# BLOCKING SETS FROM A UNION OF PLANE CURVES

SHAMIL ASGARLI, DRAGOS GHIOCA, AND CHI HOI YIP

ABSTRACT. Motivated by a question of Erdős on blocking sets in a projective plane that intersect every line only a few times, several authors have used unions of algebraic curves to construct such sets in $\mathbb{P}^2(\mathbb{F}_q)$. In this paper, we provide new constructions of blocking sets in $\mathbb{P}^2(\mathbb{F}_q)$ from a union of geometrically irreducible curves of a fixed degree $d$. We also establish lower bounds on the number of such curves required to form a blocking set. Our proofs combine tools from arithmetic geometry and combinatorics.

## 1. INTRODUCTION

Throughout the paper, $p$ denotes a prime, $q$ denotes a power of $p$, $\mathbb{F}_q$ denotes the finite field with $q$ elements, and $\overline{\mathbb{F}_q}$ denotes the algebraic closure of $\mathbb{F}_q$. A set of points $B \subseteq \mathbb{P}^2(\mathbb{F}_q)$ is a *blocking set* if it intersects every $\mathbb{F}_q$-line. A blocking set is called *trivial* if it contains all $q+1$ points of an $\mathbb{F}_q$-line; otherwise, it is *nontrivial*. The smallest trivial blocking sets are lines themselves, consisting of $q+1$ points.

The study of blocking sets is a central topic in finite geometry and design theory [7, 18]. In this paper, we study blocking sets arising from a union of plane curves. Our motivation comes from the literature on a question of Erdős [12] and from our previous work [3], which treated the case of a single irreducible plane curve.

Inspired by questions related to intersection properties of set families, Erdős [12] considered the case in which the set family consists of the lines in a projective plane; this naturally led him to study blocking sets that meet each line only a few times.[1] More precisely, let $k = k(n)$ denote the least positive integer such that in any projective plane of order $n$, there exists a blocking set $B$ of points such that $|B \cap L| < k$ for every line $L$. Erdős asked whether $k(n)$ is bounded by a universal constant. Using the probabilistic method, Erdős–Silverman–Stein [12] showed that for any constant $c > 2e$, we have $k(n) < c \log n$ for all sufficiently large $n$. In the same paper, they also provided a constructive approach to show $k(n) < n - c'\sqrt{n}$ for some absolute constant $c' > 0$. For the exposition of how the approaches used in [12] can be extended to construct blocking sets and other objects in finite geometry, we refer to the surveys by Szőnyi [21] and Gács–Szőnyi [13].

Erdős' question is still wide open, and much of the subsequent work has focused on the case of a projective plane $\mathbb{P}^2(\mathbb{F}_q)$ over a finite field of order $q$. In this setting, the algebraic and geometric structure of projective Galois planes provides tools unavailable for general projective planes. In particular, it is natural to look for constructions of blocking sets arising from algebraic curves; see, for example, [1, 21, 22, 23]. This is partly because the number of intersections between irreducible plane curves and lines is controlled by Bézout's theorem. We introduce the following definition to formalize the construction of blocking sets from collections of plane curves.

2020 *Mathematics Subject Classification.* Primary 14N05, 51E21; Secondary 14C21, 14H50, 14G15.
*Key words and phrases.* blocking set, plane curve, conic.

[1] This question is attributed to Erdős in the introduction of the paper by Erdős–Silverman–Stein [12].

**Definition 1.1.** A blocking set $B$ in $\mathbb{P}^2(\mathbb{F}_q)$ is *constructed from a union of plane curves* if $B = \bigcup_{i=1}^{\ell} C_i(\mathbb{F}_q)$ for some plane curves $C_1, \dots, C_\ell$ defined over $\mathbb{F}_q$, where $C_i$ is *geometrically irreducible* (that is, irreducible over $\overline{\mathbb{F}_q}$) and has degree $d_i = \deg(C_i) > 1$ for each $i$. We also say that $C_1, \dots, C_\ell$ form a *blocking family of degree* $(d_1, \dots, d_\ell)$.

The hypothesis $d_i > 1$ in Definition 1.1 is necessary to produce *nontrivial* blocking sets. The geometric irreducibility condition is also natural, as one could otherwise replace a reducible curve with its irreducible components. Moreover, if $C_i$ were irreducible over $\mathbb{F}_q$, but not geometrically irreducible, a standard application of Bézout's theorem shows that $|C_i(\mathbb{F}_q)| \le \frac{d_i^2}{4}$ (see, for example, [3, Lemma 3.1]); consequently, $C_i(\mathbb{F}_q)$ blocks at most $\frac{d_i^2}{4}(q+1)$ lines (which is not efficient for constructing blocking sets). In contrast, geometrically irreducible curves have $q + O(\sqrt{q})$ points by the Hasse–Weil bound (see [6] for a version that applies to singular curves).

In our previous work [2, 3, 4, 5], we studied blocking sets arising from points of an irreducible plane curve, which corresponds to the case $\ell = 1$. In particular, we showed in [3] that irreducible blocking curves of low degree $d \ge 2$ (specifically, $d < q^{1/6}$) do not exist; we also provided various constructions of irreducible blocking curves.

Let $B$ be a blocking set constructed from $C_1, \dots, C_\ell$ as in Definition 1.1. By Bézout's theorem, we have $|B \cap L| \le \sum_{i=1}^{\ell} \deg(C_i)$ for each $\mathbb{F}_q$-line $L$. This implies $k \le \sum_{i=1}^{\ell} \deg(C_i)$ for Erdős' question, though this bound is often not sharp. Next, we discuss past work using such constructions and state our new contributions.

Let $q$ be an odd prime power. Abbott and Liu [1] constructed a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ from a union of around $\log_2 q$ conics. For any constant $c > 2/\log 2$, their construction produces a set with $k < c \log q$ in Erdős' question (while their bound $c > 2/\log 2$ improves $c > 2e$ from Erdős–Silverman–Stein [12], it is specific to projective Galois planes). A similar construction was independently discovered by Ughi [23]. She also proved that the number of nonsingular (equivalently, geometrically irreducible) conics required to form a blocking set must tend to infinity as $q \to \infty$. In a related work, Szőnyi [22] constructed minimal blocking sets in $\mathbb{P}^2(\mathbb{F}_q)$ from a subset of a pencil of conics $C_a$ parametrized by $a \in \mathbb{F}_q$; the values of $a$ that realize minimal blocking sets correspond to maximal independent sets in the Paley graph over $\mathbb{F}_q$ (here $q \equiv 1 \pmod 4$). In the same paper, he also deduced that at least $c \log q$ conics from this specific pencil $\{C_a\}_{a \in \mathbb{F}_q}$ are required to form a blocking set. Our first result shows that this logarithmic lower bound holds for a blocking set formed by *any* collection of geometrically irreducible conics.

**Theorem 1.2.** *Let $q$ be an odd prime power. There is a constant $c_0 > 0$ such that no blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ can be constructed from a union of fewer than $c_0 \log q$ conics.*

For an odd prime power $q$, let $f(q)$ be the minimum integer $\ell$ such that there is a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ constructed from $\ell$ conics. By the discussion above, we know $c_1 \log q \le f(q) \le c_2 \log q$ for some absolute constants $c_1, c_2 > 0$. Determining an asymptotically sharp bound on $f(q)$ seems out of reach.

