BLOCKING SETS ARISING FROM PLANE CURVES OVER FINITE FIELDS

SHAMIL ASGARLI, DRAGOS GHIOCA, AND CHI HOI YIP

ABSTRACT. In recent years, many useful applications of the polynomial method have emerged in finite geometry. Indeed, algebraic curves, especially those defined by Rédei-type polynomials, are powerful in studying blocking sets. In this paper, we reverse the engine and study when blocking sets can arise from rational points on plane curves over finite fields. We show that irreducible curves of low degree cannot provide blocking sets and prove more refined results for cubic and quartic curves. On the other hand, using tools from number theory, we construct smooth plane curves defined over $\mathbb{F}_p$ of degree at most $4p^{3/4}+1$ whose points form blocking sets.

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. A set of points $B \subset \mathbb{P}^2(\mathbb{F}_q)$ is called a *blocking set* if every $\mathbb{F}_q$-line L intersects B. It is clear that taking $q+1$ points on a given $\mathbb{F}_q$-line form a blocking set, since any two lines meet in the projective plane; this is known as a *trivial* blocking set. A blocking set B is said to be *nontrivial* if it does not contain all the $\mathbb{F}_q$-points of any $\mathbb{F}_q$-line.

It is known that the size of a nontrivial blocking set must satisfy $|B| \geq q+\sqrt{q}+1$ [Bru70]. When $q=p$ is a prime, Blokhuis [Blo94] proved that $|B| \geq \frac{3}{2}(p+1)$. The main tool used in Blokhuis' proof and in subsequent developments in this area have been Rédei-type polynomials which are highly reducible algebraic curves. See the excellent surveys [Sző97b, SS98] for more details and other applications of algebraic curves in finite geometry.

Let $C=\{F=0\} \subset \mathbb{P}^2$ be an irreducible plane curve of degree $d \geq 2$ defined over a finite field $\mathbb{F}_q$. Let $C(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-points on C, that is, $C(\mathbb{F}_q)$ consists of all $[x:y:z] \in \mathbb{P}^2(\mathbb{F}_q)$ such that $F(x,y,z)=0$. We assume that our curve is irreducible so that the curve is "minimal" in the sense that it has no smaller component. Since smooth curves are important from algebraic geometric point of view, we will sometimes further assume C is smooth. We are interested in the following problem.

Question 1.1. When does there exist a line $L \subset \mathbb{P}^2$ defined over $\mathbb{F}_q$ such that $C \cap L$ has no $\mathbb{F}_q$-points?

One motivation for finding a positive answer to Question 1.1 comes from algebraic geometry. Suppose C is a curve which parametrizes other algebraic varieties; for instance, C could be a curve in the parameter space of all degree d hypersurfaces in $\mathbb{P}^n$. This means that a point on C corresponds to a certain hypersurface of degree d. The points in $C(\mathbb{F}_q)$ would then correspond to those hypersurfaces of degree d defined over $\mathbb{F}_q$. If we can find a line L such that $C \cap L$ has no $\mathbb{F}_q$-points, then we have constructed a certain *pencil* whose $\mathbb{F}_q$-members avoid C. In particular, one can use this idea to construct a pencil of hypersurfaces whose $\mathbb{F}_q$-members are smooth [AG22].

2020 *Mathematics Subject Classification.* Primary 51E21, 14H50; Secondary 51E15, 11T30, 11G20.

Key words and phrases. Plane curves, blocking sets, finite field, Frobenius nonclassical, projective triangle.

Using the language of blocking sets, Question 1.1 is equivalent to determining when $C(\mathbb{F}_q)$ is **not** a blocking set. We remark that questions of a similar flavor have been studied in the past. In particular, Hirschfeld and Voloch [HV88] asked when an arc is contained in an irreducible plane curve, and when an irreducible plane curve gives rise to a complete arc. One special motivation for constructing such curves lies in its application to coding theory [Bor09]. Recall that a (k,n)-*arc* in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of k points where the maximum number of collinear points is n. There is an obvious relation between arcs and blocking sets: a complement of a (k,n)-arc in the plane is a (multiple) blocking set where each line meets the point set in at least $q+1-n$ points. The case of smooth conics ($(k,2)$-arcs) was first studied by Segre [Seg67], cubic curves ($(k,3)$-arcs) were studied in [HV88, Giu02, BMP17], and some special algebraic constructions were discussed in [GPTU02, Bor09, BMT14, BM22]. Similar questions have been studied in the setting of caps in [Seg67, ABGP14, ABPG15].

For simplicity, let us call C a *blocking curve* if $C(\mathbb{F}_q)$ is a blocking set. Furthermore, C is *nontrivially blocking* if $C(\mathbb{F}_q)$ is a nontrivial blocking set. Constructing such curves appear to be more subtle, as most plane curves are not blocking [AGY22].

Motivated by the past work on arcs arising from plane curves, we begin our study with the curves of low degree with respect to the cardinality of the field. Our first main result shows that an irreducible curve of low degree cannot be blocking.

Theorem 1.2. *Let $C \subset \mathbb{P}^2$ be an irreducible curve of degree $d \geq 4$. If $q \geq (d-1)^2(d-2)^4$, then C is not blocking.*

We improve the bound $O(d^6)$ to $O(d^4)$ for the case $q = p^n$ with $n \leq 4$ in Theorem 3.3.

When $d = 2$, it is straightforward to see that an irreducible conic can never be a blocking set. For cubic curves, we have a more refined result:

Theorem 1.3. *Let $C \subset \mathbb{P}^2$ be an irreducible cubic curve. If $q \geq 5$, then C is not blocking.*

Moreover, Theorem 1.3 is sharp in a sense that there exist smooth cubic curves over $\mathbb{F}_q$ which are blocking when $q = 2, 3, 4$. See Example 3.5. We also establish a refined bound for smooth quartic curves.

Theorem 1.4. *Suppose C is a smooth plane curve of degree 4 defined over a finite field $\mathbb{F}_q$. If $q \geq 19$, then C is not blocking.*

Another aim of our paper is to construct explicit examples of smooth or irreducible blocking plane curves. When q is a nontrivial prime power, meaning that $q = p^n$ with $n \geq 2$, then it is easy to find special curves which are smooth and blocking. For example, when q is a square, we have the following well-known construction.

Example 1.5. Let q be a square. Consider the Hermitian curve given by the equation

$$\mathcal{H}: \; x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0$$

It is known that every $\mathbb{F}_q$-line meets $\mathcal{H}$ in either 1 or $\sqrt{q}+1$ points [Szőz97b, Page 212]. In particular, $\mathcal{H}$ is a smooth curve of degree $d = \sqrt{q}+1$ such that $\mathcal{H}(\mathbb{F}_q)$ is a blocking set.

We provide a more general construction using Frobenius nonclassical curves in Section 4. Such a construction relies on the subfield structure, which is not available in $\mathbb{F}_q$ when q is a prime. When $q = p$ is a prime, it seems more difficult to find explicit examples of blocking curves; we find a family of examples in Theorem 1.6 and Theorem 1.7.

It is natural to ask for the minimum degree of an irreducible curve passing through a specific blocking set. We analyze this question for the projective triangle in Section 5. Recall that the *projective triangle* is the blocking set given by,

$$\Delta = \{[0:1:-s^2], [1:-s^2:0], [-s^2:0:1] \mid s \in \mathbb{F}_q\}$$

with cardinality $3(q+1)/2$. We construct a smooth curve with degree $\frac{q+3}{2}$ passing through Δ in Theorem 5.1 when $q \equiv 3 \pmod 4$. Indeed, such a curve would have degree at least $\frac{q+3}{2}$ by Bézout's theorem (see Remark 5.2), so our construction is optimal.

