PROPORTION OF BLOCKING CURVES IN A PENCIL

SHAMIL ASGARLI, DRAGOS GHIOCA, AND CHI HOI YIP

ABSTRACT. Let $\mathcal{L}$ be a pencil of plane curves defined over $\mathbb{F}_q$ with no $\mathbb{F}_q$-points in its base locus. We investigate the number of curves in $\mathcal{L}$ whose $\mathbb{F}_q$-points form a blocking set. When the degree of the pencil is allowed to grow with respect to q, we show that the geometric problem can be translated into a purely combinatorial problem about disjoint blocking sets. We also study the same problem when the degree of the pencil is fixed.

1. INTRODUCTION

Throughout the paper, p denotes a prime, q denotes a power of p, and $\mathbb{F}_q$ denotes the finite field with q elements. Recall that a set of points $B \subseteq \mathbb{P}^2(\mathbb{F}_q)$ is a *blocking set* if every $\mathbb{F}_q$-line meets B. For example, a union of $q+1$ distinct $\mathbb{F}_q$-points on a line forms a blocking set. 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. Blocking sets have been studied extensively in finite geometry and design theory.

Inspired by the rich interaction between finite geometry and algebraic curves [SS98], the concept of blocking curves was formally introduced in [AGY22a]. Given a projective plane curve $C \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$, recall that $C(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points on C. We say that C is a *blocking curve* if $C(\mathbb{F}_q)$ is a blocking set; otherwise, it is *nonblocking*. Moreover, C is *nontrivially blocking* if $C(\mathbb{F}_q)$ is a nontrivial blocking set.

In our previous papers [AGY22a] and [AGY22b], we showed that irreducible blocking curves of low degree d (namely, satisfying $d^6 < q$) do not exist, and that blocking curves of high degree are rare. In other words, our past results suggest that a random curve over $\mathbb{F}_q$ is very likely to be nonblocking. These results rely on combinatorial properties of blocking sets as well as tools from algebraic geometry and arithmetic statistics. The main purpose of this paper is to understand a refined distribution of nonblocking curves by asking the following question:

Question 1.1. Let $\mathcal{L} = \langle F, G\rangle$ be a pencil of plane curves such that $\{F=0\}$ and $\{G=0\}$ have no common $\mathbb{F}_q$-points. Is there a quantitative lower bound for the number of curves in $\mathcal{L}$ defined over $\mathbb{F}_q$ which are nonblocking?

To elaborate further, let $\mathcal{L} = \langle F, G\rangle$ be a pencil that has no $\mathbb{F}_q$-points in its base locus. We refer to Example 3.1 which illustrates that the condition on the base locus is natural and necessary. Given such a pencil, consider the $q+1$ curves

$$C_{[s:t]} = \{sF + tG = 0\}$$

where $[s:t]$ ranges in $\mathbb{P}^1(\mathbb{F}_q)$. These curves will be called $\mathbb{F}_q$-*members* of $\mathcal{L} = \langle F, G\rangle$. Since $\mathcal{L}$ has no $\mathbb{F}_q$-points in its base locus, the sets of $\mathbb{F}_q$-rational points on these $q+1$ curves are pairwise disjoint and cover all the $\mathbb{F}_q$-points of the plane. Indeed, if $P \in \mathbb{P}^2(\mathbb{F}_q)$ is any $\mathbb{F}_q$-point, it belongs to a unique member $C_{[s:t]}$ with $[s:t] = [-G(P) : F(P)]$. In summary, the collection of sets

2020 *Mathematics Subject Classification.* Primary: 14H50, 51E21; Secondary: 14C21, 14N05, 14G15, 51E20.
Key words and phrases. Pencil, plane curves, blocking sets, finite field.

$\{C_{[s:t]}(\mathbb{F}_q)\}_{[s:t]\in\mathbb{P}^1(\mathbb{F}_q)}$ forms a partition of $\mathbb{P}^2(\mathbb{F}_q)$ into $q+1$ parts, with the understanding that some of the parts may be empty. We will say that the pencil $\mathcal{L}$ *induces* the partition $\{C_{[s:t]}(\mathbb{F}_q)\}_{[s:t]\in\mathbb{P}^1(\mathbb{F}_q)}$.