As we were finalizing the paper, we discovered that Szőnyi [21] proved an analogous lower bound for blocking sets in inversive planes constructed from a union of circles. In the final remark of the same paper, he mentioned that the same proof idea applies to conics in $\mathbb{P}^2(\mathbb{F}_q)$, so we believe that Theorem 1.2 is known to some experts. We will present our own proof of Theorem 1.2 in Section 2, and briefly explain Szőnyi's suggested proof in Remark 2.3.

The hypothesis that $q$ is odd in Theorem 1.2 is necessary. Indeed, Illés, Szőnyi, and Ferenc [15] showed that for Erdős' question in $\mathbb{P}^2(\mathbb{F}_{2^r})$, the bound $k \le 6$ holds if $r$ is even, and $k \le 7$ holds if $r$ is odd. Their construction still employs a union of nonsingular conics.

For curves of higher degree, our next result generalizes Ughi's result [23, Proposition 2] on the number of geometically irreducible conics needed to form a blocking set in odd characteristic.

**Theorem 1.3.** *Let $d \ge 3$. Let $\ell(q)$ be the minimum integer $\ell$ such that there exists a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ constructed from a union of $\ell$ plane curves each having degree at most $d$. Let $\mathcal{Q}_d$ be the set of prime powers $q$ such that $p = \mathrm{char}(\mathbb{F}_q) > d$. Then for $q \in \mathcal{Q}_d$, we have $\ell(q) \to \infty$ as $q \to \infty$.*

We prove Theorem 1.3 in Section 3. The key ingredient of the proof is a version of Chebotarev density theorem due to Entin [11]. The hypothesis $p = \mathrm{char}(\mathbb{F}_q) > d$ in Theorem 1.3 is necessary. Indeed, Bruen and Fisher [9] found a blocking set in $\mathbb{P}^2(\mathbb{F}_{3^r})$ formed by taking a union of geometrically irreducible cubic curves and showing that $k \le 5$ for Erdős' question. More generally, Boros [8] proved that if $q = p^r$ with a prime $p \ge 3$, then $k \le p + 2$ for Erdős' question; this was achieved by considering the union of two carefully chosen geometrically irreducible degree $p$ curves together with a single point. Thus, the hypothesis $p > d$ in Theorem 1.3 is sharp.

Our final result is a counterpart to these lower bounds by demonstrating that a blocking family can indeed be formed from approximately $c_d \log q$ geometrically irreducible curves of degree $d$.

**Theorem 1.4.** *Let $d \ge 3$. There exists a constant $c_d > 0$ such that for any prime power $q$ and any integer $\ell \ge c_d \log q$, there exists a blocking family of degree $\underbrace{(d, d, \ldots, d)}_{\ell \text{ times}}$ over $\mathbb{F}_q$.*

We will give two proofs of Theorem 1.4, one probabilistic in Section 4 and one through explicit equations in Section 5. In the first proof, we use a randomized construction which produces a better constant, namely, $c_d = 4 - o(1)$ as $q \to \infty$. The randomized construction is also more flexible, as it can produce multiple blocking sets; see Remark 4.5. The more precise statement for the second proof appears as Theorem 5.1, which gives $c_d = O(d)$. On the other hand, the second proof has the advantage that, when $\gcd(d, q-1) > 1$ and we restrict to a certain pencil of curves, it is optimal up to a constant multiplicative factor; see the end of Section 5 for discussion.

## 2. Constructions from conics

In this section, we prove Theorem 1.2. Throughout the section, we assume that $q$ is an odd prime power.

A key ingredient in our proof is an effective version of the Lang–Weil bound [16]. A standard application of Weil's bound gives an asymptotic formula for the number of $x \in \mathbb{F}_q$ such that $f_i(x)$ is a square in $\mathbb{F}_q$ for all $i$, where $f_1, f_2, \ldots, f_\ell \in \mathbb{F}_q[x]$ are "independent"; see, for example, [22, Lemma 1]. Recently, Slavov [19] extended this result to multivariable polynomials with the help of an explicit version of the Lang–Weil bound by Cafure and Matera [10]. The following lemma is a special case of his result [19, Theorem 3 and Remark 13].

**Lemma 2.1** (Slavov)**.** *Let $n, \ell, d$ be positive integers and $q$ be an odd prime power. Let $f_1, f_2, \ldots, f_\ell$ be polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$ with degree $d$. Suppose that for any nonempty subset $I \subseteq \{1, 2, \ldots, \ell\}$, the product $\prod_{i \in I} f_i$ is not a constant multiple of the square of a polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$. Then the number of $(a_1, a_2, \ldots, a_n) \in \mathbb{F}_q^n$ such that $f_i(a_1, a_2, \ldots, a_n)$ is a nonzero square in $\mathbb{F}_q$ for all $1 \le i \le \ell$ is*

$$\frac{q^n}{2^\ell} + O((2d)^{2\ell} q^{n-1/2} + (2d)^{13\ell/3} q^{n-1}),$$

*where the implied constant in the error term is absolute.*

Our proof also uses the concept of dual curves. Recall that the points of the *dual projective plane* $(\mathbb{P}^2)^*$ correspond to lines in $\mathbb{P}^2$. Given a geometrically irreducible plane curve $C$, the *dual curve* $C^* \subset (\mathbb{P}^2)^*$ parametrizes tangent lines to $C$. The set of $\mathbb{F}_q$-points on this curve, $C^*(\mathbb{F}_q)$, therefore represents those $\mathbb{F}_q$-lines that are tangent to $C$ at some point $P \in C(\overline{\mathbb{F}_q})$.

The proof of Theorem 1.2 combines these two tools.

*Proof of Theorem 1.2.* Suppose $\{C_1, C_2, \dots, C_\ell\}$ is a collection of geometrically irreducible conics that block all lines in $\mathbb{P}^2(\mathbb{F}_q)$. In particular, the union of these conics intersects with lines of the form $bx + cy - z = 0$ with $b, c \in \mathbb{F}_q$. The following claim provides a simple criterion for whether such a line is skew to a given conic.

**Claim 2.2.** *Let $C$ be a geometrically irreducible conic defined over $\mathbb{F}_q$:*

$$C : a_{200}x^2 + a_{020}y^2 + a_{002}z^2 + a_{110}xy + a_{101}xz + a_{011}yz = 0.$$

*Consider the polynomial $D(\alpha, \beta) \in \mathbb{F}_q[\alpha, \beta]$ defined by:*

$$D = (2a_{002}\alpha\beta + a_{110} + a_{101}\beta + a_{011}\alpha)^2 - 4(a_{200} + a_{002}\alpha^2 + a_{101}\alpha)(a_{020} + a_{002}\beta^2 + a_{011}\beta).$$

*Then for each $b, c \in \mathbb{F}_q$, $C$ does not intersect the line $L\colon bx + cy - z = 0$ at an $\mathbb{F}_q$-point provided the following two conditions hold:*

*(1)* $(a_{200} + a_{002}b^2 + a_{101}b)(a_{020} + a_{002}c^2 + a_{011}c) \neq 0$.
*(2)* $D(b, c)$ *is a non-square in* $\mathbb{F}_q$.