Note that when p is an odd prime, the projective triangle Δ is of particular interest, since it serves as an example of a nontrivial blocking set of size $\frac{3}{2}(p+1)$ over $\mathbb{F}_p$, which is the smallest possible size by Blokhuis [Blo94]. However, this does not imply that the smallest degree irreducible blocking curve C must necessarily pass through the projective triangle (the smallest blocking set) or its image under a projective transformation. Indeed, we find geometrically irreducible blocking curves with smaller degree $d = \frac{p-1}{r} + 1$ in Theorem 6.2 for a fixed r, provided that $p \equiv 1 \pmod r$ and $p > r^4$. Using tools from analytic number theory, we can prove something even stronger.

Theorem 1.6. *There are infinitely many primes p such that for each $d \geq 4p^{3/4} + 1$, there is a geometrically irreducible nontrivially blocking curve over $\mathbb{F}_p$ with degree d.*

In view of Theorem 1.6, one can ask for the smallest degree of an irreducible blocking curve over $\mathbb{F}_p$ for p prime. According to Theorem 3.3, the optimal degree for a blocking curve satisfies $d \geq C_0 p^{1/4}$ for some constant C_0, while Theorem 1.6 tells us that the optimal degree must satisfy $d \leq C_1 p^{3/4}$ for some constant C_1. Let us briefly explain why the optimal exponent of degree is likely to be near $1/2$. We expect that for any $\varepsilon > 0$, there are many blocking sets of size at most $\lambda_\varepsilon p^{1+\varepsilon}$ where λ_ε is a constant. Since the vector space V of degree d homogeneous polynomials defining plane curves has dimension $\binom{d+2}{2}$, we obtain many blocking curves provided that $\binom{d+2}{2} > \lambda_\varepsilon p^{1+\varepsilon}$. Indeed, passing through any specific point imposes at most one linear condition on V. While this furnishes numerous blocking curves of degree $d \leq C_\varepsilon p^{1/2+\varepsilon}$, this is only a heuristic because we cannot demonstrate irreducibility of any such curve in this abstract setting.

Constructing smooth blocking curves appears to be much more difficult. One difficulty in applying the heuristic above is the following: we want the smooth curve to pass through a blocking set with relatively large size, while we expect that the number of $\mathbb{F}_p$-points of most smooth curves is close to $p+1$. Nonetheless, we prove a version of Theorem 1.6 for smooth blocking curves:

Theorem 1.7. *Let $0 < \theta \leq 1/4$. Let A be a fixed positive number, with $A \leq 1/2$ if $\theta = 1/4$. There are infinitely many primes p such that for* some *$d \in [p^{1-\theta}/2A + 1, 2p^{1-\theta}/A + 1]$, there is smooth nontrivially blocking curve over $\mathbb{F}_p$ with degree d.*

The proof of Theorem 1.7 relies on a general construction of a smooth blocking curve (Theorem 6.3). In particular, we can construct smooth blocking curves of degree $\frac{q+1}{2}$. Note that the existence of degree d smooth blocking curve does not necessarily imply the existence of degree $d+1$ smooth blocking curve. Therefore, the next result would not follow from knowing the existence of smooth blocking curves of degree $d = \frac{q+1}{2}$.

Theorem 1.8. *Suppose $q \geq 5$ with $p = \mathrm{char}(\mathbb{F}_q) > 3$. There exists a smooth blocking plane curve over $\mathbb{F}_q$ with degree $d = \frac{q+3}{2}$.*

Similarly, the existence of degree d smooth blocking curve does not necessarily imply the existence of degree $d-1$ smooth blocking curve. However, we are able to exhibit a smooth blocking set of degree $\frac{q-1}{2}$ whenever $q \equiv 3 \pmod 4$.

Theorem 1.9. *Suppose $q \geq 11$ with $q \equiv 3 \pmod 4$ and $p = \mathrm{char}(\mathbb{F}_q) > 3$. There exists a smooth blocking plane curve over $\mathbb{F}_q$ with degree $d = \frac{q-1}{2}$.*

When $q \equiv 1 \pmod 4$, we expect that there should be examples with degree $\frac{q-1}{2}$ for $q \geq 13$. See Example 7.4.

Structure of the paper. In Section 2, we present some preliminary definitions, and discuss useful tools from number theory, algebra, and incidence geometry. In Section 3, we employ point-line incidence geometry to prove Theorem 1.2, Theorem 1.3 and Theorem 1.4. We turn our attention to special constructions of blocking curves using Frobenius nonclassical plane curves in Section 4. In Section 5 we construct smooth curves passing through the projective triangle. Finally, we prove Theorem 1.6 and Theorem 1.7 in Section 6, and Theorem 1.8 and Theorem 1.9 in Section 7.

2. Preliminaries and Lemmata

This section is not meant to be read in isolation, and a reader may skip to Section 3 and refer back to this section when necessary.

2.1. **Basic definitions.** The primary geometric object of our study is a plane curve defined over a finite field. Recall that a plane curve $C \subset \mathbb{P}^2$ is defined by a homogeneous polynomial $F \in \mathbb{F}_q[x,y,z]$. We say that C is *irreducible* if F is an irreducible polynomial in $\mathbb{F}_q[x,y,z]$. Moreover, C is *geometrically irreducible* if F remains irreducible in the larger ring $\overline{\mathbb{F}_q}[x,y,z]$. A plane curve C is *smooth* if for every point $P \in C$, at least one of the partial derivatives F_x, F_y or F_z does not vanish at P. Note that a smooth plane curve is geometrically irreducible.

Recall that $\Phi \colon \mathbb{P}^2 \to \mathbb{P}^2$ is the *q-th power Frobenius map* defined by $\Phi[x:y:z] = [x^q : y^q : z^q]$. This definition will be especially useful in Section 4 when we discuss Frobenius nonclassical curves.

2.2. **Character sums.** Recall that a character χ of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is called a *multiplicative character* of $\mathbb{F}_q$. For a multiplicative character χ, its order r is the smallest positive integer such that $\chi^r = \chi_0$, where χ_0 is the trivial multiplicative character of $\mathbb{F}_q$. The following lemma is a classical application of Weil's bound for complete character sums; see for example [LN97, Exercise 5.66].

Lemma 2.1. *Let $r \geq 2$ be a positive integer. Let $q \equiv 1 \pmod r$ be a prime power. Let χ be a multiplicative character of $\mathbb{F}_q$ with order r. Let $a_1, a_2, \ldots, a_k$ be k distinct elements of $\mathbb{F}_q$, and let $\epsilon_1, \ldots, \epsilon_k \in \mathbb{C}$ be r-th roots of unity. Let N denote the number of $x \in \mathbb{F}_q$ such that $\chi(x + a_i) = \epsilon_i$ for $1 \leq i \leq k$. Then*

$$N \geq \frac{q}{r^k} - \left(k - 1 - \frac{k}{r} + \frac{1}{r^k}\right)\sqrt{q} - \frac{k}{r}.$$

We apply Lemma 2.1 to deduce two useful corollaries below. They will be used to show that the curves in Section 6 and Section 7 are blocking.