Let us explain a heuristic that suggests a plausible answer to Question 1.1. Since there are $q+1$ distinct $\mathbb{F}_q$-members of $\mathcal{L}$, and together they cover q^2+q+1 points, it follows that the average number of $\mathbb{F}_q$-points on a given $\mathbb{F}_q$-member of $\mathcal{L}$ is exactly:

$$\frac{q^2+q+1}{q+1} < q+1.$$

Since there does not exist a blocking set with less than $q+1$ points, it is immediate that $\mathcal{L}$ contains at least one nonblocking curve. Note that the averaging argument does not tell us whether or not the "median" number of points on a random $\mathbb{F}_q$-member in $\mathcal{L}$ is less than $q+1$. Nevertheless, it is natural to ask whether at least half of the $\mathbb{F}_q$-members in the pencil must be nonblocking. Making this last question slightly weaker, we may instead ask the following.

Question 1.2. Let $\mathcal{L} = \langle F, G\rangle$ be a pencil of plane curves such that $\{F=0\}$ and $\{G=0\}$ have no common $\mathbb{F}_q$-points. Does there exist a universal constant $c_0>0$ such that at least $c_0 q$ distinct $\mathbb{F}_q$-members of $\mathcal{L}$ are nonblocking?

Using Blokhuis' theorem [Blo94] that a nontrivial blocking set over $\mathbb{F}_p$ has at least $\frac{3}{2}(p+1)$, it can be shown that Question 1.2 has a positive answer when p is prime, and in fact, $c_0 = 1/3$ works in this case. See Remark 3.4 for further details.

However, Question 1.2 turns out to have a negative answer in general.

Theorem 1.3. *Let $q=p^n$ be a prime power with n even. There exists a pencil of plane curves over $\mathbb{F}_q$ with no $\mathbb{F}_q$-points in its base locus which contains only $\sqrt{q}$ many nonblocking curves.*

The key ingredient in the proof of Theorem 1.3 is to establish the connection between Question 1.2 and the question of determining the maximum number of disjoint blocking sets in $\mathbb{P}^2(\mathbb{F}_q)$, first studied by Beutelspacher and Eugeni [BE86]. The latter question can be formulated more generally and abstractly in the setting of hypergraph coloring; see [BMPS06] for related discussions. We will prove in Proposition 3.2 that every pencil with no $\mathbb{F}_q$-points in its base locus has at least $\sqrt{q}$ many nonblocking curves, so Theorem 1.3 is sharp.

In Question 1.2, the constant $c_0>0$ is required to be universal. If we allow the constant to depend on the degree of the curves, then Question 1.2 has a positive answer. More precisely, we will prove the following effective result.

Theorem 1.4. *Given a pencil of plane curves of degree $d\leq q$ in $\mathbb{P}^2$ defined over $\mathbb{F}_q$ with no $\mathbb{F}_q$-points in its base locus, at least $\frac{q+1}{d+1}$ distinct $\mathbb{F}_q$-members of the pencil are nonblocking curves.*

The inequality $d\leq q$ in the hypothesis is natural. Indeed, if $d>q$, then $0<\frac{q+1}{d+1}<1$, and the conclusion still holds, because we have already seen above that the pencil must have at least one nonblocking $\mathbb{F}_q$-member.

Outline of the paper. In Section 2, we show that every partition of the q^2+q+1 points of $\mathbb{P}^2(\mathbb{F}_q)$ into $q+1$ sets can be realized by a pencil of plane curves. This key result Proposition 2.1 allows us to prove our main Theorem 1.3 in Section 3. We discuss the case of fixed degree pencils and prove Theorem 1.4 in Section 4.

2. REALIZING PARTITIONS BY PENCILS OF CURVES

The goal of this section is to prove the following result, which shows that any partition of $\mathbb{P}^2(\mathbb{F}_q)$ into $q+1$ sets (where some sets could be empty) is induced by a pencil of plane curves.