*In particular, for all but at most $4q$ pairs $(b, c) \in \mathbb{F}_q \times \mathbb{F}_q$, the line $L\colon bx + cy - z = 0$ is skew to $C$ if $D(b, c)$ is a non-square in $\mathbb{F}_q$.*

*Proof of claim.* First, note that the equation $a_{200} + a_{002}\alpha^2 + a_{101}\alpha = 0$ has at most two solutions in $\mathbb{F}_q$. Otherwise, the polynomial in $\alpha$ would be identically zero, so $a_{200} = a_{002} = a_{101} = 0$; in this case $C$ is reducible with a factor of $y$. Similarly, the equation $a_{020} + a_{002}\beta^2 + a_{011}\beta = 0$ has at most two solutions in $\mathbb{F}_q$. Thus, condition (1) holds for all but at most $4q$ pairs $(b, c) \in \mathbb{F}_q \times \mathbb{F}_q$.

Next, we compute $C \cap L$. Substituting $z = bx + cy$ into the equation of $C$ gives:

$$a_{200}x^2 + a_{020}y^2 + a_{002}(bx + cy)^2 + a_{110}xy + a_{101}x(bx + cy) + a_{011}y(bx + cy) = 0,$$

which simplifies to

$$(a_{200}+a_{002}b^2+a_{101}b)x^2+(2a_{002}bc+a_{110}+a_{101}c+a_{011}b)xy+(a_{020}+a_{002}c^2+a_{011}c)y^2 = 0. \quad (2.1)$$

If $(a_{200} + a_{002}b^2 + a_{101}b)(a_{020} + a_{002}c^2 + a_{011}c) \neq 0$, then equation (2.1) has a solution over $\mathbb{F}_q$ only when its discriminant

$$(2a_{002}bc + a_{110} + a_{101}c + a_{011}b)^2 - 4(a_{200} + a_{002}b^2 + a_{101}b)(a_{020} + a_{002}c^2 + a_{011}c)$$

is a square in $\mathbb{F}_q$. This proves the claim. ∎

For each $1 \leq i \leq \ell$, let $D_i(\alpha, \beta)$ be the corresponding polynomial of the conic $C_i$ defined in the above claim. A point $[t_0 : t_1 : t_2] \in (\mathbb{P}^2)^*$ in the dual plane corresponds to the line with equation $t_0x+t_1y+t_2z = 0$ in $\mathbb{P}^2$. From the theory of dual curves, $D_i(\alpha, \beta) = 0$ represents the affine model of the dual curve $C_i^*$. More precisely, $\{D_i(\alpha, \beta) = 0\} \subseteq \mathbb{A}^2_{\alpha,\beta}$ is the restriction of $C_i^*$ to the affine chart $t_2 = 1$. In particular, $D_i \in \mathbb{F}_q[\alpha, \beta]$ is an irreducible polynomial of degree 2. Moreover, for $1 \leq i < j \leq \ell$, $C_i$ and $C_j$ are distinct conics, so their dual curves are also distinct, that is, $C_i^*$ and $C_j^*$ are distinct and thus $D_i$ and $D_j$ are distinct in the sense that $D_j \neq \lambda D_i$ for any $\lambda \in \mathbb{F}_q$.

Therefore, for any nonempty subset $I \subseteq \{1, 2, \ldots, \ell\}$, the polynomial $\prod_{i \in I} D_i$ is not a constant multiple of the square of a polynomial in $\mathbb{F}_q[\alpha, \beta]$.

Thus, Lemma 2.1 implies that the number of pairs $(b, c) \in \mathbb{F}_q \times \mathbb{F}_q$ such that $D_i(b, c)$ is a nonsquare for all $1 \leq i \leq \ell$ is at least

$$\frac{q^2}{2^\ell} - K(4^{2\ell} q^{3/2} + 4^{13\ell/3} q),$$

where $K$ is an absolute constant. It follows from Claim 2.2 that the number of pairs $(b, c) \in \mathbb{F}_q \times \mathbb{F}_q$ for which the line $L\colon bx + cy - z = 0$ is simultaneously skew to the conics $C_1, C_2, \ldots, C_\ell$ is at least

$$\frac{q^2}{2^\ell} - K(4^{2\ell} q^{3/2} + 4^{13\ell/3} q) - 4q\ell;$$

however, by the blocking set assumption, no such line exists. It follows that

$$\frac{q^2}{2^\ell} - K(4^{2\ell} q^{3/2} + 4^{13\ell/3} q) - 4q\ell \leq 0,$$

that is, $\ell \geq c \log q$ for some absolute positive constant $c$. □

**Remark 2.3.** In the final remark of [21], Szőnyi suggested a proof along the following lines, which shares some similarities with our proof. We now explain the details implicit in his remark. We fix a point $P \in \mathbb{P}^2(\mathbb{F}_q)$ (to be specified) and consider all the $q + 1$ $\mathbb{F}_q$-lines in $\mathbb{P}^2$ that pass through $P$. Call these lines $L_1, L_2, \ldots, L_{q+1}$. The condition that $L_i$ is skew to a given conic can be expressed as a certain single-variable quadratic function achieving a nonsquare value (this step requires some verification). Using Weil's bound, one can show that if the collection contains fewer than $c_0 \log q$ conics, then at least one line $L_i$ through $P$ is skew to all of them. To apply Weil's bound, one needs to be careful that no nonempty subcollection of these single-variable polynomials has a product equal to a constant multiple of a square of a polynomial. To rule out this scenario, one needs to find a point $P$ such that none of the $q + 1$ lines through $P$ is tangent to more than one conic. The difference between Szőnyi's method and our proof is that we need not reduce to a single-variable polynomial, as we can rely on Lemma 2.1.

## 3. Blocking families and Chebotarev Density Theorem

This section is devoted to proving Theorem 1.3. Throughout the section, we assume that $q$ is odd. We establish a more general result (Theorem 3.1 below), showing that under a mild hypothesis, any bounded collection of curves fails to form a blocking set for sufficiently large $q$. Theorem 1.3 will then follow as a corollary.

**Theorem 3.1.** *Let $C \subset \mathbb{P}^2$ be a plane curve of degree $\widetilde{d}$ defined over $\mathbb{F}_q$. Suppose each geometrically irreducible component of $C$ has degree at least 2 and is reflexive. Then $C(\mathbb{F}_q)$ is not a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$ for $q$ sufficiently large with respect to $\widetilde{d}$.*

To prove that $C(\mathbb{F}_q)$ is not a blocking set, it suffices to demonstrate the existence of at least one $\mathbb{F}_q$-line $L$ that is skew to $C$, meaning $(L \cap C)(\mathbb{F}_q) = \emptyset$. The existence of such a skew line is an arithmetic question over $\mathbb{F}_q$, but it can be studied by analyzing the geometry of the intersection over the algebraic closure $\overline{\mathbb{F}_q}$.

To build this connection, let us first consider the case where $C$ is a single geometrically irreducible curve of degree $d$. For a transverse $\mathbb{F}_q$-line $L$, the intersection $L \cap C$ consists of $d$ distinct points in $\mathbb{P}^2(\overline{\mathbb{F}_q})$. The geometric Frobenius map, $\sigma\colon [x : y : z] \mapsto [x^q : y^q : z^q]$, permutes these $d$

points because both $L$ and $C$ are defined over $\mathbb{F}_q$. This permutation partitions the set of intersection points into orbits. Each orbit corresponds to a set of roots of an irreducible polynomial over $\mathbb{F}_q$, and the size of the orbit is the degree of that polynomial. The partition of the integer $d$ into the sizes of these orbits is the cycle type of the permutation, which defines a unique conjugacy class in the symmetric group $S_d$. We denote this class by $\mathrm{Frob}(C \cap L)$.