Corollary 2.2. *Let $r \geq 2$ be a positive integer. Let $q \equiv 1 \pmod{r}$ be a prime power such that $q > r^4$. Let χ be a multiplicative character of $\mathbb{F}_q$ with order r, and let $\omega_1, \omega_2 \in \mathbb{C}$ be two r-th roots of unity. Then for any $b, c \in \mathbb{F}_q^*$, there are $y, z \in \mathbb{F}_q$ such that $\chi(y) = \omega_1, \chi(z) = \omega_2$ and $by + cz = -1$.*

Proof. Note that $by + cz = -1$ is equivalent to $z = -\frac{b}{c}(y + \frac{1}{b})$. Thus, it suffices to find $y \in \mathbb{F}_q$ such that $\chi(y) = \omega_1$ and $\chi(y + \frac{1}{b}) = w_2\chi(-\frac{c}{b})$. Using Lemma 2.1 with $k = 2$, the number of such y is at least

$$\frac{q}{r^2} - \left(1 - \frac{2}{r} + \frac{1}{r^2}\right)\sqrt{q} - \frac{2}{r} = \left(\frac{q}{r^2} - \sqrt{q}\right) + \left(\frac{2}{r} - \frac{1}{r^2}\right)\sqrt{q} - \frac{2}{r} > \frac{\sqrt{q} - 2}{r} > 0$$

since $q > r^4$. Thus, such an element y exists. □

Corollary 2.3. *Let q be an odd prime power such that $q \geq 47$, and χ be the quadratic character of $\mathbb{F}_q$. Then for any nonzero $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha \neq \beta$, there is $x \in \mathbb{F}_q$, such that $\chi(x), \chi(x + \alpha), \chi(x + \beta)$ have the prescribed values (1 or -1).*

Proof. For $q \geq 47$, we have

$$\frac{q}{8} > \frac{5}{8}\sqrt{q} + \frac{3}{2}.$$

The result follows immediately from Lemma 2.1 with $k = 3$ and $r = 2$. □

2.3. **Irreducibility criterion.** In Section 6 we will construct a family of geometrically irreducible blocking curves. The following lemma provides a useful criterion to check the (absolute) irreducibility of a polynomial.

Lemma 2.4. *Let K be a field and let $f, g \in K[y, z]$ homogeneous polynomials such that $\gcd(f, g) = 1$. Assume that either f or g has a non-repeated irreducible factor. Then the polynomial*

$$F(x, y, z) = f(y, z)x^r + g(y, z)$$

is irreducible for each $r \geq 1$.

Proof. First, suppose $h(y, z)$ is an irreducible polynomial such that $h \mid g$ but $h^2 \nmid g$. Since $\gcd(f, g) = 1$, we know that $h \nmid f$. By Eisenstein's criterion with the underlying ring $K[y, z]$ (see for example [Gao01, Page 502]), the polynomial $f(y, z)x^r + g(y, z)$ is irreducible in the ring $(K[y, z])[x]$. Since $\gcd(f, g) = 1$, the polynomial is also irreducible in $K[x, y, z]$.

Next, suppose that $h(y, z)$ is an irreducible polynomial such that $h \mid f$ but $h^2 \nmid f$. By applying the same argument in the first paragraph, the polynomial $g(y, z)x^r + f(y, z)$ is irreducible. It follows that $f(y, z)x^r + g(y, z)$ is also irreducible. This is because the two polynomials are related by the transformation $x \mapsto 1/x$ and multiplication by x^r. □

2.4. **Divisors of $p - 1$.** In this subsection, we show that for any $\theta < 1/2$, there are infinitely many primes p with a divisor that is close to p^θ. We first recall some standard notations. For any real number x, let $\pi(x)$ be the number of primes up to x. For positive integers r and a such that $\gcd(r, a) = 1$, we use $\pi(x; r, a)$ to denote the number of primes up to x which are in the arithmetic progression $a + r\mathbb{Z}$. The prime number theorem for arithmetic progressions states that $\pi(x; r, a)$ is very close to $\pi(x)/\phi(r)$ if r is fixed and x is large. For our purposes, r is close to x^θ, so we need deeper tools from analytic number theory.

The following explicit version of Brun-Titchmarsh inequality is due to Montgomery and Vaughan [MV73].

Theorem 2.5 (Brun-Titchmarsh inequality)**.** *If $x > r$, then*

$$\pi(x; r, a) \leq \frac{2x}{\phi(r) \log \frac{x}{r}}.$$

We also need the following version of the celebrated Bombieri–Vinogradov theorem [Bom65].

Theorem 2.6 (Bombieri–Vinogradov theorem)**.** *Let $\theta < 1/2$. There is a constant C, such that*

$$\sum_{r \leq x^\theta} \max_{\gcd(a,r)=1} \left| \pi(x; r, a) - \frac{\pi(x)}{\phi(r)} \right| \leq \frac{Cx}{(\log x)^2}. \tag{1}$$

Corollary 2.7. *Let $0 < \theta < 1/2$ and $0 < A$ be fixed constants. There are infinitely many primes p such that $p - 1$ has a divisor in $[Ap^\theta/2, 2Ap^\theta]$.*

Proof. We prove the statement for the case $A = 1$; the proof for the general case is similar (but a bit messier).

Let $0 < \alpha < 1/4$ such that $\alpha^{-\theta} < 2$. Let x be sufficiently large so that $\alpha x^{1-\theta} > x^{1/2}$. By Bombieri–Vinogradov theorem, the inequality (1) holds. In particular, we can find some $r_0 \in [x^\theta/2, x^\theta]$ such that

$$\left| \pi(x; r_0, 1) - \frac{\pi(x)}{\phi(r_0)} \right| \leq \frac{2Cx}{x^\theta (\log x)^2} < \frac{2Cx}{\phi(r_0)(\log x)^2}.$$

On the other hand, Brun-Titchmarsh inequality implies that

$$\pi(\alpha x; r_0, 1) \leq \frac{2\alpha x}{\phi(r_0) \log \frac{\alpha x}{r_0}} \leq \frac{2\alpha x}{\phi(r_0) \log(\alpha x^{1-\theta})} \leq \frac{2\alpha x}{\phi(r_0) \log(x^{1/2})} = \frac{4\alpha x}{\phi(r_0) \log x}.$$

Combining the above estimates, we have

$$\pi(x; r_0, 1) - \pi(\alpha x; r_0, 1) \geq \frac{\pi(x)}{\phi(r_0)} - \frac{2Cx}{\phi(r_0)(\log x)^2} - \frac{4\alpha x}{\phi(r_0) \log x}.$$

Note that $4\alpha < 1$, so the prime number theorem implies that $\pi(x; r_0, 1) - \pi(\alpha x; r_0, 1) > 0$ holds for sufficiently large x. In particular, there is a prime $p \in (\alpha x, x]$ such that $p \equiv 1 \pmod{r_0}$ with $r_0 \in [x^\theta/2, x^\theta]$, which implies that $r_0 \in [p^\theta/2, (p/\alpha)^\theta] \subset [p^\theta/2, 2p^\theta]$. □

Remark 2.8. Let $P(a, r)$ be the least prime in an arithmetic progression $a \pmod{r}$, where a and r are coprime positive integers. Linnik [Lin44a, Lin44b] proved that there exist effectively computable constants C and L such that $P(a, r) \leq Cr^L$. The constant L is known as *Linnik's constant*. The best-known upper bound for L is 5, due to Xylouris [Xyl11]. Using Linnik's theorem with $r = 2^n$ and $L = 5$, one can give a simple proof for Corollary 2.7 when $\theta < 1/5$. However, in our application, we need the statement to be true for $\theta \leq 1/4$. We also remark that Corollary 2.7 is trivial if one replaces primes with prime powers.

