-line in $\mathbb{P}^2$. Let*

$$\mathcal{E}_L = \bigcup_{d\geq 1}\{F \in S_d \mid C_F \cap L \text{ has no } \mathbb{F}_q\text{-points}\}.$$

Then $\mu_d(\mathcal{E}_L) = \left(1 - \dfrac{1}{q}\right)^{q+1}$ for $d \geq q$, which is approximately $\dfrac{1}{e}$ for q large.

Proof. Let

$$\mathcal{A}_d = \{F \in S_d \mid C_F \cap L \text{ has at least one } \mathbb{F}_q\text{-point}\}.$$

For each $\mathbb{F}_q$-point $P \in L$, define:

$$\mathcal{A}_d^P = \{F \in S_d \mid P \in C_F \cap L\}.$$

It is clear that

$$\mathcal{A}_d = \bigcup_{P\in L(\mathbb{F}_q)} \mathcal{A}_d^P.$$

Let $N = \binom{d+2}{2}$. For any $1 \leq k \leq q+1$ points $P_1, P_2, \ldots, P_k \in L(\mathbb{F}_q)$, by Proposition 3.1,

$$\#\bigcap_{i=1}^{k} \mathcal{A}_d^{P_i} = q^{N-k}$$

for $d \geq k - 1$. Using the principle of inclusion and exclusion, we obtain:

$$\#\mathcal{A}_d = \#\bigcup_{P\in L(\mathbb{F}_q)} \mathcal{A}_d^P = \sum_{k=1}^{q+1} \binom{q+1}{k}(-1)^{k+1} \cdot \left(q^{N-k}\right)$$

$$= q^N \sum_{k=1}^{q+1} \binom{q+1}{k}(-1)^{k+1}(q^{-1})^k = q^N + q^N \sum_{k=0}^{q+1} \binom{q+1}{k}(-1)^{k+1}(q^{-1})^k$$

10

$$= q^N - q^N \sum_{k=0}^{q+1} \binom{q+1}{k} (-q^{-1})^k = q^N - q^N (1 - q^{-1})^{q+1}$$

for $d \geq q$. Thus,

$$\mu_d(\mathcal{A}_d) = \frac{q^N - q^N(1 - q^{-1})^{q+1}}{q^N} = 1 - (1 - q^{-1})^{q+1}.$$

Therefore,

$$\mu_d(\mathcal{E}_L) = 1 - \mu_d(\mathcal{A}_d) = 1 - (1 - (1 - q^{-1})^{q+1}) = (1 - q^{-1})^{q+1} \approx \frac{1}{e}$$

as desired. $\qquad\square$

Proposition 4.2 already allows us to deduce one of our main results, namely Theorem 1.3, on the expected number of skew lines.

Proof of Theorem 1.3. As a preliminary step, we observe the Taylor expansion,

$$\left(1 - \frac{1}{x}\right)^x - \frac{1}{e} = -\frac{1}{2ex} - \frac{5}{24ex^2} + O\left(\frac{1}{x^3}\right). \tag{2}$$

By Proposition 4.2, the probability that a fixed line L is skew to a random plane curve C of degree $d \geq q$ is exactly $\left(1 - \frac{1}{q}\right)^{q+1}$. Using (2), we obtain

$$\left(1 - \frac{1}{q}\right)^{q+1} = \left(\frac{1}{e} - \frac{1}{2eq} - \frac{5}{24eq^2} + O\left(\frac{1}{q^3}\right)\right)\left(1 - \frac{1}{q}\right) = \frac{1}{e} - \frac{3}{2eq} + \frac{7}{24eq^2} + O\left(\frac{1}{q^3}\right).$$

Thus, by the linearity of expectation, the expected number of skew lines to C is

$$\frac{q^2 + q + 1}{e} - \frac{3(q^2 + q + 1)}{2eq} + \frac{7(q^2 + q + 1)}{24eq^2} + O\left(\frac{1}{q}\right) = \frac{q^2}{e} - \frac{q}{2e} - \frac{5}{24e} + O\left(\frac{1}{q}\right)$$

as desired. $\qquad\square$

The next result gives an explicit formula for the natural density $\mu_d(\mathcal{E})$ in terms of the statistics on the number of $\mathbb{F}_q$-points contained in a union of $\mathbb{F}_q$-lines.

Proposition 4.3. *Let $\mathbb{F}_q$ be a finite field. Let $(\mathbb{P}^2)^*(\mathbb{F}_q)$ denote the set of all $\mathbb{F}_q$-lines in the plane. For $d \geq 2q - 1$, we have*

$$\mu_d(\mathcal{E}) = \sum_{k=1}^{q^2+q+1} \sum_{\substack{T \subset (\mathbb{P}^2)^*(\mathbb{F}_q) \\ |T|=k}} (-1)^{k+1} \cdot \left(1 - \frac{1}{q}\right)^{\#(\bigcup_{L \in T} L)(\mathbb{F}_q)}.$$

In particular, the formula above also computes the constant $\mathrm{nb}(q) = \lim_{d \to \infty} \mu_d(\mathcal{E})$.