This framework extends naturally to a reducible curve whose $\mathbb{F}_q$-irreducible components are geometrically irreducible. Let $C = \bigcup_{i=1}^m C_i$ be a plane curve with geometrically irreducible components $C_i$ of degree $d_i$. For a transverse $\mathbb{F}_q$-line $L$, the Frobenius map again permutes the intersection points. Since each $C_i$ is defined over $\mathbb{F}_q$, the action preserves the subsets $L \cap C_i$. We can therefore analyze the permutation on each subset independently. The action on the $d_i$ points of $L \cap C_i$ defines a conjugacy class in $S_{d_i}$ as described above. Taken together, the total permutation defines a conjugacy class in the product group $S_{d_1} \times \cdots \times S_{d_m}$.

Crucially, a point in the intersection $C \cap L$ is defined over $\mathbb{F}_q$ if and only if it is a fixed point of the Frobenius permutation. Therefore, a line $L$ is skew to $C$ if and only if its associated Frobenius action is a *derangement* (a permutation with no fixed points). Our task is now translated into an arithmetic-geometric one: counting lines whose Frobenius action corresponds to a derangement.

To count these lines, we use a version of the Chebotarev density theorem, due to Entin [11, Theorem 1]. The hypothesis of Entin's theorem depends on a technical condition known as reflexivity. A plane curve $C$ is called *reflexive* if a generic tangent line to $C$ has contact of order exactly 2 (i.e., is not a flex) and is tangent at a unique point (i.e., not bitangent). Every geometrically irreducible plane curve of degree $d$ is reflexive when the characteristic $p$ satisfies $p > d$ (see [14, p. 5]). This motivates the hypothesis in Theorem 1.3. Entin's theorem is stated for the slightly more general condition of *quasireflexivity* to handle cases in characteristic 2, but since we assume $q$ is odd in this section, the reflexivity condition is sufficient for our purposes. Indeed, when $\mathrm{char}(\mathbb{F}_q)$ is odd, the notions of reflexivity and quasireflexivity are equivalent [11, Proposition 2.1].

**Theorem 3.2** (Entin)**.** *Let $C \subset \mathbb{P}^2$ be a reflexive plane curve of degree $\tilde{d}$ defined over $\mathbb{F}_q$. Suppose the irreducible components of $C$ are $C_1, \ldots, C_m$ where each $C_i$ is geometrically irreducible and $\deg(C_i) = d_i$ for $1 \le i \le m$. Let $U \subseteq (\mathbb{P}^2)^*$ denote the open subset of lines not tangent to $C$. Let $\mathcal{C}$ be a conjugacy class in the product group $S_{d_1} \times \cdots \times S_{d_m}$. Then*

$$|\{L \in U(\mathbb{F}_q) : \mathrm{Frob}(C \cap L) = \mathcal{C}\}| = \frac{|\mathcal{C}|}{|S_{d_1} \times S_{d_2} \times \cdots \times S_{d_m}|} q^2 \left(1 + O_{\tilde{d}}(q^{-1/2})\right).$$

We illustrate Theorem 3.2 in the special case where the conjugacy class in $S_{d_1} \times \cdots \times S_{d_m}$ corresponds to special derangements. More precisely, let $\mathcal{C}$ be the conjugacy class of derangements corresponding to a product of cycles of full length, i.e., a $d_i$-cycle in each component $S_{d_i}$. The size of this conjugacy class is $|\mathcal{C}| = \prod_{i=1}^m (d_i - 1)!$. Applying Theorem 3.2, the number of transverse $\mathbb{F}_q$-lines $L$ for which $\mathrm{Frob}(C \cap L) = \mathcal{C}$ is

$$\frac{|\mathcal{C}|}{d_1! \cdot d_2! \cdots d_m!} q^2 \left(1 + O_{\tilde{d}}(q^{-1/2})\right) = \left(\prod_{i=1}^m \frac{1}{d_i}\right) q^2 \left(1 + O_{\tilde{d}}(q^{-1/2})\right). \tag{3.1}$$

Since this quantity is positive for sufficiently large $q$, there must exist at least one line that is skew to all geometrically irreducible components $C_1, \ldots, C_m$. In particular, for $q$ sufficiently large, we see that a positive fraction of $\mathbb{F}_q$-lines are skew to $C$. We now have the tools to prove the main technical result of this section.

*Proof of Theorem 3.1.* Decompose $C$ into its irreducible components over $\mathbb{F}_q$ in the following way:

$$C = C_1 \cup \cdots \cup C_m \cup C_{m+1} \cup \cdots \cup C_r,$$

where

- $C_i$ is irreducible over $\mathbb{F}_q$ and $d_i = \deg(C_i) \geq 2$ for each $i \geq 1$.
- $C_i$ is irreducible over $\overline{\mathbb{F}_q}$ for each $i \leq m$, and $C_i$ is *not* irreducible over $\overline{\mathbb{F}_q}$ for each $i > m$.

By hypothesis, $C_i$ is reflexive for each $1 \leq i \leq m$. By the above discussion, the number of $\mathbb{F}_q$-lines that are skew to $C_i$ for each $1 \leq i \leq m$ is at least the quantity given by equation (3.1). On the other hand, for each $m+1 \leq i \leq r$, the curve $C_i$ is irreducible over $\mathbb{F}_q$ but not geometrically irreducible. For these curves, a standard application of Bézout's theorem shows that $|C_i(\mathbb{F}_q)| \leq \frac{d_i^2}{4}$ (see, for example, [3, Lemma 3.1]). Consequently, for each $m+1 \leq i \leq r$, all but at most $\frac{d_i^2}{4}(q+1)$ lines are skew to the curve $C_i$. Thus, the number of skew lines to $C$ is at least:

$$\left(\prod_{i=1}^{m} \frac{1}{d_i}\right) q^2 \left(1 + O_{\widetilde{d}}(q^{-1/2})\right) - \frac{q+1}{4} \sum_{i=m+1}^{r} d_i^2 \geq \frac{1}{\widetilde{d}^m} q^2 \left(1 + O_{\widetilde{d}}(q^{-1/2})\right) - \frac{(q+1)\widetilde{d}^2}{4}. \quad (3.2)$$

For $q$ sufficiently large with respect to $\widetilde{d}$, the lower bound (3.2) yields a positive fraction of $\mathbb{F}_q$-lines $L$ for which $(L \cap C)(\mathbb{F}_q) = \emptyset$. In particular, $C(\mathbb{F}_q)$ is not a blocking set. □

We are now equipped to prove Theorem 1.3.

*Proof of Theorem 1.3.* The result is a direct consequence of Theorem 3.1. If $\ell(q)$ were bounded by a constant, then the corresponding union of curves would have a total degree bounded by a constant. The condition $q \in \mathcal{Q}_d$ ensures that each component curve is reflexive, so for $q$ sufficiently large, Theorem 3.1 implies this union cannot be a blocking set, a contradiction. □

**Remark 3.3.** The hypothesis $p > d$ in Theorem 1.3 ensures that the component curves are reflexive. This condition $p > d$ can be relaxed for families of *nonsingular* curves. By a result of Pardini [17], a nonsingular curve of degree $d$ is nonreflexive only if $d \equiv 1 \pmod{p}$. Thus, the weaker condition $p \nmid (d-1)$ is sufficient to guarantee reflexivity for nonsingular curves. The conclusion of Theorem 1.3 therefore holds if each curve $C_i$ is nonsingular and its degree $d_i$ satisfies $p \nmid (d_i - 1)$.