2.5. **Point-line incidences.** The following lemma collects the three useful identities that will be repeatedly used in Section 3.

Lemma 2.9. *Let C be an irreducible blocking plane curve of degree d defined over a finite field $\mathbb{F}_q$. Suppose that t_i denotes the number of $\mathbb{F}_q$-lines intersecting $C(\mathbb{F}_q)$ in exactly i points. Let $N = |C(\mathbb{F}_q)|$. Then we have $t_0 = 0$ and $t_i = 0$ when $i > d$. Moreover,*

$$\sum_{i=1}^{d} t_i = q^2 + q + 1,$$

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

Proof. The proof relies on a standard counting of point-line incidences in two different ways. Note that the sums run up to $i = d$, because $t_i = 0$ for $i > d$ by Bézout's theorem which is applicable as C is irreducible. For complete details, see for example the proof of [AG22, Proposition 2.1]. □

Remark 2.10. The sequence $\{t_i\}$, known as the *intersection distribution*, makes sense for any point set S in $\mathbb{P}^2(\mathbb{F}_q)$. Such distribution is closely related to many problems in finite geometry [LP20, Remark 1.4]. In particular, Li and Pott [LP20] studied the sequence $\{t_i\}$ when S is the graph of a polynomial $f \in \mathbb{F}_q[x]$, and found connections to permutation polynomials [AGW11].

As an immediate corollary of Lemma 2.9, we have a criterion for showing that a blocking curve is nontrivially blocking.

Corollary 2.11. *If $C \subset \mathbb{P}^2$ is an irreducible blocking plane curve of degree $d < q+1$, then C is nontrivially blocking.*

As another corollary of Lemma 2.9, we obtain the following inequality which relates the degree and the number of rational points of a blocking curve, and the cardinality of the ground field.

Corollary 2.12. *Let C be an irreducible blocking plane curve of degree d over $\mathbb{F}_q$. Using the notation in Lemma 2.9, the following inequality holds:*

$$N(d(q+1)+1-N) \geq d(q^2+q+1).$$

Proof. By Lemma 2.9, we have

$$\sum_{i=1}^{d} t_i = q^2+q+1, \quad \sum_{i=1}^{d} it_i = (q+1)N, \quad \sum_{i=1}^{d} t_i \binom{i}{2} = \binom{N}{2}$$

where the third sum starts with $i = 1$ for convenience. Now, the last two equations imply that

$$\sum_{i=1}^{d} i^2 t_i = 2\sum_{i=1}^{d} t_i \binom{i}{2} + \sum_{i=1}^{d} it_i = N(N-1) + (q+1)N = N(N+q).$$

Thus,

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

which implies that

$$\sum_{i=1}^{d} (i-1)^2 t_i \leq (d-1)\sum_{i=1}^{d} (i-1)t_i = (d-1)(q+1)N - (d-1)(q^2+q+1).$$

On the other hand,

$$\sum_{i=1}^{d} (i-1)^2 t_i = \sum_{i=1}^{d} i^2 t_i - 2\sum_{i=1}^{d} it_i + \sum_{i=1}^{d} t_i = N(N+q) - 2(q+1)N + q^2 + q + 1.$$

Combining the two estimates above, we get

$$(d-1)(q+1)N-(d-1)(q^2+q+1) \geq N(N+q)-2(q+1)N+q^2+q+1 = N(N-q-2)+q^2+q+1.$$

Simplifying yields

$$N(d(q+1)+1-N) \geq d(q^2+q+1),$$

as desired. □

3. Low degree plane curves are not blocking

In this section, we prove Theorem 1.2 to establish that curves of low degree can never be blocking, and present an improved result in Theorem 3.3 for the case $q = p^n$ when $n \leq 4$. We also prove Theorem 1.3 and Theorem 1.4, which provide refined results for cubic and quartic curves, respectively.

3.1. **Proof of Theorem 1.2.** Before we proceed with the proof of Theorem 1.2, we present a quick lemma that allows us to reduce to the case of geometrically irreducible curves.

Lemma 3.1. *Let C be an irreducible plane curve of degree d defined over $\mathbb{F}_q$. Suppose that C is not geometrically irreducible. If $q \geq d^2/4$, then C is not blocking.*

Proof. Under the given hypothesis, it is well-known that $|C(\mathbb{F}_q)| \leq d^2/4$ [AG22, Remark 2.2]. Thus, the total number of $\mathbb{F}_q$-lines passing through some point of $C(\mathbb{F}_q)$ is at most

$$\frac{d^2}{4} \cdot (q+1) \leq q(q+1) < q^2+q^2+1$$

and hence there is some $\mathbb{F}_q$-line L which does not meet $C(\mathbb{F}_q)$. Thus, C is not blocking. □

Next, we give a proof of Theorem 1.2. We remark that Theorem 1.2 improves [AG22, Proposition 2.1] by the multiplicative factor given by $(\frac{1+\sqrt{2}}{2})^2 \approx 1.457$.

Proof of Theorem 1.2. Suppose, to the contrary, that C is blocking. In view of Lemma 3.1, we may assume that C is geometrically irreducible.

Let N denote the number of $\mathbb{F}_q$-points of C. Motivated by Corollary 2.12, we are led to consider the function $f(x) := x(d(q+1)+1-x)$. Note that $f(x)$ increases as a function of x whenever $0 \leq x < \frac{d(q+1)+1}{2}$.

Let us first show that N must be in the interval $\left(0, \frac{d(q+1)+1}{2}\right)$. By the Hasse-Weil bound for geometrically irreducible curves [AP96, Corollary 2.5]:

$$N \leq q+1+(d-1)(d-2)\sqrt{q}.$$

It suffices to establish $q+1+(d-1)(d-2)\sqrt{q} < \frac{d(q+1)+1}{2}$. Since $d \geq 4$ and $q \geq (d-1)^2(d-2)^4$, it follows that $q \geq 16(d-1)^2$. Therefore,

$$\begin{aligned}\frac{d(q+1)+1}{2} - q - 1 - (d-1)(d-2)\sqrt{q} &> \frac{(d-2)(q+1)}{2} - (d-1)(d-2)\sqrt{q} \\ &> (d-2)\left(\frac{q}{2} - (d-1)\sqrt{q}\right) \geq 0\end{aligned}$$

as desired. This shows N is in the interval where $f(x)$ is increasing. As a result,

$$\begin{aligned}&N(d(q+1)+1-N) = f(N) \leq f(q+1+(d-1)(d-2)\sqrt{q}) = \\ &= (d-1)(q+1)^2+q+1+((d-2)(q+1)+1)(d-1)(d-2)\sqrt{q}-(d-1)^2(d-2)^2q.\end{aligned}$$

Thus, Corollary 2.12 implies that

$$q^2 \leq 2(d-1)q + (d-1)(d-2)^2 q\sqrt{q} + (d-1)^2(d-2)\sqrt{q} - (d-1)^2(d-2)^2 q.$$

Since $q \geq 4(d-1)^2$ and $d \geq 4$, we have

$$(d-1)^2(d-2)^2 q \geq 2(d-1)^3(d-2)^2\sqrt{q}, \quad (d-1)^2(d-2)^2 q \geq 4(d-1)q,$$

thus

$$(d-1)^2(d-2)^2 q \geq 2(d-1)q + (d-1)(d-2)^2\sqrt{q}.$$

We conclude that

$$q^2 \leq (d-1)(d-2)^2 q\sqrt{q},$$

that is, $q \leq (d-1)^2(d-2)^4$. Since q is a prime power and $(d-1)^2(d-2)^2$ has at least two distinct prime factors for $d \geq 4$, we deduce that $q < (d-1)^2(d-2)^4$. This is a contradiction, and the proof is complete. □

Before discussing our next result, we mention a fundamental result on blocking sets. A blocking set of size less than $3(q+1)/2$ is known as a *small blocking set*. Szőnyi [Sző97a] proved that a small blocking set must have a special incidence structure.