Proposition 2.1. *Suppose $U_1, U_2, \ldots, U_{q+1}$ form a partition of $\mathbb{P}^2(\mathbb{F}_q)$. Then there exists a pencil of curves $\mathcal{L} = \langle F, G\rangle$ whose base locus has no $\mathbb{F}_q$-points such that $\mathcal{L}$ induces the partition $\{U_i\}_{i=1}^{q+1}$.*

The proof of Proposition 2.1 relies on two lemmas.

Lemma 2.2. *Given any $Q \in \mathbb{P}^2(\mathbb{F}_q)$, there exists a homogeneous polynomial $S_Q \in \mathbb{F}_q[x, y, z]$ of degree $3(q-1)$ such that $S_Q(Q) = 1$, while $S_Q(P) = 0$ for each point $P \neq Q$ in $\mathbb{P}^2(\mathbb{F}_q)$.*

Proof. Suppose $Q := [a_0 : b_0 : c_0] \in \mathbb{P}^2(\mathbb{F}_q)$. Without loss of generality, we may assume that $c_0 \neq 0$. Let L_1 and L_2 be two (distinct) $\mathbb{F}_q$-lines passing through the point Q; we let their equations be $\alpha_1 x+\beta_1+\gamma_1 z = 0$ and $\alpha_2 x+\beta_2 y+\gamma_2 z = 0$ for some $\alpha_i, \beta_i, \gamma_i \in \mathbb{F}_q$. Consider the homogeneous polynomial S_Q of degree $3(q-1)$ given by

$$S_Q(x, y, z) = z^{q-1} \cdot \left(z^{q-1} - (\alpha_1 x + \beta_1 y + \gamma_1 z)^{q-1}\right) \cdot \left(z^{q-1} - (\alpha_2 x + \beta_2 y + \gamma_2 z)^{q-1}\right).$$

Since z-coordinate of Q is nonzero by assumption, we get $S_Q(Q) = 1$. On the other hand, $S_Q(P) = 0$ for each point $P \neq Q$ in $\mathbb{P}^2(\mathbb{F}_q)$. Indeed, given such a point $P = [a_1 : b_1 : c_1]$, we have two cases: $c_1 = 0$ and $c_1 \neq 0$. If $c_1 = 0$, then $S_Q(P) = 0$ is immediate. If $c_1 \neq 0$, then P cannot be on both L_1 and L_2, and we again obtain $S_Q(P) = 0$. □

Remark 2.3. In Lemma 2.2, we arranged S_Q to have degree divisible by $q-1$. This allows us to view S_Q as a well-defined function $\mathbb{P}^2(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$. Indeed, if $[x_0 : y_0 : z_0]$ and $[x_1 : y_1 : z_1]$ represent the same point in $\mathbb{P}^2(\mathbb{F}_q)$, then $(x_1, y_1, z_1) = (\lambda x_0, \lambda y_0, \lambda z_0)$ for some $\lambda \in \mathbb{F}_q^*$. As a result, $S_Q(x_1, y_1, z_1) = \lambda^{3(q-1)} S_Q(x_0, y_0, z_0) = S_Q(x_0, y_0, z_0)$, confirming that S_Q is a well-defined function on $\mathbb{P}^2(\mathbb{F}_q)$.

Lemma 2.4. *For any function $f : \mathbb{P}^2(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ which is not identically zero, there exists a homogeneous polynomial $R_f \in \mathbb{F}_q[x, y, z]$ of degree $3(q-1)$ such that $R_f(a, b, c) = f([a : b : c])$ for each $[a : b : c] \in \mathbb{P}^2(\mathbb{F}_q)$.*

Proof. Borrowing the notation from Lemma 2.2, we set

$$R_f := \sum_{Q \in \mathbb{P}^2(\mathbb{F}_q)} f(Q) \cdot S_Q$$

which satisfies the desired condition. □

We have now gathered the tools to prove Proposition 2.1.