Proof. Note that $F \in \mathcal{E}$ if and only if $C_F \cap L$ has no $\mathbb{F}_q$-points for some $\mathbb{F}_q$-line L. Using the notation used in Proposition 4.2, we have

$$\mathcal{E} = \bigcup_{L \in (\mathbb{P}^2)^*(\mathbb{F}_q)} \mathcal{E}_L.$$

11

Using the principle of inclusion and exclusion, we get:

$$|\mathcal{E} \cap S_d| = \sum_{k=1}^{q^2+q+1} \sum_{\substack{T \subset (\mathbb{P}^2)^*(\mathbb{F}_q) \\ |T|=k}} (-1)^{k+1} \cdot \left| \bigcap_{L \in T} \mathcal{E}_L \cap S_d \right|.$$

It remains to calculate the density of $\bigcap_{L \in T} \mathcal{E}_L$. Using the same idea as in Proposition 3.3 and Proposition 4.2, we obtain:

$$\mu_d \left(\bigcap_{L \in T} \mathcal{E}_L \right) = \left(1 - \frac{1}{q} \right)^{\#(\bigcup_{L \in T} L)(\mathbb{F}_q)}$$

as desired. $\qquad \square$

Even though Proposition 4.3 gives us the theoretical answer for the proportion of non-blocking curves, it is not feasible in practice. The inequalities in our main Theorem 1.4 are more applicable. We present the proof of these inequalities by estimating the "main term" contribution to the sum in Proposition 4.3.

Proof of Theorem 1.4. We start with the proof of the upper bound on $\mathrm{nb}(q)$. Our goal is to prove:

$$1 - \mathrm{nb}(q) \geq \frac{1}{q} \left(1 - \left(1 - \left(\frac{1}{q} \right)^q \right)^{q+1} \right) + \frac{1}{q} \sum_{j=1}^{q} \left(1 - \frac{1}{q} \right)^j \left(1 - \left(1 - \left(\frac{1}{q} \right)^q \right)^q \right). \quad (3)$$

Note that $1 - \mathrm{nb}(q)$ is the density of blocking curves. On the other hand, we claim that the right-hand side of inequality (3) represents the density of a particular family of (trivially) blocking curves. To see this, consider $q + 1$ collinear $\mathbb{F}_q$-points $P_0, \ldots, P_q$ on a fixed $\mathbb{F}_q$-line L_0. Let us say that a plane curve C is *trivially blocking with respect to* a point P, if C contains all the $\mathbb{F}_q$-points of *some* $\mathbb{F}_q$-line L passing through P. For each $0 \leq j \leq q$, consider

$$\mathcal{B}_j = \{ F \in \mathcal{B} \mid C_F \text{ is trivially blocking with respect to } P_j, \text{ and } P_i \notin C_F \text{ for } i < j \}.$$

Then by the same idea as in Proposition 3.3,

$$\mu(\mathcal{B}_0) = \frac{1}{q} \left(1 - \left(1 - \left(\frac{1}{q} \right)^q \right)^{q+1} \right),$$

$$\mu(\mathcal{B}_j) = \frac{1}{q} \left(1 - \frac{1}{q} \right)^j \left(1 - \left(1 - \left(\frac{1}{q} \right)^q \right)^q \right) \qquad \text{for } j \geq 1.$$

Indeed, $\mu(\mathcal{B}_0)$ counts the density of curves that are trivially blocking with respect to P_0. First, we restrict ourselves to the event where the curve passes through P_0. Given a line $L \ni P_0$, note that $1 - \left(\frac{1}{q} \right)^q$ is the density of curves C such that $L(\mathbb{F}_q) \not\subset C(\mathbb{F}_q)$. By independence, $\left(1 - \left(\frac{1}{q} \right)^q \right)^{q+1}$ is the density of curves for which all the $q+1$ lines passing through P satisfy $L(\mathbb{F}_q) \not\subset C(\mathbb{F}_q)$. By looking at the complement, we obtain the formula for $\mu(\mathcal{B}_0)$. The analogous argument works for $\mu(\mathcal{B}_j)$ for $j \geq 1$ with the exception that one of the $\mathbb{F}_q$-lines passing through P_j is L_0 which already satisfies $L_0(\mathbb{F}_q) \not\subset C(\mathbb{F}_q)$ so we can ignore it while counting the $\mathbb{F}_q$-lines passing through P_j. As the subsets $\mathcal{B}_j$ for $j = 0, 1, \ldots, q$ are disjoint, the inequality (3) readily follows.

The proof of the lower bound on $\mathrm{nb}(q)$ is established in a similar manner. To give a quick overview, we want to establish

$$\mathrm{nb}(q) \geq \left(1 - \frac{1}{q}\right)\left(1 - \left(1 - \left(1 - \frac{1}{q}\right)^q\right)^{q+1}\right) + \left(1 - \frac{1}{q}\right)\sum_{j=1}^q \left(\frac{1}{q}\right)^j\left(1 - \left(1 - \left(1 - \frac{1}{q}\right)^q\right)^q\right)$$

(4)

Let us say that a plane curve C is *skew with respect to* a point P, if C contains none of the $\mathbb{F}_q$-points of *some* $\mathbb{F}_q$-line L passing through P. For $0 \leq j \leq q$, consider the disjoint sets:

$$\mathcal{D}_j = \{F \in \mathcal{E} \mid C_F \text{ is skew with respect to } P_j, \text{ and } P_i \in C_F \text{ for } i < j\}.$$

The first term in the right-hand side of inequality (4) comes from $\mu(\mathcal{D}_0)$, and the j-th summand in the sum is due to $\mu(\mathcal{D}_j)$ for $j = 1, \ldots, q$. The difference between the cases $j = 0$ and $j \geq 1$ is reflected by the fact that L_0 cannot be skew to C_F for $F \in \mathcal{D}_j$ once $j \geq 1$. This completes the proof of the lower bound (4). $\qquad\square$

The discussion above leads to an instant proof of our first main theorem.