## 4. First Proof of Theorem 1.4: randomized construction

In this section, we give a non-constructive proof of Theorem 1.4. We rely on a covering lemma due to S. K. Stein [20], stated as in [13, Lemma 2.3], whose proof uses a randomized construction.

**Lemma 4.1** (Stein)**.** *Consider a bipartite graph with bipartition $A \cup B$. Let $\delta$ be the minimum degree of a vertex in $A$. If $|A| \geq 2$, then there is a set $B' \subseteq B$ such that*

$$|B'| \leq \left\lceil |B| \frac{\log |A|}{\delta} \right\rceil \quad (4.1)$$

*and $B'$ dominates $A$ (that is, for each $a \in A$, there is $b \in B'$ such that $a$ and $b$ are adjacent).*

As preparation, we need a few lemmas. The first lemma is about an estimate on binomial coefficients.

**Lemma 4.2.** *Let $d \geq 2$. If $D \mid d$, then we have $D\binom{d/D+2}{2} \leq \binom{d+2}{2}$.*

*Proof.* Observe that the function $\binom{t+2}{2}$ is strictly convex for real $t > 0$. It follows that for all positive integers $n$ and $m$, we have $\binom{n+m+2}{2} - \binom{n+2}{2} > \binom{m+2}{2} - \binom{0+2}{2} = \binom{m+2}{2} - 1$, that is, $\binom{n+m+2}{2} \geq \binom{n+2}{2} + \binom{m+2}{2}$. Repeatedly applying this inequality, we obtain $D\binom{d/D+2}{2} \leq \binom{d+2}{2}$. □

The next lemma is a standard interpolation lemma; see, for example, [4, Proposition 3.1].

**Lemma 4.3.** *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 $d \geq k-1$, then passing through $P_1, P_2, \ldots, P_k$ imposes linearly independent conditions in the vector space of degree $d$ plane curves over $\mathbb{F}_q$.*

Next, we deduce the following corollary.

**Corollary 4.4.** *Let $d \geq 3$ and $N = \binom{d+2}{2}$. Uniformly for all $P \in \mathbb{P}^2(\mathbb{F}_q)$, the number of geometrically irreducible degree $d$ plane curves defined over $\mathbb{F}_q$ that pass through $P$ is $\frac{q^{N-1} - O_d(q^{N-2})}{q-1}$.*

*Proof.* Fix a point $P \in \mathbb{P}^2(\mathbb{F}_q)$. For each $1 \leq j \leq d$, let $\mathcal{S}_j$ denote the set of degree $j$ homogeneous polynomials in $\mathbb{F}_q[x, y, z]$ (together with the zero polynomial) and let $\mathcal{T}_j \subseteq \mathcal{S}_j$ denote the subset of polynomials $F$ in $\mathcal{S}_j$ such that the curve $\{F = 0\}$ passes through $P$. Note that for each $1 \leq j \leq d$, we have $|\mathcal{S}_j| = q^{\binom{j+2}{2}}$ and $|\mathcal{T}_j| = q^{\binom{j+2}{2}-1}$ by Lemma 4.3.

Let $\mathcal{R}_d \subseteq \mathcal{T}_d \setminus \{0\}$ denote the set of polynomials in $\mathcal{T}_d \setminus \{0\}$ that are reducible over $\mathbb{F}_q$. If $F \in \mathcal{R}_d$, then we can write $F = GH$ for some nonconstant polynomials $G, H$ such that the curve $\{G = 0\}$ passes through $P$. It follows that

$$|\mathcal{R}_d| \leq \sum_{j=1}^{d-1} |\mathcal{T}_j||\mathcal{S}_{d-j}| = \sum_{j=1}^{d-1} q^{\binom{j+2}{2}+\binom{d-j+2}{2}-1} \leq 2 \sum_{j=1}^{\lceil (d-1)/2 \rceil} q^{\binom{j+2}{2}+\binom{d-j+2}{2}-1}$$

Since the function $\binom{t+2}{2}$ is strictly convex for real $t > 0$, for each $1 \leq j \leq d-2$, we have $\binom{d+2}{2} - \binom{d-j+2}{2} \geq \binom{j+2}{2} - \binom{0+2}{2} + d - j$, which implies that $N = \binom{d+2}{2} \geq \binom{j+2}{2} + \binom{d-j+2}{2} + 1$. Since $d - 2 \geq \lceil (d-1)/2 \rceil$ for $d \geq 3$, it follows that

$$|\mathcal{R}_d| \leq 2 \sum_{j=1}^{\lceil (d-1)/2 \rceil} q^{\binom{j+2}{2}+\binom{d-j+2}{2}-1} \leq dq^{N-2}.$$

Let $\mathcal{G}_d \subseteq \mathcal{T}_d \setminus \{0\}$ denote the set of polynomials in $\mathcal{T}_d \setminus \{0\}$ that are irreducible over $\mathbb{F}_q$ but geometrically reducible. Note that if $F \in \mathcal{G}_d$, then necessarily $F = \mathrm{Norm}_{\mathbb{F}_{q^D}/\mathbb{F}_q}(G)$ for some $D \mid d$ with $D \geq 2$ and some polynomial $G$ with degree $d/D$ defined over $\mathbb{F}_{q^D}$ such that the curve $\{G = 0\}$ passes through $P$. It follows from Lemma 4.2 and Lemma 4.3 that

$$|\mathcal{G}_d| \leq \sum_{D|d, D\geq 2} (q^D)^{\binom{d/D+2}{2}-1} \leq q^{-2} \sum_{D|d, D\geq 2} q^{D\binom{d/D+2}{2}} \leq q^{-2} \sum_{D|d, D\geq 2} q^{\binom{d+2}{2}} \leq (d-1)q^{N-2}.$$

Combining the two estimates above, the corollary follows. □

We are now ready to present our first proof of Theorem 1.4. The proof shows that $c_d$ can be taken arbitrarily close to 4 when $q$ is sufficiently large.

*Proof of Theorem 1.4.* We build a bipartite graph with bipartition $A \cup B$ as in Lemma 4.1, where $A$ is the set of all $q^2 + q + 1$ lines in $\mathbb{P}^2$ defined over $\mathbb{F}_q$ and $B$ is the set of all geometrically irreducible curves defined over $\mathbb{F}_q$ with degree $d$. We draw an edge between a vertex $L \in A$ and a vertex $C \in B$ if the intersection $C \cap L$ contains an $\mathbb{F}_q$-point.