Proof of Proposition 2.1. Given a partition of $\mathbb{P}^2(\mathbb{F}_q)$ into $q+1$ sets $U_1, \ldots, U_{q+1}$, there exists a function $\varphi : \mathbb{P}^2(\mathbb{F}_q) \longrightarrow \mathbb{P}^1(\mathbb{F}_q)$ with the property that the preimages $\varphi^{-1}(Q)$ for the $q+1$ points $Q \in \mathbb{P}^1(\mathbb{F}_q)$ provide exactly the same partition of $\mathbb{P}^2(\mathbb{F}_q)$ as $U_1, \ldots U_{q+1}$. We can find two functions $f : \mathbb{P}^2(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ and $g : \mathbb{P}^2(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ such that for each $P \in \mathbb{P}^2(\mathbb{F}_q)$,

$$\varphi(P) = [f(P) : g(P)]. \tag{1}$$

By Lemma 2.4, we have two homogeneous polynomials R_f and R_g both of degree $3(q-1)$ which induce f and g, respectively.

Let $F = -R_g$ and $G = R_f$. We claim that the pencil $\mathcal{L} = \langle F, G\rangle$ induces the partition $U_1, \dots U_{q+1}$. First, $\mathcal{L}$ has no $\mathbb{F}_q$-points in its base locus since $f(P)$ and $g(P)$ cannot be zero simultaneously for any $P \in \mathbb{P}^2(\mathbb{F}_q)$ by (1). Next, for any $[u : v] \in \mathbb{P}^1$ and a point $P \in \mathbb{P}^2$, we have

$$uF(P) + vG(P) = 0 \iff [u : v] = [G(P) : -F(P)] = [f(P) : g(P)] = \varphi(P).$$

Thus, a given $\mathbb{F}_q$-point P belongs to the $\mathbb{F}_q$-member of the pencil $\mathcal{L}$ parametrized by $[u : v] \in \mathbb{P}^1(\mathbb{F}_q)$ if and only if $P \in \phi^{-1}([u : v])$. Consequently, the sets of $\mathbb{F}_q$-points contained in the $q + 1$ distinct $\mathbb{F}_q$-members of the pencil $\mathcal{L} = \langle F, G\rangle$ precisely correspond to the partition $U_1, \dots, U_{q+1}$. □

Remark 2.5. It is possible to generalize Proposition 2.1 where $U_1, U_2, ..., U_{q+1}$ together cover $\mathbb{P}^2(\mathbb{F}_q)$, although they are no longer assumed to be pairwise disjoint. In order to obtain a pencil of curves that induces the sets $U_1, U_2, ..., U_{q+1}$, it is necessary that the equality

$$U_i \cap U_j = B := \bigcap_{k=1}^{q+1} U_k$$

is satisfied for each $i \neq j$. Under this assumption, one can prove that there exists a pencil $\mathcal{L}$ of plane curves with $\mathbb{F}_q$-members $C_1, C_2, ..., C_{q+1}$ such that $C_i(\mathbb{F}_q) = U_i$ for each $1 \leq i \leq q + 1$. The proof is almost identical to the current proof of Proposition 2.1. We start by picking

$$\varphi \colon \mathbb{P}^2(\mathbb{F}_q) \setminus B \longrightarrow \mathbb{P}^1(\mathbb{F}_q)$$

so that the preimages $\varphi^{-1}(\alpha_i)$ of the points $\alpha_1, ..., \alpha_{q+1}$ in $\mathbb{P}^1(\mathbb{F}_q)$ coincide with the pairwise disjoint sets $U_i \setminus B$ for $i = 1, .., q + 1$. By using Lemma 2.4, we can find homogeneous polynomials F and G which both vanish on B such that the pencil $\mathcal{L} = \langle F, G\rangle$ satisfies the desired properties.

3. Lower bounds on the number of nonblocking curves

The averaging argument presented in the introduction showed that if a pencil of plane curves has no $\mathbb{F}_q$-points in its base locus, there must be at least one nonblocking curve in the pencil. We explain what happens when the hypothesis on the base locus is dropped. If the set of $\mathbb{F}_q$-points of the base locus is itself a blocking set, then clearly all the curves in the pencil are blocking. Additional examples of pencils whose $\mathbb{F}_q$-members are all blocking can be constructed using the explicit families of blocking curves in [AGY22a, Proposition 6.1]; in such pencils, the base locus may have a large number of $\mathbb{F}_q$-points. It may be tempting to believe that there should be at least some nonblocking curves if the base locus is small. However, we will now exhibit a pencil $\mathcal{L}$ of plane curves of degree $d \geq 2$ over $\mathbb{F}_q$ containing *exactly one* $\mathbb{F}_q$-point in its base locus such that every $\mathbb{F}_q$-member of $\mathcal{L}$ is a blocking curve. This example shows that the hypothesis that the base locus has no $\mathbb{F}_q$-points cannot be relaxed.