Proof of Theorem 1.1. The result immediately follows from the lower bound in Theorem 1.4 and the last assertion in Proposition 4.3. $\qquad\square$

While we know that $\lim_{q\to\infty}\mathrm{nb}(q) = 1$, it is less clear how $\mathrm{nb}(q)$ and $\mathrm{nb}(q')$ compare for different values of q and q'. Based on various computations we made (see also Section 7 in which we will calculate the exact values of $\mathrm{nb}(2)$, $\mathrm{nb}(3)$, and $\mathrm{nb}(4)$), we advance the following question.

Question 4.4. Is $\mathrm{nb}(q)$ an increasing function of q?

We observe that Theorem 1.4 yields an increasing sequence of prime powers $q_1 < q_2 < q_3 < \cdots$ such that $\mathrm{nb}(q_1) < \mathrm{nb}(q_2) < \mathrm{nb}(q_3) < \cdots$, providing some evidence for a positive answer to Question 4.4.

5. PROPORTION OF SMOOTH BLOCKING CURVES

Let q be a fixed prime power. When $d \to \infty$, Poonen's result [Poo04, Theorem 1.1] implies that the density of smooth curves over $\mathbb{F}_q$ is $\zeta_{\mathcal{P}^2}(3)^{-1} = (1 - 1/q)(1 - 1/q^2)(1 - 1/q^3)$. The following lemma [BDFL10, Equation 8] provides an effective version with an explicit error bound.

Lemma 5.1. *We have*

$$\frac{\#S_d^{\mathrm{ns}}}{\#S_d} = \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)\left(1 - \frac{1}{q^3}\right)\left(1 + O\left(\frac{d^{-1/3}}{1 - q^{-1} - 2d^{-1/3}}\right)\right)$$
$$+ O\left(\frac{d^{-1/3}}{1 - q^{-1}} + (d-1)^2 q^{-\min\left(\lfloor\frac{d}{p}\rfloor+1, \frac{d}{3}\right)} + dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right).$$

Corollary 5.2. *As $q, d \to \infty$ and $d \geq \min\{2q, 3p\}$, we have*

$$\frac{\#S_d^{\mathrm{ns}}}{\#S_d} \geq \frac{21}{64} + o(1).$$

Proof. When $q, d \to \infty$, it is clear that

$$\frac{d^{-1/3}}{1 - q^{-1}} \to 0, \qquad \frac{d^{-1/3}}{1 - q^{-1} - 2d^{-1/3}} \to 0.$$

13

Moreover, under the extra condition $d \geq 3p$, we have shown in equation (1) that

$$(d-1)^2 q^{-\min\left(\lfloor \frac{d}{p}\rfloor + 1, \frac{d}{3}\right)} + dq^{-\lfloor \frac{d-1}{p}\rfloor - 1} \to 0.$$

If instead we have $d \geq 2q$, one can prove the same estimate by mimicking the proof of Corollary 2.3 by separating the analysis into two cases $p \leq 11$ and $p > 11$.

Thus, the statement follows immediately from Lemma 5.1 and the fact that

$$\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right)\left(1 - \frac{1}{q^3}\right) \geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{2^3}\right) = \frac{21}{64}$$

holds for all q. □

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. When $d \geq 2q$, the result follows immediately from combining Theorem 1.1 and Corollary 5.2. For the remainder of the proof, we assume that $d \geq 3p$.

Let C be a random smooth plane curve of degree d defined over $\mathbb{F}_q$, uniformly chosen from S_d^{ns}. In view of Theorem 2.1, the following three conditions would guarantee that $C(\mathbb{F}_q)$ is not a blocking set:

- $C(\mathbb{F}_q)$ does not contain an $\mathbb{F}_q$-line.
- If q is a square and $q > 16$, then $C(\mathbb{F}_q)$ does not contain a Baer subplane.
- $\#C(\mathbb{F}_q) < q + 1 + q^{2/3}/2^{1/3}$.

If $d < q + 1$, then the first condition is automatically true since it follows from Bézout's theorem that $\#(C \cap L) < q + 1$ for any line L defined over $\mathbb{F}_q$. If $d \geq q + 1$, then for any given L, Proposition 3.1 implies that the proportion of degree d plane curves defined over $\mathbb{F}_q$ which contain the line L is $(\frac{1}{q})^{q+1}$. Since there are in total $q^2 + q + 1$ lines, it follows from the union bound and Corollary 5.2 that

$$\Pr\big(C(\mathbb{F}_q) \text{ contains some } \mathbb{F}_q\text{-line}\big) \leq \left(\frac{64}{21} + o(1)\right)(q^2 + q + 1)\left(\frac{1}{q}\right)^{q+1} = o(1).$$