Next, we give a lower bound on the minimum degree $\delta$ of a vertex in $A$. By definition, we fix an $\mathbb{F}_q$-line $L$ and count the number of geometrically irreducible curves $C \in B$ such that $(C \cap L)(\mathbb{F}_q) \neq \emptyset$. As each $\mathbb{F}_q$-line has $q+1$ points, we can express $L(\mathbb{F}_q) = \{P_1, P_2, \ldots, P_{q+1}\}$. For each subset $S \subseteq \mathbb{P}^2(\mathbb{F}_q)$, define

$$\psi(S) = \#\{\text{geometrically irreducible curves } C \text{ of degree } d \text{ such that } S \subseteq C(\mathbb{F}_q)\}.$$

By the principle of inclusion-exclusion, the degree of the vertex $L$ in the bipartite graph is at least:

$$\sum_{1 \leq i \leq q+1} \psi(\{P_i\}) - \sum_{1 \leq i < j \leq q+1} \psi(\{P_i, P_j\}). \tag{4.2}$$

Let $N = \binom{d+2}{2}$ denote the dimension of the $\mathbb{F}_q$-vector space parameterizing all degree $d$ homogeneous polynomials in three variables. By Lemma 4.3 and Corollary 4.4, we have

$$\psi(\{P\}) = \frac{q^{N-1} - O_d(q^{N-2})}{q-1}, \quad \psi(\{P,Q\}) \leq \frac{q^{N-2}-1}{q-1}$$

for any two distinct points $P, Q \in \mathbb{P}^2(\mathbb{F}_q)$. The lower bound (4.2) for the degree of $L$ thus becomes:

$$(q+1) \cdot \frac{q^{N-1} - O_d(q^{N-2})}{q-1} - \binom{q+1}{2} \cdot \frac{q^{N-2}-1}{q-1} = \frac{1}{2} q^{N-1} - O_d(q^{N-2}).$$

This allows us to conclude that $\delta \geq \frac{1}{2} q^{N-1} - O_d(q^{N-2})$ for the minimum degree of a vertex in $A$. Applying inequality (4.1), we find a subset $B' \subseteq B$ dominating $A$ with

$$\begin{aligned} |B'| &\leq |B| \frac{\log(|A|)}{\delta} + 1 \leq \frac{q^N - 1}{q-1} \cdot \frac{\log(q^2+q+1)}{\frac{1}{2}q^{N-1} - O_d(q^{N-2})} + 1 \\ &\leq (4 + o(1)) \log q, \end{aligned}$$

as $q \to \infty$. Equivalently, we can find a blocking set constructed from $(4+o(1)) \log q$ geometrically irreducible curves of degree $d$, as required. □

**Remark 4.5.** It is straightforward to modify the above proof to construct multiple blocking sets using a union of geometrically irreducible degree $d$ curves. Recall that for each positive integer $t$, a *$t$-fold blocking set* in $\mathbb{P}^2(\mathbb{F}_q)$ is a subset of $\mathbb{P}^2(\mathbb{F}_q)$ such that it intersects each $\mathbb{F}_q$-line with at least $t$ points. To form a $t$-fold blocking set in $\mathbb{P}^2(\mathbb{F}_q)$, a similar computation shows that $(\frac{2(t+1)!}{t} + o(1)) \log q$ curves are sufficient if $d \geq \min\{t, 3\}$.

## 5. Second Proof of Theorem 1.4: Explicit Construction

Let $d \geq 3$ be an integer and consider the curves $C_\alpha$ (parametrized by $\alpha \in \mathbb{F}_q$) given by

$$yz^{d-1} = x^d - \alpha z^d. \tag{5.1}$$

Each $C_\alpha$ is geometrically irreducible: the defining equation (5.1) is linear in $y$, so any nontrivial factorization of $yz^{d-1} - x^d + \alpha z^d$ in $\overline{\mathbb{F}_q}[x,y,z]$ would involve a nonconstant factor from $\overline{\mathbb{F}_q}[x,z]$; however, this is impossible since $z^{d-1}$ and $x^d - \alpha z^d$ share no common factor in $\overline{\mathbb{F}_q}[x,z]$.

**Theorem 5.1.** *There exists a subset $S \subseteq \mathbb{F}_q$ of size at most $1 + \left\lfloor \frac{2 \log q}{\log\left(\frac{d}{d-1}\right)} \right\rfloor$ with the property that*

$$U := \bigcup_{\alpha \in S} C_\alpha(\mathbb{F}_q) \tag{5.2}$$

*is a blocking set in* $\mathbb{P}^2(\mathbb{F}_q)$.

*Proof.* We will choose a subset $S \subseteq \mathbb{F}_q$ and set $U := \bigcup_{\alpha \in S} C_\alpha(\mathbb{F}_q)$. The goal is to select $S$ so that $U$ meets each $\mathbb{F}_q$-line of $\mathbb{P}^2$. Our strategy is to include $\mathbb{F}_q$-points of curves $C_\alpha$ for suitable values of $\alpha$, chosen sequentially to block as many new lines as possible at each step.

Let $L \subseteq \mathbb{P}^2$ be an $\mathbb{F}_q$-line; so, the equation of $L$ is $ax + by + cz = 0$ for some $[a : b : c] \in \mathbb{P}^2(\mathbb{F}_q)$. Since $[0 : 1 : 0] \in C_\alpha$ for each $\alpha$, we may assume from now on that $b \neq 0$ (otherwise $[0 : 1 : 0] \in L(\mathbb{F}_q)$ already). Moreover, if $\alpha \in \mathbb{F}_q$ and $[x_0 : y_0 : z_0] \in C_\alpha(\mathbb{F}_q)$ with $z_0 = 0$, then necessarily $[x_0 : y_0 : z_0] = [0 : 1 : 0]$ and hence $[x_0 : y_0 : z_0] \notin L(\mathbb{F}_q)$. Thus, it suffices to compute $L(\mathbb{F}_q) \cap \{[x_0 : y_0 : z_0] \in \mathbb{P}^2(\mathbb{F}_q) : z_0 \neq 0\}$. Writing $u := a/b$ and $v := c/b$, this set is given by $\{[x : -ux - v : 1] : x \in \mathbb{F}_q\}$. Consequently, $U \cap L(\mathbb{F}_q) \neq \emptyset$ if and only if there is some $\alpha \in S$, such that there is $x \in \mathbb{F}_q$ with $[x : -ux - v : 1] \in C_\alpha(\mathbb{F}_q)$, that is, $x^d + ux + v = \alpha$.

To this end, for each $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$, define

$$T_{u,v} := \left\{a^d + ua + v \colon a \in \mathbb{F}_q\right\} \subseteq \mathbb{F}_q\,. \tag{5.3}$$

By the discussion above, $U$ is a blocking set if and only if

$$S \cap T_{u,v} \neq \emptyset \quad \text{for each } (u, v) \in \mathbb{F}_q \times \mathbb{F}_q\,. \tag{5.4}$$

Since $f_{u,v}(x) := x^d + ux + v$ is a polynomial of degree $d$, every value $b \in \mathbb{F}_q$ has at most $d$ preimages in $\mathbb{F}_q$. Therefore,

$$|T_{u,v}| \geq \frac{q}{d} \quad \text{for each } (u, v) \in \mathbb{F}_q \times \mathbb{F}_q\,. \tag{5.5}$$

We construct, by induction on $\ell$, a sequence of elements $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q$ together with sets $S^{(i)}_{\alpha_i} \subseteq \mathbb{F}_q \times \mathbb{F}_q$ (for $i = 1, \ldots, \ell$) satisfying the following properties:

(I) for each $i = 1, \ldots, \ell$ and each $(u, v) \in S^{(i)}_{\alpha_i}$, we have $\alpha_i \in T_{u,v}$. Moreover, for each $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$, if $\alpha_i \in T_{u,v}$, then $(u, v) \in S^{(j)}_{\alpha_j}$ for some $1 \leq j \leq i$.