Example 3.1. Let $m = \max\{0, q-3\}$ and consider the polynomial $H(x, y, z)$ of degree q^2+q+1 which is the product of all linear polynomials $ax + by + cz$, where $[a : b : c] \in \mathbb{P}^2(\mathbb{F}_q)$. Let

$$F(x, y, z) = x^m H(x, y, z) + y^{q^2+q+1+m}$$

and

$$G(x, y, z) = x^m H(x, y, z) + z^{q^2+q+1+m}.$$

Then the only $\mathbb{F}_q$-point in the intersection of $\{F = 0\}$ and $\{G = 0\}$ is $[1 : 0 : 0]$. Thus, $\mathcal{L} = \langle F, G\rangle$ is a pencil of plane curves with exactly one $\mathbb{F}_q$-point in its base locus. However, for each $[a:b] \in \mathbb{P}^1(\mathbb{F}_q)$, the curve $C_{[a:b]} = \{aF + bG = 0\}$ intersects any given $\mathbb{F}_q$-line L at some $\mathbb{F}_q$-point. Indeed, specializing $aF + bG = 0$ along the line L yields to

$$ay^{q^2+q+1+m} + bz^{q^2+q+1+m} = 0. \tag{2}$$

Since m was chosen so that $\gcd(q-1, q^2+q+1+m) = 1$, the map $t \mapsto t^{q^2+q+1+m}$ is an automorphism of the cyclic group $(\mathbb{F}_q^*, \cdot)$. Thus, regardless of the line L along which we specialize, the equation (2) has a nonzero solution (that is, not both y and z are zero) in $\mathbb{F}_q$ for each $[a:b] \in \mathbb{P}^1(\mathbb{F}_q)$. Consequently, every $\mathbb{F}_q$-member of $\mathcal{L}$ is a blocking curve.

An alternative construction can be carried out by using the generalized version of Proposition 2.1 (see Remark 2.5) where $U_1, U_2, ..., U_{q+1}$ consist of $\mathbb{F}_q$-points of $q+1$ distinct lines passing through a common point. The pencil produced using that method will have degree $3(q-1)$.

We have seen that having even a single $\mathbb{F}_q$-point in the base locus may result in all of the $\mathbb{F}_q$-members to be blocking curves. Thus, for the remainder of the paper, we will work under the hypothesis that there are no $\mathbb{F}_q$-points in the base locus of a given pencil. Our first quantitative lower bound on the number of nonblocking curves is implicit in the finite geometry literature [BE86, Theorem 2.2]. We include a simple proof for a sake of completeness; the ideas and notation used in this proof will also be needed in the remarks that follow.

Proposition 3.2. *Every pencil of plane curves over $\mathbb{F}_q$ with no $\mathbb{F}_q$ points in its base locus has at least $\sqrt{q}$ many $\mathbb{F}_q$-members which are nonblocking.*

Proof. Let $\mathcal{L} = \langle F, G \rangle$ be a pencil of plane curves with no $\mathbb{F}_q$-members in its base locus. If $\mathcal{L}$ has an $\mathbb{F}_q$-member C whose $\mathbb{F}_q$-rational points which is a trivial blocking set, then there exists an $\mathbb{F}_q$-line L such that $L(\mathbb{F}_q) \subseteq C(\mathbb{F}_q)$. In this case, the other q members of $\mathcal{L}$ will be nonblocking by virtue of being disjoint from $L(\mathbb{F}_q)$. Thus, we may assume that each $\mathbb{F}_q$-member of the pencil is not trivially blocking.