As for the second condition, it is known that each Baer subplane in $\mathbb{P}^2(\mathbb{F}_q)$ is isomorphic to $\mathbb{P}^2(\mathbb{F}_{\sqrt{q}}) \subset \mathbb{P}^2(\mathbb{F}_q)$ and thus the number of Baer subplanes is bounded by a polynomial in q. More precisely, the number of Baer subplanes in $\mathbb{P}^2(\mathbb{F}_q)$ is $q^{3/2}(q^{3/2} + 1)(q + 1)$ [Mad00, Corollary 1.3]. Note that each Baer subplane has $q + \sqrt{q} + 1 > 5$ points when $q > 16$, so if $d \geq 5$, Proposition 3.1 implies that the proportion of degree d plane curves defined over $\mathbb{F}_q$ which contain a given Baer subplane B is at most $(\frac{1}{q})^5$ since the curve must pass through any given 5 points in B in order to contain B. It follows from the union bound and Corollary 5.2 that

$$\Pr(C(\mathbb{F}_q) \text{ contains some Baer subplane}) \leq \left(\frac{64}{21} + o(1)\right)q^{3/2}(q^{3/2} + 1)(q + 1)\left(\frac{1}{q}\right)^5 = o(1).$$

Regarding the third condition, we apply Corollary 2.3 and Chebyshev's inequality:

$$\Pr\left(\#C(\mathbb{F}_q) \geq q + 1 + q^{2/3}/2^{1/3}\right) = \Pr\left(\frac{\#C(\mathbb{F}_q) - (q+1)}{\sqrt{q+1}} \geq \frac{q^{2/3}}{2^{1/3}\sqrt{q+1}}\right)$$

$$\leq \frac{M_2(q,d) \cdot 2^{2/3}(q+1)}{q^{4/3}} \cdot (1 + o(1)) = o(1).$$

14

While applying Chebyshev's inequality, we used the fact that the mean of $(\#C(\mathbb{F}_q) - (q + 1))/\sqrt{q+1}$ is $M_1(q,d) = o(1)$ from Theorem 2.2.

We conclude that

$$\Pr(C \text{ is not blocking}) \geq 1 - \Pr(C(\mathbb{F}_q) \text{ contains some } \mathbb{F}_q\text{-line})$$

$$- \Pr(C(\mathbb{F}_q) \text{ contains some Baer subplane}) - \Pr\left(\#C(\mathbb{F}_q) \geq q + 1 + q^{2/3}/2^{1/3}\right) = 1 - o(1),$$

as required. $\qquad\square$

Remark 5.3. Using an argument similar to the above proof, we can instead use Proposition 3.3 to deduce Theorem 1.1. In fact, we can get an explicit lower bound on $\mathrm{nb}(q)$. However, even if we use the Chernoff bound (for example Bernstein inequality) instead of Chebyshev's inequality to get a sharper estimate on the tail distribution $\Pr\left(\#C(\mathbb{F}_q) \geq q + 1 + q^{2/3}/2^{1/3}\right)$, the lower bound on $\mathrm{nb}(q)$ obtained in this manner is still much worse compared to the combinatorial lower bound from Section 4.

Corollary 5.4. *Let r be an integer such that $r \geq 7$. Let $q = p^r$. Then for any sequence $\{d_p\}$, as $p \to \infty$, almost all degree d_p smooth curves over $\mathbb{F}_q$ are not blocking.*

Proof. We can decompose the sequence into two parts: the parts with $d_p^6 < q$, that is, $d_p < p^{r/6}$ (such low degree curves are not blocking by [AGY22, Theorem 1.2]); the parts with $d_p > p^{r/6}$. Thus, it suffices to consider any subsequence $\{p_n\}_{n=1}^{\infty}$ of the primes, such that $d_{p_n} > p_n^{r/6}$. However, note that $d_{p_n}/p_n \to \infty$ since $r \geq 7$. Consequently, the density is also 1 as $n \to \infty$ by Theorem 1.2. $\qquad\square$

6. INDEPENDENCE BETWEEN BEING SMOOTH AND BEING BLOCKING

In this section, we investigate the probabilistic independence between the properties of smoothness and being blocking. Given that we obtained a stronger result for the density of smooth blocking curves in Section 5, it is natural to ask whether the probability of a random plane curve being blocking is affected when conditioning on the event that the curve is smooth. We will show that for a fixed $\mathbb{F}_q$ with q large, it is more likely for a smooth curve to be non-blocking compared to a general curve. However, we will show that these two probabilities are asymptotically equal to each other as $q \to \infty$. Recall that

$$\mathrm{nb}(q) = \lim_{d \to \infty} \frac{\#\{F \in S_d : C_F \text{ is not blocking}\}}{\#S_d},$$

and

$$\mathrm{nb}^{\mathrm{ns}}(q) = \lim_{d \to \infty} \frac{\#\{F \in S_d^{\mathrm{ns}} : C_F \text{ is not blocking}\}}{\#S_d^{\mathrm{ns}}}.$$

We introduce further notations to simplify the upcoming proof. For each set $B \subseteq \mathbb{P}^2(\mathbb{F}_q)$, we define

$$\nu(q, B) = \lim_{d \to \infty} \frac{\#\{F \in S_d : C_F(\mathbb{F}_q) = B\}}{\#S_d}. \tag{5}$$

Similarly, we define

$$\nu^{\mathrm{ns}}(q, B) = \lim_{d \to \infty} \frac{\#\{F \in S_d^{\mathrm{ns}} : C_F(\mathbb{F}_q) = B\}}{\#S_d^{\mathrm{ns}}}. \tag{6}$$

We prove a more refined version of Theorem 1.5 from the introduction.