Theorem 3.2 ([Sző97a])**.** *If $B \subset \mathbb{P}^2(\mathbb{F}_q)$ is a nontrivial blocking set of size less than $3(q+1)/2$, then each line intersects B in 1 modulo p points.*

When $q = p^n$, where $n \leq 4$, the $O(d^6)$ bound in Theorem 1.2 can be further improved to $O(d^4)$.

Theorem 3.3. *Let C be an irreducible plane curve of degree $d \geq 4$ defined over $\mathbb{F}_q$, where $q = p^n$ such that $n \in \{1,2,3,4\}$. If $q \geq 4(d-1)^2(d-2)^2$, then C is not blocking.*

Proof. Suppose to the contrary that C is blocking. In view of Lemma 3.1, we may assume that C is geometrically irreducible. Using the Hasse-Weil bound and the hypothesis $\frac{q}{4} \geq (d-1)^2(d-2)^2$, we obtain:

$$|C(\mathbb{F}_q)| \leq q + 1 + (d-1)(d-2)\sqrt{q} \leq q + 1 + \frac{\sqrt{q}}{2}\sqrt{q} = \frac{3q}{2} + 1 < \frac{3(q+1)}{2}.$$

Since C is irreducible and $d < q+1$, it follows that C is nontrivially blocking by Corollary 2.11 (that is, $C(\mathbb{F}_q)$ does not contain all the $\mathbb{F}_q$-points of an $\mathbb{F}_q$-line since that would make $C(\mathbb{F}_q)$ a blocking set in a trivial manner). By Theorem 3.2, each line intersects $C(\mathbb{F}_q)$ in 1 modulo p points. Note that $p^4 \geq q \geq 4(d-1)^2(d-2)^2$, so $p^2 \geq 2(d-1)(d-2)$, which implies that $p \geq d$ provided that $d \geq 4$. This forces $t_1 = q^2+q+1$ and $t_i = 0$ for $i > 1$ (since $p \geq d$) by Lemma 2.9. Applying Lemma 2.9 again, we obtain the equation,

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

which is impossible since $(q+1) \nmid (q^2+q+1)$. □

Remark 3.4. When $q = p$ is a prime, one can obtain a simpler proof of Theorem 3.3 by comparing the lower bound given by $\frac{3}{2}(p+1)$ in Blokhuis' theorem [Blo94] with the Hasse-Weil bound.

3.2. **Cubic plane curves.** We will next show that a cubic plane curve is almost never blocking.

Proof of Theorem 1.3. Assume, to the contrary, that $C(\mathbb{F}_q)$ is a blocking set. Let $N = \#C(\mathbb{F}_q)$. As before, let t_i denote the number of $\mathbb{F}_q$-lines intersecting $C(\mathbb{F}_q)$ in i points. By Lemma 2.9,

$$\begin{aligned} t_1 + t_2 + t_3 &= q^2 + q + 1, \\ t_1 + 2t_2 + 3t_3 &= N(q+1), \\ 2t_2 + 6t_3 &= N(N-1). \end{aligned}$$

Subtracting the first equation from the second, we get $t_2 + 2t_3 = N(q+1) - (q^2+q+1)$. Combining this equation with the third displayed equation, we get:

$$\begin{aligned} t_2 &= 3(t_2 + 2t_3) - (2t_2 + 6t_3) \\ &= 3N(q+1) - 3(q^2+q+1) - N(N-1). \end{aligned}$$

Since $t_2 \geq 0$, we obtain:

$$3N(q+1) - 3(q^2+q+1) - N(N-1) \geq 0$$

which is a quadratic inequality in N:

$$N^2 - (3q+4)N + 3(q^2+q+1) \leq 0. \tag{2}$$

The discriminant is given by:

$$\Delta = (3q+4)^2 - 12(q^2+q+1) = -(3q^2 - 12q - 4) < 0$$

for $q \geq 5$. Indeed, $3q^2 - 12q - 4 = 3(q-5)^2 + 18q - 79 > 0$ for $q \geq 5$. Since $\Delta < 0$, the quadratic function $f(N) = N^2 - (3q+4)N + 3(q^2+q+1)$ has no real roots, and therefore should always be positive. This contradicts the inequality (2), and completes the proof. □

Example 3.5. Consider the following three plane cubic curves:

- $C_2 : x^3 + y^3 + z^3 = 0$ defined over $\mathbb{F}_2$;
- $C_3 : y^2z - x^3 - x^2z - xz^2 = 0$ defined over $\mathbb{F}_3$;
- $C_4 : x^3 + y^3 + z^3 = 0$ defined over $\mathbb{F}_4$.

One can show that C_i is a smooth blocking curve for each $i = 2, 3, 4$. Note C_4 is an example of Hermitian curve mentioned earlier in Example 1.5. Thus, the condition $q \geq 5$ required in Theorem 1.3 is both necessary and sharp.

Remarks 3.6. The irreducibility hypothesis on the cubic curve C is necessary. Indeed, a reducible cubic curve C over $\mathbb{F}_q$ must have a component of degree 1, that is, an $\mathbb{F}_q$-line. But then $C(\mathbb{F}_q)$ would be a trivial blocking set.

Remark 3.7. The same proof works for $(k, 3)$-arcs. More precisely, if $\mathcal{A}$ is a $(k, 3)$-arc in $\mathbb{P}^2(\mathbb{F}_q)$ with $q \geq 5$, then $\mathcal{A}$ is not a blocking set.

3.3. **Quartic plane curves.** Obtaining a more refined result for quartic plane curves is more complicated, and our proof below crucially relies on the smoothness hypothesis.

Proof of Theorem 1.4. Assume, to the contrary, that $C(\mathbb{F}_q)$ is a blocking set. By Lemma 2.9,

$$\begin{aligned} t_1 + t_2 + t_3 + t_4 &= q^2 + q + 1, \\ t_1 + 2t_2 + 3t_3 + 4t_4 &= N(q+1), \\ 2t_2 + 6t_3 + 12t_4 &= N(N-1). \end{aligned}$$

We subtract the first equation from the second to get:

$$t_2 + 2t_3 + 3t_4 = N(q+1) - (q^2+q+1). \tag{3}$$

Now,

$$t_2 + 2t_3 + 3t_4 = \frac{t_2+t_3}{2} + \frac{2t_2+6t_3+12t_4}{4} \geq \frac{t_2}{2} + \frac{N(N-1)}{4}. \tag{4}$$

Let $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$. Consider the $\mathbb{F}_q$-line L_P joining P and its Frobenius image $\Phi(P)$. Note that $L_P = L_{\Phi(P)}$. We claim that the number of such lines is exactly

$$\frac{\#C(\mathbb{F}_{q^2}) - \#C(\mathbb{F}_q)}{2}. \tag{5}$$

In order to prove the formula (5), it suffices to show that $L_P = L_{P'}$ if and only if $\{P, \Phi(P)\} = \{P', \Phi(P')\}$. Assuming $\{P, \Phi(P)\} \neq \{P', \Phi(P')\}$, the condition $L_P = L_{P'}$ would imply that then $L_P \cap C$ has 4 points, namely $P, \Phi(P), P', \Phi(P')$, implying that $L_P \cap C(\mathbb{F}_q) = \emptyset$, contradicting the assumption that C is blocking. This completes the proof of our claim that the number of distinct lines L_P (joining P and its Frobenius image $\Phi(P)$) is given by the formula (5).