Suppose we have m blocking and $q+1-m$ nonblocking $\mathbb{F}_q$-members of $\mathcal{L}$. Since a nontrivial blocking set has at least $q + \sqrt{q} + 1$ points [Bru71], the following inequality holds:

$$m(q + \sqrt{q} + 1) \leq \sum_{\substack{C \text{ is } \mathbb{F}_q\text{-member of } \mathcal{L} \\ C \text{ is blocking}}} \#C(\mathbb{F}_q) \leq \sum_{C \text{ is } \mathbb{F}_q\text{-member of } \mathcal{L}} \#C(\mathbb{F}_q) = q^2 + q + 1.$$

It follows that,

$$m \leq \frac{q^2 + q + 1}{q + \sqrt{q} + 1} = q - \sqrt{q} + 1$$

Thus, the number of nonblocking $\mathbb{F}_q$-members is $q + 1 - m \geq \sqrt{q}$, as desired. □

As a complement to the previous proposition, we now present a quick proof of Theorem 1.3 which guarantees the existence of a pencil which has exactly $\sqrt{q}$ many nonblocking members. 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 well-known that Baer subplanes are blocking sets.

Proof of Theorem 1.3. Since q is a square, it is known that that $\mathbb{P}^2(\mathbb{F}_q)$ can be partitioned into

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

Baer subplanes [Hir79, Theorem 4.3.6]. Now, Proposition 2.1 implies that we can find a pencil of curves which has exactly $\sqrt{q}$ many $\mathbb{F}_q$-members which are nonblocking. □

Remark 3.3. When q is a square, we have seen that the number of nonblocking curves in a pencil must be at least $\sqrt{q}$, and this lower bound is sharp. When q is not a square, we know each nontrivial blocking set has size at least $q+1+cq^{2/3}$ [BSS99], so the same argument in Proposition 3.2 can be adapted to show that there are at least $c'q^{2/3}$ many nonblocking $\mathbb{F}_q$-members in any pencil with no $\mathbb{F}_q$-points in its base locus. This can be seen by mimicking the same proof as in Proposition 3.2 to get the following upper bound on the number of blocking curves in the given pencil:

$$\frac{q^2+q+1}{q+1+q^{2/3}} = \frac{q^2+q-q^{4/3}}{q+1+q^{2/3}} + \frac{q^{4/3}}{q+1+q^{2/3}} \approx q+1-q^{2/3} + \frac{q^{4/3}}{q+1+q^{2/3}} \approx q+1-q^{2/3}+q^{1/3}.$$

Remark 3.4. When $q = p$ is prime, we can improve the lower bound in Proposition 3.2 significantly by relying on Blokhuis' theorem that a nontrivial blocking set in $\mathbb{P}^2(\mathbb{F}_p)$ has at least $\frac{3}{2}(p+1)$ points [Blo94]. By imitating the proof of Proposition 3.2, we see that the number of blocking curves satisfies $m \leq \frac{p^2+p+1}{\frac{3}{2}(p+1)} < \frac{2}{3}(p+1)$. It follows that the number of nonblocking curves is $p+1-m \geq \frac{1}{3}(p+1)$, thereby answering Question 1.2 affirmatively in the case when $q = p$ is a prime. On the other hand, it is possible to construct $(1/3 - o(1))p$ disjoint blocking sets in $\mathbb{P}^2(\mathbb{F}_p)$ [BMPS06]. Thus, Proposition 2.1 implies the existence of a pencil with at least $1/3$ members being blocking, or equivalently, at most $2/3$ members are nonblocking. It is conjectured by Kriesell that $\mathbb{P}^2(\mathbb{F}_q)$ can be partitioned into $\lfloor q/2 \rfloor$ blocking sets (he verified the conjecture for $q \leq 8$) [BMPS06, Page 150], so the best possible constant in Question 1.2 is conjecturally $1/2$ (when $q = p$ is prime).

Remark 3.5. Szőnyi [Sző97, Theorem 5.7] showed if $q = p^2$ with p prime, a nontrivial blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ that avoids Baer subplanes has size at least $3(q+1)/2$. Note that this result is analogous to Blokhuis' result over $\mathbb{F}_p$ with p prime. Let us explain how this observation helps us answer Question 1.2 affirmatively in the case $q = p^2$ for certain pencils.