15

Theorem 6.1. *For sufficiently large q, we have $\mathrm{nb}(q) < \mathrm{nb}^{\mathrm{ns}}(q)$, and therefore, the events of being smooth and being blocking are not independent for curves over $\mathbb{F}_q$. However,*

$$\lim_{q\to\infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} = 1.$$

Thus, the events of being smooth and being blocking are asymptotically independent.

Proof. Since q is fixed, there are only finitely many configurations of blocking sets B in $\mathbb{P}^2(\mathbb{F}_q)$. Thus, we can interchange the limit and summation to get

$$1 - \mathrm{nb}(q) = \sum_{B \subseteq \mathbb{P}^2(\mathbb{F}_q) \text{ blocking set}} \nu(q, B).$$

Similarly, we have

$$1 - \mathrm{nb}^{\mathrm{ns}}(q) = \sum_{B \subseteq \mathbb{P}^2(\mathbb{F}_q) \text{ blocking set}} \nu^{\mathrm{ns}}(q, B).$$

Let A_i and A_i^{ns} be the contribution to $1 - \mathrm{nb}(q)$ and $1 - \mathrm{nb}^{\mathrm{ns}}(q)$ from blocking sets with size i, respectively.

Let B be a blocking set with $|B| = t$; then we know $t \geq q + 1$. By [BDFL10, p. 2537], we have

$$\nu^{\mathrm{ns}}(q, B) = \left(\frac{q+1}{q^2+q+1}\right)^t \left(\frac{q^2}{q^2+q+1}\right)^{q^2+q+1-t}. \tag{7}$$

On the other hand, in the proof of Proposition 3.3, we have shown that

$$\nu(q, B) = \left(\frac{1}{q}\right)^t \left(\frac{q-1}{q}\right)^{q^2+q+1-t}. \tag{8}$$

It follows from equations (7) and (8) that

$$\frac{\nu^{\mathrm{ns}}(q, B)}{\nu(q, B)} = \left(1 - \frac{1}{q^2}\right)^t \left(1 + \frac{1}{q^3-1}\right)^{q^2+q+1}. \tag{9}$$

Note that the ratio is a decreasing function in t. When $t = o(q^2)$, the above ratio is close to 1. However, if $t \approx Cq^2$, then the above ratio is close to $1/e^C < 1$. Summing over the contribution from all blocking sets B, this already implies that

$$\frac{1}{e} \leq \liminf_{q\to\infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} \leq \limsup_{q\to\infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} \leq 1. \tag{10}$$

We first show $\mathrm{nb}^{\mathrm{ns}}(q) > \mathrm{nb}(q)$, or equivalently, $1 - \mathrm{nb}(q) > 1 - \mathrm{nb}^{\mathrm{ns}}(q)$, when q is sufficiently large. Using the Taylor expansion, it is easy to see that, when q is sufficiently large, the ratio in equation (9) is less than 1 whenever $t = |B| \geq q + 2$. Thus, $A_i > A_i^{\mathrm{ns}}$ for $i \geq q + 2$. It suffices to show that,

$$A_{q+4} + A_{q+1} > A_{q+4} > A_{q+4}^{\mathrm{ns}} + A_{q+1}^{\mathrm{ns}}. \tag{11}$$

By Theorem 2.1, a blocking set with size $q + 1$ or $q + 4$ must be a trivial blocking set. Thus, the number of blocking sets with size $q + 1$ is $q^2 + q + 1$ (the number of $\mathbb{F}_q$-lines), and the number of blocking sets with size $q + 4$ is $(q^2 + q + 1) \cdot \binom{q^2}{3}$ (pick an $\mathbb{F}_q$-line, and then pick three points outside the line). This observation, together with equations (7) and (8), allows one to deduce that the contribution from blocking sets with size $q + 1$ is negligible compared to the contribution from blocking sets with size $q + 4$, when q is large. More precisely, when q is sufficiently large, from

16

equation (9), we obtain that $A_{q+4} > A^{\mathrm{ns}}_{q+4}(1+1/q^2)$ and $A^{\mathrm{ns}}_{q+1} = o(A^{\mathrm{ns}}_{q+4}/q^2)$. Thus, $A_{q+4}+A_{q+1} > A_{q+4} > A^{\mathrm{ns}}_{q+4} + A^{\mathrm{ns}}_{q+1}$ when q is large, confirming equation (11). Now, $1 - \mathrm{nb}(q) > 1 - \mathrm{nb}^{\mathrm{ns}}(q)$ follows from equation (11) and the previous observation $A_i > A^{\mathrm{ns}}_i$ for $i \geq q+2$.