Given $P \in C(\mathbb{F}_{q^2}) \setminus C(\mathbb{F}_q)$, we know that $L_P \cap C$ has 4 points over $\overline{\mathbb{F}_q}$ counted with multiplicity. Moreover, 2 of those 4 points are already accounted by P and $\Phi(P)$, neither of which is an $\mathbb{F}_q$-point. Thus, either L_P contributes to t_2 or L is a tangent line to C at some $\mathbb{F}_q$-point, that is, L meets C at some $\mathbb{F}_q$-point with multiplicity exactly 2. Since C is smooth, the number of tangent lines is at most $N = \#C(F_q)$. Therefore,

$$t_2 \geq \frac{\#C(\mathbb{F}_{q^2}) - \#C(\mathbb{F}_q)}{2} - N. \tag{6}$$

Using the Hasse-Weil bound, $\#C(\mathbb{F}_{q^2}) \geq q^2 + 1 - 6q$. Thus, equation (6) yields that

$$t_2 \geq \frac{q^2+1-6q-N}{2} - N. \tag{7}$$

Substituting the lower bound for t_2 from equation (7) into the equation (4), we obtain

$$t_2 + 2t_3 + 3t_4 \geq \frac{q^2+1-6q-N}{4} - \frac{N}{2} + \frac{N(N-1)}{4}. \tag{8}$$

Therefore, equations (3) and (8) yield that

$$N(q+1) - (q^2+q+1) \geq \frac{q^2+1-6q-N}{4} - \frac{N}{2} + \frac{N(N-1)}{4}. \tag{9}$$

Rearranging inequality (9) into a quadratic equation in N, we obtain:

$$\frac{1}{4}N^2 - (2+q)\,N + \frac{5}{4}q^2 - \frac{1}{2}q + \frac{5}{4} \leq 0. \tag{10}$$

The discriminant of the quadratic from (10) is given by:

$$\Delta = (2+q)^2 - \left(\frac{5}{4}q^2 - \frac{1}{2}q + \frac{5}{4}\right) = -\frac{1}{4}\left(q^2 - 18q - 11\right).$$

Note that $\Delta < 0$ for $q \geq 19$, which contradicts the earlier inequality $\frac{1}{4}N^2 - (2+q)\,N + \frac{5}{4}q^2 - \frac{1}{2}q + \frac{5}{4} \leq 0$. Thus, the desired conclusion from Theorem 1.4 is proved for $q \geq 19$. □

Remarks 3.8. The Hermitian curve from Example 1.5 gives an example of a smooth quartic blocking curve when $q = 9$. We do not know if there exist smooth or irreducible blocking plane curves of degree 4 over $\mathbb{F}_q$ when $q \in \{11, 13, 16, 17\}$. The brute force method of enumerating all irreducible quartic plane curves over $\mathbb{F}_q$ is infeasible.

4. Connection with Frobenius nonclassical plane curves

In this section, we construct blocking plane curves that arise from Frobenius nonclassical curves. The concept of Frobenius nonclassical curves first naturally appeared in the work by Stöhr and Voloch [SV86] in their new proof of the Riemann hypothesis for curves over finite fields. Afterwards, Hefez and Voloch carried out a thorough investigation of these curves, and in particular, determined the precise number of $\mathbb{F}_q$-points on a nonsingular Frobenius nonclassical plane curve of degree d [HV90, Theorem 1]. The abundance of points on Frobenius nonclassical plane curves can be used to construct new complete arcs [GPTU02]. Our approach will be similar to [GPTU02], except we are interested in using these curves to construct blocking sets instead of arcs.

While Frobenius nonclassical curves can live in a projective space of arbitrary dimension, we will primarily focus on the case of plane curves. We begin with a fundamental definition.

Definition 4.1. Suppose $C = \{F = 0\}$ is a plane curve defined over $\mathbb{F}_q$. We say that C is *Frobenius nonclassical* if the polynomial $x^q F_x + y^q F_y + z^q F_z$ is divisible by F.

Geometrically, a plane curve C is Frobenius nonclassical if and only if for every non-singular point $P \in C$, the tangent line $T_P C$ contains $\Phi(P)$. Our goal is to prove Theorem 4.3 on the existence of blocking plane curves of degree $d = o(q)$ where $q = p^n$ is a prime power with $n \geq 2$; see Remark 4.4 for more details on the size of the degree. We begin with a general result.

Proposition 4.2. *Let C be a smooth plane curve of degree d defined over $\mathbb{F}_q$ where $p = \mathrm{char}(\mathbb{F}_q) \geq 3$. Suppose that C is Frobenius nonclassical. Then C is blocking.*

Proof. Since C is a smooth Frobenius nonclassical plane curve, it follows that C is non-reflexive [HV90, Proposition 1]. Therefore, $d \equiv 1 \pmod{p}$ by Pardini's theorem [Par86, Corollary 2.2]. Applying [ADL22, Corollary 2.3], we obtain that $C(\mathbb{F}_q)$ is a blocking set. □

Theorem 4.3. *Suppose $q = p^n$ where $n \geq 2$ and $p \geq 3$. Let $1 \leq n' < n$ be a positive divisor of n, and set $q' = p^{n'}$. There exists a smooth blocking plane curve defined over $\mathbb{F}_q$ with degree $d = \frac{q-1}{q'-1}$.*

Proof. Consider the curve $C \subset \mathbb{P}^2$ defined by the equation,

$$x^{\frac{q-1}{q'-1}} + y^{\frac{q-1}{q'-1}} + z^{\frac{q-1}{q'-1}} = 0.$$

The smoothness of the curve C is clear. Moreover, C is Frobenius nonclassical over $\mathbb{F}_q$. Indeed,

$$\begin{aligned} x^q F_x + y^q F_y + z^q F_z &= x^{\frac{q-1}{q'-1}-1+q} + y^{\frac{q-1}{q'-1}-1+q} + z^{\frac{q-1}{q'-1}-1+q} \\ &= x^{\frac{q'(q-1)}{q'-1}} + y^{\frac{q'(q-1)}{q'-1}} + z^{\frac{q'(q-1)}{q'-1}} = F^{q'}. \end{aligned}$$

In particular, $x^q F_x + y^q F_y + z^q F_z$ is divisible by F. We conclude that $C = \{F = 0\}$ is a smooth Frobenius nonclassical plane curve of degree $d = \frac{q-1}{q'-1}$. The desired result follows immediately from Proposition 4.2. □

Remark 4.4. As an illustration of Theorem 4.3, we can let $n' = 1$. We obtain a smooth blocking plane curve of degree $d = \frac{q-1}{p-1}$ over $\mathbb{F}_q$ for every $q = p^n$ with $n \geq 2$. For example, when $q = p^3$ with p an odd prime, this yields a blocking curve of degree $d = \frac{q-1}{p-1} = p^2 + p + 1$. Note that $d \approx q^{2/3}$, and that the exponent $2/3$ is smaller than the exponent $3/4$ in Theorem 1.7. For $n \geq 4$, we obtain a smooth blocking plane curve of degree $d \approx q^{(n-1)/n} = q^{1-1/n}$ that works for every q. However, Theorem 1.7 has the advantage that it works in the case when $q = p$ is a prime.