We say that a pencil of curves over $\mathbb{F}_q$ is *generic* if the number of singular members (defined over the algebraic closure $\overline{\mathbb{F}_q}$) is finite. The terminology is justified by the fact that a generic line (over $\overline{\mathbb{F}_q}$) in the parameter space of plane curves of degree d meets the discriminant hypersurface in finitely many points. It follows that a given pencil $\mathcal{L}$ is either generic or every $\overline{\mathbb{F}_q}$-member of $\mathcal{L}$ is a singular curve. Thus, non-generic pencils are extremely special. When $d = o(\sqrt{q})$, we can show that for any generic pencil, at least $(1/3 - o(1))q$ members that are not blocking. We may assume that no curve in the pencil is trivially blocking, for otherwise, q of the curves are nonblocking. For each generic pencil there are at most $3(d-1)^2 = o(q)$ many singular curves by [EH16, Proposition 7.4]. Note for each smooth curve in the pencil, by Bézout's theorem, it does not contain a Baer subplane (otherwise, there is a line that intersects at the curve with at least $\sqrt{q}+1 > d$ points). Thus, if a smooth member in the pencil is blocking, then it has size at least $3(q+1)/2$; therefore, there are at most $2q/3$ smooth blocking curves in our pencils. Hence, we have more than $q/3 - 3(d-1)^2 = (1/3 - o(1))q$ nonblocking curves in our pencil.

4. Proof of Theorem 1.4

In this section, we will show that Question 1.2 has a positive answer if the constant c_0 is allowed to depend on d. More precisely, we will prove Theorem 1.4, which guarantees that at least $\frac{1}{d+1}$ fraction of the $\mathbb{F}_q$-members of a given pencil are nonblocking.

As a preparation, we start by proving a lower bound on the number of $\mathbb{F}_q$-rational points on a blocking plane curve. The following lemma is implicitly contained in [AGY22a, Section 2.5]. For the sake of completeness, we present a self-contained proof.

Lemma 4.1. *Suppose C is a plane curve of degree d defined over $\mathbb{F}_q$. If $C(\mathbb{F}_q)$ is a nontrivial blocking set, then $\#C(\mathbb{F}_q) > q + \frac{q+\sqrt{q}}{d}$.*

Proof. Let t_i denote the number of $\mathbb{F}_q$-lines L such that $C \cap L$ has exactly i distinct $\mathbb{F}_q$-points. Let $N = \#C(\mathbb{F}_q)$ denote the number of $\mathbb{F}_q$-points of C. Since C is nontrivially blocking, it cannot contain any $\mathbb{F}_q$-line as a component. Thus, $t_0 = 0$, and $t_i = 0$ for $i > d$ by Bézout's theorem. Moreover, a standard double counting argument on point-line incidences (see for example [AGY22a, Lemma 2.9]) leads to the following three identities:

$$\sum_{i=1}^{d} t_i = q^2 + q + 1, \qquad \sum_{i=1}^{d} i \cdot t_i = (q+1)N, \qquad \sum_{i=2}^{d} \binom{i}{2} \cdot t_i = \binom{N}{2}.$$

By combining the first two identities, we obtain

$$q^2 + q + 1 = (q+1)N - \sum_{i=2}^{d} (i-1)t_i, \tag{3}$$

while the third identity implies

$$\sum_{i=2}^{d} (i-1)t_i \geq \frac{N(N-1)}{d}. \tag{4}$$

The inequalities (3) and (4) together yield,

$$q^2 + q + 1 \leq (q+1)N - \frac{N(N-1)}{d}. \tag{5}$$

Since $C(\mathbb{F}_q)$ is a *nontrivial* blocking set, we have $N \geq q + \sqrt{q} + 1$ by [Bru71]. Now, the inequality (5) implies,

$$(q+1)N \geq q^2 + q + 1 + \frac{(q+\sqrt{q}+1)(q+\sqrt{q})}{d} > (q+1)q + \frac{(q+1)(q+\sqrt{q})}{d}.$$

It follows that $N > q + \frac{q+\sqrt{q}}{d}$, as desired. □

Remark 4.2. One can obtain a slightly stronger conclusion $N > \left(\frac{d}{d-1}\right) q \cdot (1 + o(1))$ by analyzing the inequality (5) more carefully.