We proceed to prove the second assertion regarding the asymptotic independence. We know that $1 - \mathrm{nb}(q) \geq (\frac{1}{q})^{q+1}$ by Theorem 1.4. We claim that the contribution to $1 - \mathrm{nb}(q)$ coming from blocking sets with size greater than $q^2/\log q$ is negligible:

$$\sum_{i \geqslant q^2/\log q} A_i \leq \sum_{\substack{B \subseteq \mathbb{P}^2(\mathbb{F}_q), \\ |B| \geqslant q^2/\log q}} \left(\frac{1}{q}\right)^{|B|} \leq 2^{q^2+q+1}\left(\frac{1}{q}\right)^{q^2/\log q} = \left(\frac{2 + o(1)}{e}\right)^{q^2} = o\left(\frac{1}{q^{q+1}}\right). \quad (12)$$

Combining equations (9) and (12), we obtain the following lower bound:

$$\begin{aligned}
1 - \mathrm{nb}^{\mathrm{ns}}(q) &\geq \sum_{i \leqslant q^2/\log q} A^{\mathrm{ns}}_i \geq \sum_{i \leqslant q^2/\log q} \left(1 - \frac{1}{q^2}\right)^{q^2/\log q}\left(1 + \frac{1}{q^3 - 1}\right)^{q^2+q+1} A_i \\
&\geq \left(1 - \frac{1}{q^2}\right)^{q^2/\log q}\left(1 + \frac{1}{q^3 - 1}\right)^{q^2+q+1}\left(1 - \mathrm{nb}(q) - \sum_{i \geqslant q^2/\log q} A_i\right) \\
&= \left(1 - O\left(\frac{1}{\log q}\right)\right)\left(1 + O\left(\frac{1}{q}\right)\right)\left(1 - \mathrm{nb}(q)\right)\left(1 - o(1)\right).
\end{aligned}$$

Consequently,

$$\liminf_{q \to \infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} \geq 1.$$

In view of inequality (10), we deduce that

$$\lim_{q \to \infty} \frac{1 - \mathrm{nb}^{\mathrm{ns}}(q)}{1 - \mathrm{nb}(q)} = 1.$$

Thus, the event of being smooth and the event of being blocking are asymptotically independent. $\square$

Remark 6.2. In our analysis above, the quantities $\nu(q, B)$ and $\nu^{\mathrm{ns}}(q, B)$ already take into account the condition $d \to \infty$. However, by a more careful computation (especially by analyzing equation (7) more closely), one can obtain an effective estimate. We could get the same final answer by considering degree d plane curves with $d > q^{3(q^2+q+1)+\epsilon}$ instead of letting $d \to \infty$.

Remark 6.3. The class of geometrically irreducible plane curves include smooth curves. Moreover, it is known that the density of geometrically irreducible curves of degree d over a fixed $\mathbb{F}_q$ approaches 1 as $d \to \infty$ [Poo04, Proposition 2.7]. The same result as in Theorem 1.5 will hold, that is, being blocking and geometrically irreducible are asymptotically independent. One can combine the proof idea in our result with the analysis in Poonen [Poo04, Proposition 2.7] to obtain a better effective version for the statement involving independence. For example, the bound $d > q^{\varepsilon}$ would suffice instead of $d > q^{3(q^2+q+1)+\epsilon}$ as in Remark 6.2.

Remark 6.4. Our proof can be adapted to show the asymptotic independence for the events of being smooth, and satisfying other combinatorial properties described by passing through a specific collection of points. For example, if k is fixed, we can show that being a k-arc and being smooth are independent events. The reason is that the inequality (10) holds when the condition of being

blocking is replaced by any other property. Moreover, the upper bound in Theorem 1.4 was the only ingredient that we needed in order to ensure that the final limit is 1. Any other combinatorial structure satisfying an analogous lower bound will yield the same limit.

However, without an analogue of Theorem 1.4, we cannot guarantee that the final limit is 1. In particular, consider the event E that a random plane curve is space-filling (that is, passing through all $q^2 + q + 1$ distinct $\mathbb{F}_q$-points of $\mathbb{P}^2$). Then E is not independent from the event that a random plane curve is smooth, and the limiting ratio of the respective probabilities is $1/e$.

7. PROPORTION OF BLOCKING CURVES OVER SMALL FINITE FIELDS

In this section, we have used SageMath [The22] to carry out the exact computation for $\mathrm{nb}(q)$ for $q = 2, 3, 4$ by applying the explicit formula given in Proposition 4.3. The formula involves counting all possible frequencies of the number of $\mathbb{F}_q$-rational points contained in a union of k distinct $\mathbb{F}_q$-lines for $k = 1, 2, \ldots, q^2 + q + 1$. This directly provides an algorithm of running time $O(q^2 2^{q^2+q+1})$ which is infeasible for q already moderately large.

Recall that $\mathrm{nb}(q)$ is the limiting proportion (as $d \to \infty$) of degree d non-blocking plane curves among all degree d plane curves defined over $\mathbb{F}_q$. As we saw earlier in Section 4, the constant $\mathrm{nb}(q)$ coincides with the density of fixed degree d non-blocking curves whenever $d \geq 2q - 1$.

Example 7.1. Let us calculate $\mathrm{nb}(2)$. We have $q^2 + q + 1 = 7$ distinct $\mathbb{F}_2$-lines. Using SageMath, we have tabulated the number of points in the union of k lines for $1 \leq k \leq 7$.