Remark 4.5. Let q be a square. The Hermitian curve $\mathcal{H}$ given by the equation $x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0$ from Example 1.5 is an example of Frobenius nonclassical plane curve over $\mathbb{F}_q$. In fact, $d = \sqrt{q} + 1$ is the smallest possible degree of a geometrically irreducible Frobenius nonclassical plane curve over $\mathbb{F}_q$. Moreover, every such curve of degree $d = \sqrt{q} + 1$ is $\mathbb{F}_q$-isomorphic to $\mathcal{H}$ [BH17, Corollary 3.2].

5. Smooth curves passing through the projective triangle

Theorem 5.1. *Let $q \equiv 3 \pmod 4$ be a prime power with $p > 3$. There exists a smooth curve C of degree $d = \frac{q+3}{2}$ defined over $\mathbb{F}_q$ such that $C(\mathbb{F}_q)$ is nontrivially blocking, and $C(\mathbb{F}_q)$ contains the projective triangle Δ.*

Proof. Consider the plane curve C defined by the equation,

$$xy(x^{(q-1)/2} + y^{(q-1)/2}) + yz(y^{(q-1)/2} + z^{(q-1)/2}) + zx(z^{(q-1)/2} + x^{(q-1)/2}) = 0.$$

Note that C passes through $[1 : 0 : 0]$, $[0 : 1 : 0]$, and $[0 : 0 : 1]$. Moreover, for any $s \in \mathbb{F}_q^*$, we have $(-s^2)^{(q-1)/2} = -1$ since $(q-1)/2$ is odd by hypothesis. As a result, the curve C passes through each point of the projective triangle

$$\Delta = \{[0 : 1 : -s^2], [1 : -s^2 : 0], [-s^2 : 0 : 1] \mid s \in \mathbb{F}_q\}$$

and thus C is nontrivially blocking by Corollary 2.11 assuming that C is irreducible. It remains to show that C is smooth. Note that smooth plane curves are irreducible.

The defining polynomial for C can be rewritten as:

$$F = x^{(q+1)/2}(y + z) + y^{(q+1)/2}(z + x) + z^{(q+1)/2}(x + y).$$

Assume, to the contrary, that C is singular at a point $P = [x : y : z]$. Then the three partial derivatives F_x, F_y and F_z must vanish at P. Writing down $F_x = F_y = F_z = 0$ and multiplying both sides of each equation by 2 leads to the following:

$$\begin{aligned} x^{(q-1)/2}(y + z) + 2y^{(q+1)/2} + 2z^{(q+1)/2} &= 0, \\ 2x^{(q+1)/2} + y^{(q-1)/2}(z + x) + 2z^{(q+1)/2} &= 0, \\ 2x^{(q+1)/2} + 2y^{(q+1)/2} + z^{(q-1)/2}(x + y) &= 0. \end{aligned}$$

Let $m = (q-1)/2$ for simplicity. We can rewrite the above system of equations in the matrix form $M\mathbf{v} = \mathbf{0}$ where

$$M = \begin{pmatrix} y + z & 2y & 2z \\ 2x & z + x & 2z \\ 2x & 2y & x + y \end{pmatrix} \quad \text{and} \quad \mathbf{v} = \begin{pmatrix} x^m \\ y^m \\ z^m \end{pmatrix}.$$

Since $\mathbf{v} \neq \mathbf{0}$ by assumption, it follows that $\det(M) = 0$. After expanding the determinant and dividing both sides by 3 (which is permissible as $p > 3$), we obtain the relation:

$$x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2 = 6xyz. \tag{11}$$

The system of equations on the partial derivatives above can also be written as $N\mathbf{w} = 0$ where

$$N = \begin{pmatrix} 0 & x^m + 2y^m & x^m + 2z^m \\ y^m + 2x^m & 0 & y^m + 2z^m \\ z^m + 2x^m & z^m + 2y^m & 0 \end{pmatrix} \text{ and } \mathbf{w} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Since $\mathbf{w} \neq \mathbf{0}$ by assumption, it follows that $\det(N) = 0$. After expanding the determinant and factoring, we obtain the relation:

$$6(x^m + y^m + z^m)(x^m y^m + y^m z^m + z^m x^m) = 0 \tag{12}$$

Since $p > 3$, we can conclude that either $x^m + y^m + z^m = 0$ or $x^m y^m + y^m z^m + z^m x^m = 0$.

Case 1. $x^m + y^m + z^m = 0$.

In this case, we can substitute $x^m = -y^m - z^m$ into the equation $x^m(y+z) + 2y^{m+1} + 2z^{m+1} = 0$ given by the vanishing of the partial derivative F_x. We obtain,

$$-(y^m + z^m)(y + z) + 2y^{m+1} + 2z^{m+1} = (y - z)(y^m - z^m) = 0. \tag{13}$$

Equation (13) yields that $y^m = z^m$. By symmetry, we can apply the same argument to the equations given by $F_y = 0$ and $F_z = 0$ to get $z^m = x^m$, and also, $x^m = y^m$. We can then conclude that $x^m = y^m = z^m$, and thus $x^m + y^m + z^m = 0$ implies that $3x^m = 0$. Since $p > 3$, we must have $x = y = z = 0$, which is a contradiction.

Case 2. $x^m y^m + y^m z^m + z^m x^m = 0$.

We split the analysis into two sub-cases.

Case 2.1. $xyz = 0$.

Without loss of generality, suppose $z = 0$. Then the equation $F_z = 0$ becomes:

$$2x^{m+1} + 2y^{m+1} = 0. \tag{14}$$

Now, combining $z = 0$ and $x^m y^m + y^m z^m + z^m x^m = 0$, we must have $x^m y^m = 0$, that is, either $x = 0$ or $y = 0$. However, both possibilities imply $x = y = 0$ using (14), which is a contradiction, since at least one of x, y, z must be non-zero.

Case 2.2. $xyz \neq 0$.

We introduce new variables $A = 1/x, B = 1/y$ and $C = 1/z$. The relation $x^m y^m + y^m z^m + z^m x^m = 0$ implies

$$A^m + B^m + C^m = 0. \tag{15}$$

The defining equation for the curve can be expressed as,

$$\frac{B + C}{A^{m+1}BC} + \frac{C + A}{B^{m+1}CA} + \frac{A + B}{C^{m+1}AB} = 0.$$

After multiplying both sides by ABC, we get

$$\frac{B + C}{A^m} + \frac{C + A}{B^m} + \frac{A + B}{C^m} = 0.$$

The last equation can be rewritten as,

$$C \cdot \left(\frac{1}{A^m} + \frac{1}{B^m}\right) + B \cdot \left(\frac{1}{C^m} + \frac{1}{A^m}\right) + A \cdot \left(\frac{1}{B^m} + \frac{1}{C^m}\right) = 0.$$

Combining the last relation with (15),

$$0 = C \cdot \left(\frac{A^m + B^m}{(AB)^m}\right) + B \cdot \left(\frac{C^m + A^m}{(CA)^m}\right) + A \cdot \left(\frac{B^m + C^m}{(BC)^m}\right)$$

$$= C \cdot \frac{(-C^m)}{(AB)^m} + B \cdot \frac{(-B^m)}{(CA)^m} + A \cdot \frac{(-A^m)}{(BC)^m}.$$