(II) the sets $S^{(i)}_{\alpha_i}$ are disjoint and

$$\sum_{i=1}^{\ell} \left|S^{(i)}_{\alpha_i}\right| \geq q^2 \cdot \left(1 - \left(\frac{d-1}{d}\right)^{\ell}\right). \tag{5.6}$$

We first prove the base case $\ell = 1$ of the construction satisfying the conditions (I)-(II). For each $\beta \in \mathbb{F}_q$, we define:

$$S^{(1)}_{\beta} := \{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q \colon \beta \in T_{u,v}\}\,. \tag{5.7}$$

A simple counting argument, coupled with inequality (5.5), yields:

$$\sum_{\beta \in \mathbb{F}_q} \left|S^{(1)}_{\beta}\right| = \sum_{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q} |T_{u,v}| \geq q^2 \cdot \frac{q}{d}. \tag{5.8}$$

Choose $\alpha_1 \in \mathbb{F}_q$ such that

$$\left|S^{(1)}_{\alpha_1}\right| \geq \left|S^{(1)}_{\beta}\right| \text{ for each } \beta \in \mathbb{F}_q\,. \tag{5.9}$$

Inequalities (5.8) and (5.9) yield:

$$\left|S^{(1)}_{\alpha_1}\right| \geq \frac{q^2}{d} = q^2 \cdot \left(1 - \frac{d-1}{d}\right). \tag{5.10}$$

This completes the proof of the base case $\ell = 1$ for the construction of the points $\alpha_1, \ldots, \alpha_\ell$ along with the sets $S^{(1)}_{\alpha_1}, \ldots, S^{(\ell)}_{\alpha_\ell}$ satisfying the properties (I)-(II) above.

We continue with the inductive step. Suppose we have constructed $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_q$ (for some $k \geq 1$) along with some sets $S^{(1)}_{\alpha_1}, \ldots, S^{(k)}_{\alpha_k} \subseteq \mathbb{F}_q \times \mathbb{F}_q$ satisfying the properties (I)-(II). We now construct another set $S^{(k+1)}_{\alpha_{k+1}} \subseteq \mathbb{F}_q \times \mathbb{F}_q$ corresponding to another point $\alpha_{k+1} \in \mathbb{F}_q$ still satisfying properties (I)-(II). In particular, the sets $S^{(1)}_{\alpha_1}, \ldots, S^{(k)}_{\alpha_k}$ are disjoint and

$$\sum_{i=1}^{k} \left| S^{(i)}_{\alpha_i} \right| \geq q^2 \cdot \left( 1 - \left( \frac{d-1}{d} \right)^k \right). \tag{5.11}$$

By the inductive hypothesis (I), we know that for each $i = 1, \ldots, k$ and each $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$,

$$\text{if } \alpha_i \in T_{u,v}, \text{ then } (u, v) \in S^{(j)}_{\alpha_j} \text{ for some } j \leq i; \tag{5.12}$$

also, the inductive hypothesis (I) yields

$$\text{for each } i = 1, \ldots, k \text{ and for each } (u, v) \in S^{(i)}_{\alpha_i}, \text{ we have } \alpha_i \in T_{u,v}. \tag{5.13}$$

We let

$$W := (\mathbb{F}_q \times \mathbb{F}_q) \setminus \left( \bigcup_{i=1}^{k} S^{(i)}_{\alpha_i} \right). \tag{5.14}$$

Also, we let $V := \mathbb{F}_q \setminus \{\alpha_1, \ldots, \alpha_k\}$. Using equations (5.12) and (5.14), we have that

$$T_{u,v} \subseteq V \text{ for each } (u, v) \in W. \tag{5.15}$$

Then we define for each $\beta \in V$ the set:

$$S^{(k+1)}_{\beta} := \{(u, v) \in W \colon \beta \in T_{u,v}\};$$

according to equations (5.15) and (5.13), we have that

$$S^{(k+1)}_{\beta} \cap S^{(i)}_{\alpha_i} = \emptyset \text{ for each } i = 1, \ldots, k. \tag{5.16}$$

Due to the definition of each set $S^{(k+1)}_{\beta}$, we get that if $\beta \in T_{u,v}$ (for any $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$), then either $(u, v) \in S^{(i)}_{\alpha_i}$ for some $i = 1, \ldots, k$, or $(u, v) \in S^{(k+1)}_{\beta}$. Using again (5.15), we obtain:

$$\sum_{\beta \in V} \left| S^{(k+1)}_{\beta} \right| = \sum_{(u,v) \in W} |T_{u,v}| \geq |W| \cdot \frac{q}{d}. \tag{5.17}$$

In the last inequality from (5.17), we also employed (5.5). Then we pick $\alpha_{k+1} \in V$ (clearly, $\alpha_{k+1} \neq \alpha_i$ for $i = 1, \ldots, k$ due to the definition of $V$) such that

$$\left| S^{(k+1)}_{\alpha_{k+1}} \right| \geq \left| S^{(k+1)}_{\beta} \right| \text{ for each } \beta \in V. \tag{5.18}$$

Therefore, equations (5.17) and (5.18) yield

$$\left| S^{(k+1)}_{\alpha_{k+1}} \right| \geq \frac{|W| \cdot q}{d \cdot |V|} > \frac{|W|}{d}. \tag{5.19}$$

We note that the sets $S_{\alpha_i}^{(i)}$ are all disjoint for $i = 1, \ldots, k+1$ (by the inductive hypothesis coupled with equation (5.16)); furthermore, condition (I) above is satisfied for the points $\alpha_1, \ldots, \alpha_{k+1}$. Combining the equations (5.19), (5.14) and (5.11), we obtain that

$$\begin{aligned}\sum_{i=1}^{k+1} \left|S_{\alpha_i}^{(i)}\right| &\geq \left|\bigcup_{i=1}^{k} S_{\alpha_i}^{(i)}\right| + \frac{q^2 - \sum_{i=1}^{k}\left|S_{\alpha_i}^{(i)}\right|}{d} \\ &\geq \frac{q^2}{d} + q^2 \cdot \left(1 - \left(\frac{d-1}{d}\right)^k\right) \cdot \frac{d-1}{d} \geq q^2 \cdot \left(1 - \left(\frac{d-1}{d}\right)^{k+1}\right),\end{aligned}$$

as desired for proving that also condition (II) holds for $S_{\alpha_1}^{(1)}, \ldots, S_{\alpha_{k+1}}^{(k+1)}$.