We now proceed with the proof of Theorem 1.4 on the number of nonblocking curves in a pencil of fixed degree.

Proof of Theorem 1.4. Given a pencil $\mathcal{L}$ with no $\mathbb{F}_q$-points in its base locus, suppose m of the $\mathbb{F}_q$-members are blocking and $q + 1 - m$ of the $\mathbb{F}_q$-members are nonblocking. If any $\mathbb{F}_q$-member of $\mathcal{L}$ is trivially blocking, then applying the same argument as at the beginning of Proposition 3.2, we see that the other q members of the pencil are nonblocking. So, we may assume that all the blocking $\mathbb{F}_q$-members are nontrivially blocking.

By applying Lemma 4.1, we obtain the following inequality:

$$m\left(\frac{qd+q+\sqrt{q}}{d}\right) < \sum_{\substack{C \text{ is } \mathbb{F}_q\text{-member of } \mathcal{L} \\ C \text{ is blocking}}} \#C(\mathbb{F}_q) \leq \sum_{C \text{ is } \mathbb{F}_q\text{-member of } \mathcal{L}} \#C(\mathbb{F}_q) = q^2+q+1.$$

Therefore, using the hypothesis $d \leq q$, we obtain

$$m \leq \frac{(q^2+q+1)d}{qd+q+\sqrt{q}} = \frac{(q+1)(q+\frac{1}{q+1})d}{(d+1)(q+\frac{\sqrt{q}}{d+1})} \leq \frac{d}{d+1}(q+1).$$

We conclude that the number of nonblocking $\mathbb{F}_q$-members of the pencil $\mathcal{L}$ is $q+1-m \geq \frac{q+1}{d+1}$. □

Remark 4.3. The hypothesis $d \leq q$ in Theorem 1.4 is natural. However, when $\sqrt{q} \leq d \leq q$, Theorem 1.4 only guarantees $\frac{q+1}{\sqrt{q}+1} = \sqrt{q}-1$ many nonblocking curves, which was already proved in Proposition 3.2. For Theorem 1.4 to yield more refined results, we would need to assume $d < \sqrt{q}$.

On the other hand, if d gets too small compared to q, namely, $d < q^{1/6}$ then we can refine Theorem 1.4 for generic pencils (as defined in Remark 3.5). More precisely, when $q > d^6$, then the lower bound in Theorem 1.4 can be improved significantly so that the answer to Question 1.2 would be positive with $c_0 = 1-o(1)$. This follows from the observation that the number of singular members in a generic pencil is at most $3(d-1)^2 = o(q)$ as stated in Remark 3.5, and our earlier result that a smooth member in the pencil is not blocking whenever $q > d^6$ [AGY22a, Theorem 1.2]. We also mention that there are other refined sufficient conditions on nonblocking smooth curves in [AGY22a].

Acknowledgements

The second author is supported by an NSERC Discovery grant. The third author is supported by a doctoral fellowship from the University of British Columbia.

References

[AGY22a] 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.

[AGY22b] ———, *Most plane curves over finite fields are not blocking*, arXiv e-prints (2022), available at https://arxiv.org/abs/2211.08523.

[BE86] A. Beutelspacher and F. Eugeni, *On n-fold blocking sets*, Combinatorics '84 (Bari, 1984), 1986, pp. 31–38.

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

[BMPS06] J. Barát, S. Marcugini, F. Pambianco, and T. Szőnyi, *Note on disjoint blocking sets in Galois planes*, J. Combin. Des. **14** (2006), no. 2, 149–158.

[Bru71] A. Bruen, *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.

[EH16] D. Eisenbud and J. Harris, *3264 and all that—a second course in algebraic geometry*, Cambridge University Press, Cambridge, 2016.

[Hir79] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1979.

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

[Sző97] T. Szőnyi, *Blocking sets in Desarguesian affine and projective planes*, Finite Fields Appl. **3** (1997), no. 3, 187–202.

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