Value of k	# of $\mathbb{F}_2$-points	frequency	Value of k	# of $\mathbb{F}_2$-points	frequency
$k = 1$	3	7	$k = 4$	7	28
$k = 2$	5	21	$k = 5$	7	21
$k = 3$	6	28	$k = 6$	7	7
$k = 3$	7	7	$k = 7$	7	1
$k = 4$	6	7			

Applying Proposition 4.3, we get that for $d \geq 3$,

$$\mu_d(\mathcal{E}) = 7 \cdot \left(\frac{1}{2}\right)^3 - 21 \cdot \left(\frac{1}{2}\right)^5 + 28 \cdot \left(\frac{1}{2}\right)^6 + 7 \cdot \left(\frac{1}{2}\right)^7$$

$$- 7 \cdot \left(\frac{1}{2}\right)^6 - 28 \cdot \left(\frac{1}{2}\right)^7 + (21 - 7 + 1) \cdot \left(\frac{1}{2}\right)^7$$

$$= 7 \cdot \left(\frac{1}{2}\right)^3 - 21 \cdot \left(\frac{1}{2}\right)^5 + 21 \cdot \left(\frac{1}{2}\right)^6 - 6 \cdot \left(\frac{1}{2}\right)^7 = \frac{1}{2}$$

We conclude that for each $d \geq 3$, the density of curves of degree d over $\mathbb{F}_2$ which do not provide a blocking set is equal to $1/2$. In particular, $\mathrm{nb}(2) = 1/2$.

In contrast, the density is different when $d = 1$ or $d = 2$. For $d = 1$, we know that 100% of the curves are blocking. For $d = 2$, the only blocking conics are unions of (not necessarily distinct) $\mathbb{F}_q$ lines. Thus, the proportion of conic blocking curves is given by:

$$\frac{(\frac{1}{2}(q^2 + q + 1)(q^2 + q) + (q^2 + q + 1))(q - 1) + 1}{q^6}$$

which evaluates to $11/32$ when $q = 2$. Thus, the proportion of non-blocking conics over $\mathbb{F}_q$ is $\frac{21}{32}$.

Example 7.2. Let us calculate $\mathrm{nb}(3)$. We have $q^2 + q + 1 = 13$ distinct $\mathbb{F}_3$-lines. Using SageMath, we have tabulated the number of points in the union of k lines for $1 \leq k \leq 13$.

Value of k	# of $\mathbb{F}_3$-points	frequency	Value of k	# of $\mathbb{F}_3$-points	frequency
$k = 1$	4	13	$k = 6$	13	702
$k = 2$	7	78	$k = 7$	12	468
$k = 3$	9	234	$k = 7$	13	1248
$k = 3$	10	52	$k = 8$	12	117
$k = 4$	10	234	$k = 8$	13	1170
$k = 4$	11	468	$k = 9$	12	13
$k = 4$	13	13	$k = 9$	13	702
$k = 5$	11	468	$k = 10$	13	286
$k = 5$	12	702	$k = 11$	13	78
$k = 5$	13	117	$k = 12$	13	13
$k = 6$	11	78	$k = 13$	13	1
$k = 6$	12	936			

Applying Proposition 4.3, we get that for $d \geq 5$,

$$
\mu_d(\mathcal{E}) = 13 \cdot \left(\frac{2}{3}\right)^4 - 78 \cdot \left(\frac{2}{3}\right)^7 + 9 \cdot \left(\frac{2}{3}\right)^9 + (52 - 234) \cdot \left(\frac{2}{3}\right)^{10} +
$$

$$
+ (-468 + 468 - 78) \cdot \left(\frac{2}{3}\right)^{11} + (702 - 936 + 468 - 117 + 13) \left(\frac{2}{3}\right)^{12}
$$

$$
+ (-13 + 117 - 702 + 1248 - 1170 + 702 - 286 + 78 - 13 + 1) \left(\frac{2}{3}\right)^{13}
$$

$$
= \frac{1336688}{1594323} = \frac{2^4 \cdot 19 \cdot 4397}{3^{13}} \approx 0.8384
$$

We conclude that for each $d \geq 5$, the density of curves of degree d over $\mathbb{F}_3$ which do not provide a blocking set is approximately equal to 0.8384. In particular, $\mathrm{nb}(3) \approx 0.8384$.

Example 7.3. The proportion of non-blocking curves over $\mathbb{F}_4$ is

$$
\mathrm{nb}(4) = \frac{2112952233969}{2199023255552} = \frac{3^6 \cdot 29 \cdot 67 \cdot 1491727}{2^{41}} \approx 0.96086.
$$

The table below shows how many $\mathbb{F}_4$-points are contained in a union of k distinct $\mathbb{F}_4$-lines in $\mathbb{P}^2$. For example, when $k = 4$, then there are 2520 configurations of 4 lines which contain 14 distinct $\mathbb{F}_4$-points, 3360 configurations of 4 lines which contain 15 distinct $\mathbb{F}_4$-points, and 105 configurations which contain 17 distinct $\mathbb{F}_4$-points.