So, inductively, we obtain the construction of points $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q$ such that for the corresponding (disjoint) sets $S_{\alpha_i}^{(i)} \subseteq \mathbb{F}_q \times \mathbb{F}_q$, we have the inequality

$$\left|\bigcup_{i=1}^{\ell} S_{\alpha_i}^{(i)}\right| \geq q^2 \cdot \left(1 - \left(\frac{d-1}{d}\right)^{\ell}\right). \tag{5.20}$$

Furthermore, by construction, for each $(u, v) \in \bigcup_{i=1}^{\ell} S_{\alpha_i}^{(i)}$, there exists some $i \in \{1, \ldots, \ell\}$ such that $\alpha_i \in T_{u,v}$. Our construction stops when we achieve that

$$\bigcup_{i=1}^{\ell} S_{\alpha_i}^{(i)} = \mathbb{F}_q \times \mathbb{F}_q \tag{5.21}$$

because then the corresponding set $S := \{\alpha_1, \ldots, \alpha_\ell\}$ will have the desired property (5.4). So, in order to obtain (5.21), it suffices to have that

$$\left|\bigcup_{i=1}^{\ell} S_{\alpha_i}^{(i)}\right| > q^2 - 1. \tag{5.22}$$

Using inequality (5.20), we see that inequality (5.22) is achieved once we have:

$$\left(\frac{d-1}{d}\right)^{\ell} < \frac{1}{q^2}. \tag{5.23}$$

So, indeed, we can find a set $S$ such that $|S| \leq 1 + \left\lfloor \frac{2\log q}{\log\left(\frac{d}{d-1}\right)} \right\rfloor$, as required. □

**Remark 5.2.** Assume that $d' = \gcd(d, q-1) > 1$. In this case, we can show that if $\bigcup_{\alpha \in S} C_\alpha(\mathbb{F}_q)$ is a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$, then necessarily $|S| \geq c_{d'} \log q$ for some constant $c_{d'}$ depending on $d'$. Indeed, by equation (5.4), we have $S \cap T_{u,v} \neq \emptyset$ for all $u, v \in \mathbb{F}_q$; in particular, for each $v \in \mathbb{F}_q$, we have $S \cap T_{0,v} = S \cap \{a^{d'} + v : a \in \mathbb{F}_q\} \neq \emptyset$. Now, if $|S| < c_{d'} \log q$, then a standard application of Weil's bound (see for example [3, Lemma 2.1]) shows that there is $x \in \mathbb{F}_q$, such that $s - x$ is not a $d'$-th power in $\mathbb{F}_q$ for each $s \in S$, that is, $S \cap T_{0,x} = \emptyset$, contradicting to the above assumption on $S$. Thus, it follows that $|S| \geq c_{d'} \log q$.

We end the paper with the following open question regarding the family of curves $C_\alpha \subset \mathbb{P}^2$ defined by $yz^{d-1} = x^d - \alpha z^d$.

**Question 5.3.** *Given $q$ and $d$, what is the smallest possible size of $S \subset \mathbb{F}_q$ such that $\bigcup_{\alpha \in S} C_\alpha(\mathbb{F}_q)$ is a blocking set in $\mathbb{P}^2(\mathbb{F}_q)$?*

When $\gcd(d, q-1) > 1$, we have shown that the answer to Question 5.3 is between $c_1 \log q$ and $c_2 \log q$, where $c_1$ is a constant depending only on $\gcd(d, q-1)$ and $c_2$ is a constant depending only on $d$. Getting an asymptotically sharp answer in this case seems challenging.

By contrast, if $\gcd(d, q-1) = 1$, then our argument for the lower bound no longer applies. Indeed, the map $\mathbb{F}_q \to \mathbb{F}_q$ given by $x \mapsto x^d$ is a permutation, and so, it is not useful to consider $d$-th power residues. It would be interesting to establish the asymptotic behavior of the answer to Question 5.3 in this case.

## ACKNOWLEDGMENTS

We are grateful to Alexei Entin for helpful discussions regarding Theorem 3.2.

## REFERENCES

[1] H. L. Abbott and A. Liu. Property $B(s)$ and projective planes. *Ars Combin.*, 20:217–220, 1985.
[2] S. Asgarli, D. Ghioca, and C. H. Yip. Existence of pencils with nonblocking hypersurfaces. *Finite Fields Appl.*, 92:Paper No. 102283, 11, 2023.
[3] S. Asgarli, D. Ghioca, and C. H. Yip. Plane curves giving rise to blocking sets over finite fields. *Des. Codes Cryptogr.*, 91(11):3643–3669, 2023.
[4] S. Asgarli, D. Ghioca, and C. H. Yip. Most plane curves over finite fields are not blocking. *J. Combin. Theory Ser. A*, 204:Paper No. 105871, 26, 2024.
[5] S. Asgarli, D. Ghioca, and C. H. Yip. Proportion of blocking curves in a pencil. *Discrete Math.*, 349(1):Paper No. 114668, 2026.
[6] Y. Aubry and M. Perret. A Weil theorem for singular curves. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pages 1–7. de Gruyter, Berlin, 1996.
[7] A. Blokhuis, P. Sziklai, and T. Szőnyi. Blocking sets in projective spaces. In L. Storme and J. De Beule, editors, *Current Research Topics in Galois Geometry*, pages 61–84. Nova Science Publishers, Inc., New York, 2012. Electronic ISBN: 9781620813638; 24 pages.
[8] E. Boros. $\mathrm{PG}(2, p^s),\ p > 2$, has property $B(p+2)$. *Ars Combin.*, 25:111–113, 1988.
[9] A. Bruen and J. C. Fisher. Blocking sets and complete $k$-arcs. *Pacific J. Math.*, 53:73–84, 1974.
[10] A. Cafure and G. Matera. Improved explicit estimates on the number of solutions of equations over a finite field. *Finite Fields Appl.*, 12(2):155–185, 2006.
[11] A. Entin. Monodromy of hyperplane sections of curves and decomposition statistics over finite fields. *Int. Math. Res. Not. IMRN*, (14):10409–10441, 2021.
[12] P. Erdős, R. Silverman, and A. Stein. Intersection properties of families containing sets of nearly the same size. *Ars Combin.*, 15:247–259, 1983.
[13] A. Gács and T. Szőnyi. Random constructions and density results. *Des. Codes Cryptogr.*, 47(1-3):267–287, 2008.
[14] A. Hefez. Nonreflexive curves. *Compositio Math.*, 69(1):3–35, 1989.
[15] T. Illés, T. Szőnyi, and F. Wettl. Blocking sets and maximal strong representative systems in finite projective planes. In *Proceedings of the First International Conference on Blocking Sets (Giessen, 1989)*, number 201, pages 97–107, 1991.
[16] S. Lang and A. Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.
[17] R. Pardini. Some remarks on plane curves over fields of finite characteristic. *Compositio Math.*, 60(1):3–17, 1986.
[18] V. Pepe and L. Storme. The use of blocking sets in Galois geometries and in related research areas. In *Buildings, finite geometries and groups*, volume 10 of *Springer Proc. Math.*, pages 305–327. Springer, New York, 2012.
[19] K. Slavov. Square values of several polynomials over a finite field. *Finite Fields Appl.*, 109:Paper No. 102696, 2026.
[20] S. K. Stein. Two combinatorial covering theorems. *J. Combinatorial Theory Ser. A*, 16:391–397, 1974.
[21] T. Szőnyi. Blocking sets in finite planes and spaces. *Ratio Mathematica*, 5:93–106, 1992.
[22] T. Szőnyi. Note on the existence of large minimal blocking sets in Galois planes. *Combinatorica*, 12(2):227–235, 1992.

[23] E. Ughi. On $(k, n)$-blocking sets which can be obtained as a union of conics. *Geom. Dedicata*, 26(3):241–245, 1988.

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE, SANTA CLARA UNIVERSITY, CA 95053, UNITED STATES
*Email address*: sasgarli@scu.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRITISH COLUMBIA, VANCOUVER, BC V6T 1Z2, CANADA
*Email address*: dghioca@math.ubc.ca

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GA 30332, UNITED STATES
*Email address*: cyip30@gatech.edu