Value of k	# of $\mathbb{F}_4$-points	frequency	Value of k	# of $\mathbb{F}_4$-points	frequency
$k = 1$	5	21	$k = 9$	18	1120
$k = 2$	9	210	$k = 9$	19	42840
$k = 3$	12	1120	$k = 9$	20	151200
$k = 3$	13	210	$k = 9$	21	98770
$k = 4$	14	2520	$k = 10$	19	13860
$k = 4$	15	3360	$k = 10$	20	140448
$k = 4$	17	105	$k = 10$	21	198408
$k = 5$	15	1008	$k = 11$	19	2520
$k = 5$	16	10080	$k = 11$	20	86688
$k = 5$	17	7560	$k = 11$	21	263508
$k = 5$	18	1680	$k = 12$	19	210
$k = 5$	21	21	$k = 12$	20	37800
$k = 6$	15	168	$k = 12$	21	255920
$k = 6$	17	18480	$k = 13$	20	11760
$k = 6$	18	22680	$k = 13$	21	191730
$k = 6$	19	12600	$k = 14$	20	2520
$k = 6$	21	336	$k = 14$	21	113760
$k = 7$	17	2520	$k = 15$	20	336
$k = 7$	18	31920	$k = 15$	21	53928
$k = 7$	19	55440	$k = 16$	20	21
$k = 7$	20	23520	$k = 16$	21	20328
$k = 7$	21	2880	$k = 17$	21	5985
$k = 8$	18	10290	$k = 18$	21	1330
$k = 8$	19	73080	$k = 19$	21	210
$k = 8$	20	93240	$k = 20$	21	21
$k = 8$	21	26880	$k = 21$	21	1

REFERENCES

[AF21] S. Asgarli and B. Freidin, *On the proportion of transverse-free plane curves*, Finite Fields Appl. **72** (2021), Paper No. 101833, 25.

[AGY22] S. Asgarli, D. Ghioca, and C. H. Yip, *Blocking sets arising from plane curves over finite fields*, arXiv e-prints (2022), available at https://arxiv.org/abs/2208.13299.

[AL20] R. Ait El Manssour and A. Lerario, *Probabilistic enumerative geometry over p-adic numbers: linear spaces on complete intersections*, arXiv e-prints (2020), available at https://arxiv.org/abs/2011.07558. To appear in Ann. Henri Lebesgue.

[BDFL10] A. Bucur, C. David, B. Feigon, and M. Lalín, *Fluctuations in the number of points on smooth plane curves over finite fields*, J. Number Theory **130** (2010), no. 11, 2528–2541.

[Bil95] P. Billingsley, *Probability and measure*, Third, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995. A Wiley-Interscience Publication.

[Blo94] A. Blokhuis, *On the size of a blocking set in* $\mathrm{PG}(2, p)$, Combinatorica **14** (1994), no. 1, 111–114.

[Bru70] A. Bruen, *Baer subplanes and blocking sets*, Bull. Amer. Math. Soc. **76** (1970), 342–344.

[Bru71] _____ , *Blocking sets in finite projective planes*, SIAM J. Appl. Math. **21** (1971), 380–392.

[BSS99] A. Blokhuis, L. Storme, and T. Szőnyi, *Lacunary polynomials, multiple blocking sets and Baer subplanes*, J. London Math. Soc. (2) **60** (1999), no. 2, 321–332.

[Ent21] A. Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, Int. Math. Res. Not. IMRN **14** (2021), 10409–10441.

[HK18] M. Homma and S. J. Kim, *The second largest number of points on plane curves over finite fields*, Finite Fields Appl. **49** (2018), 80–93.

[Kho07] D. Khoshnevisan, *Probability*, Graduate Studies in Mathematics, vol. 80, American Mathematical Society, Providence, RI, 2007.

[KL21] Avinash Kulkarni and Antonio Lerario, *p-adic integral geometry*, SIAM J. Appl. Algebra Geom. **5** (2021), no. 1, 28–59.

[Leo06] V. K. Leont'ev, *On the roots of random polynomials over a finite field*, Mat. Zametki **80** (2006), no. 2, 313–316.

[LL21] K. Liu and M. Lu, *On the degree of the GCD of random polynomials over a finite field*, J. Math. (2021), Art. ID 3619347, 6.

[LRR⁺19] R. Lercier, C. Ritzenthaler, F. Rovetta, J. Sijsling, and B. Smith, *Distributions of traces of Frobenius for smooth plane curves over finite fields*, Exp. Math. **28** (2019), no. 1, 39–48.

[Mad00] R. Maddock, *The bose representation of $PG(2, q^2)$ and some associated varieties*, 2000. Thesis (Ph.D.)– University of Adelaide.

[MSG20] M. Makhul, J. Schicho, and M. Gallet, *Probabilities of incidence between lines and a plane curve over finite fields*, Finite Fields Appl. **61** (2020), 101582, 22.

[Poo04] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127.

[SS98] P. Sziklai and T. Szőnyi, *Blocking sets and algebraic curves*, Rend. Circ. Mat. Palermo (2) Suppl. **51** (1998), 71–86.

[Sző97a] T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, Finite Fields Appl. **3** (1997), no. 3, 187–202.

[Sző97b] _____ , *Some applications of algebraic curves in finite geometry and combinatorics*, Surveys in combinatorics, 1997 (London), 1997, pp. 197–236.

[The22] The Sage Developers, *SageMath, the Sage Mathematics Software System*, 2022. DOI 10.5281/zenodo.6259615.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, SANTA CLARA UNIVERSITY, 500 EL CAMINO REAL, USA 95053

Email address: sasgarli@scu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

Email address: dghioca@math.ubc.ca

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, 1984 MATHEMATICS ROAD, CANADA V6T 1Z2

Email address: kyleyip@math.ubc.ca