Next, we multiply the last equation by $(ABC)^m$ to arrive to,

$$0 = C^{2m+1} + B^{2m+1} + A^{2m+1}.$$

Recalling that $m = \frac{q-1}{2}$, we have $2m + 1 = q$. Thus,

$$0 = C^q + B^q + A^q = (A + B + C)^q$$

as we are working in characteristic p. We conclude that $A + B + C = 0$, or equivalently, $xy + yz + zx = 0$. In particular, we must have $(x + y + z)(xy + yz + zx) = 0$, that is,

$$x^2y + xy^2 + y^2z + yz^2 + z^2x + zx^2 + 3xyz = 0. \tag{16}$$

Finally, combining (11) and (16), we conclude that

$$6xyz + 3xyz = 0 \;\Rightarrow\; 9xyz = 0 \;\Rightarrow\; xyz = 0$$

as we are assuming $p > 3$. This contradicts the assumption that $xyz \neq 0$.

We deduce that the curve C is smooth, and the proof is complete. □

Remark 5.2. Note that $(q+3)/2$ is a lower bound on the degree of an irreducible curve that passes through all the points of the projective triangle. Indeed, the intersection between such a curve and the line $x = 0$ includes the points $\{[0 : 1 : -s^2] \mid s \in \mathbb{F}_q^*\} \cup \{[0 : 1 : 0], [0 : 0 : 1]\}$. Since there are at least $(q - 1)/2 + 2 = (q + 3)/2$ intersection points, the degree must be at least $(q + 3)/2$ by Bézout's theorem. We have shown that this is tight when $q \equiv 3 \pmod 4$.

Note that $(p+3)/2$ is also a lower bound on the degree of an irreducible curve that passes through a blocking set of Rédei type over $\mathbb{F}_p$. A blocking set B is of *Rédei type* if there is a line L such that $|B \cap L| = |B| - q$. For example, the projective triangle is of Rédei type. Blokhuis [Blo94] showed each nontrivial blocking set in $\mathbb{P}^2(\mathbb{F}_p)$ has size at least $3(p + 1)/2$, and so a nontrivial blocking set of Rédei type in $\mathbb{P}^2(\mathbb{F}_p)$ contains a line L with at least $3(p + 1)/2 - p = (p + 3)/2$ points. In fact, Gács [Gác03] showed that if a blocking set of Rédei type in $\mathbb{P}^2(\mathbb{F}_p)$ is not projectively equivalent to the projective triangle, then it has size at least $p + 2(p - 1)/3 + 1$. It follows that any irreducible plane curve passing through a Rédei type blocking set other than the projective triangle (and its image under a projective transformation) must have degree at least $2p/3$.

Remark 5.3. Note that our proof relies on the fact that -1 is a non-square in $\mathbb{F}_q$ provided that $q \equiv 3 \pmod 4$. When $q \equiv 1 \pmod 4$, -1 is a square in $\mathbb{F}_q$, and one can instead consider the curve given by,

$$xy(x^{(q-1)/2} - y^{(q-1)/2}) + yz(y^{(q-1)/2} - z^{(q-1)/2}) + zx(z^{(q-1)/2} - x^{(q-1)/2}) = 0$$

which does pass through the points of the projective triangle, and hence is a blocking curve. However, the curve above is reducible (in fact, contains the lines $x = y$, $y = z$ and $z = x$). Nonetheless, we believe that there is a smooth degree $\frac{q+3}{2}$ curve that passes through the points of the projective triangle when $q \equiv 1 \pmod 4$. In fact, for every homogeneous polynomial $g(x, y, z)$ of degree $\frac{q-3}{2}$, any plane curve defined by

$$xy(x^{(q-1)/2} - y^{(q-1)/2}) + yz(y^{(q-1)/2} - z^{(q-1)/2}) + zx(z^{(q-1)/2} - x^{(q-1)/2}) + xyz \cdot g(x, y, z) = 0$$

passes through the projective triangle, and thus, is a blocking curve. The subtle point is to find a suitable g to ensure that the curve is smooth. We believe that already taking $g(x, y, z) = x^{(q-3)/2}$ would produce a smooth curve, but we were unable to prove this for all $q \equiv 1 \pmod 4$.

6. Constructions of irreducible and smooth blocking curves

The fact that the projective triangle is a blocking set relies on nice properties of squares and non-squares. Inspired by this observation, we provide a systematic approach to constructing blocking curves using power residues in the following proposition.

Proposition 6.1. *Let $r \geq 2$ be a positive integer. Let $q \equiv 1 \pmod{r}$ be a prime power such that $q > r^4$. Let $f, g, h \in \mathbb{F}_q[x, y, z]$ be homogeneous polynomials with the same degree, such that $f = -g - h$, $f(1, 0, 0) = 0, g(0, 1, 0) = 0$, and $h(0, 0, 1) = 0$. Consider the curve C defined by*

$$f(x, y, z)x^m + g(x, y, z)y^m + h(x, y, z)z^m = 0,$$

where $m = (q - 1)/r$. Then C is blocking.

Proof. By hypothesis, it is clear that C passes through the points $[0 : 0 : 1], [0 : 1 : 0], [1 : 0 : 0]$. Moreover, since $f = -g - h$, the curve C passes through $[1 : y : z]$ whenever y and z are r-th powers in $\mathbb{F}_q^*$. Thus, it suffices to show that

$$B = \{[0 : 0 : 1], [0 : 1 : 0], [1 : 0 : 0]\} \cup \{[1 : y : z] \mid y \text{ and } z \text{ are } r\text{-th powers in } \mathbb{F}_q^*\}$$

forms a blocking set.

Consider an $\mathbb{F}_q$-line $L\colon ax + by + cz = 0$. If $abc = 0$, then the line L contains a point in $\{[0 : 0 : 1], [0 : 1 : 0], [1 : 0 : 0]\}$. Next assume that $abc \neq 0$. We may further assume that $a = 1$. To show $B \cap L \neq \emptyset$, it suffices to show that $by + cz = -1$ holds for some y and z that are r-th powers in $\mathbb{F}_q^*$. This is guaranteed by Corollary 2.2. □

Nonetheless, it is not clear which curves in the family given by the previous proposition are smooth or irreducible. By specializing the choice of f, g, h, we construct a geometrically irreducible blocking curve in every degree starting from $d = \frac{q-1}{r} + 1$.

Theorem 6.2. *Let $r \geq 2$ be a positive integer. Let $q \equiv 1 \pmod{r}$ be a prime power such that $q > r^4$. Let $k \in \mathbb{F}_q^*$ such that $-k$ is not an r-th power in $\mathbb{F}_q^*$. Let $m = \frac{q-1}{r}$. Then the curve C defined by*

$$-(ky^\ell + z^\ell)x^m + z^\ell y^m + ky^\ell z^m = 0$$

is geometrically irreducible and nontrivially blocking for each $\ell \geq 1$.

Proof. We first show that $\gcd(ky^\ell + z^\ell, z^\ell y^m + ky^\ell z^m) = 1$. It suffices to show that there are no $y, z \neq 0$ in $\overline{\mathbb{F}_q}$ such that $ky^\ell + z^\ell = 0$ and $y^{m-\ell} + kz^{m-\ell} = 0$ hold at the same time. Otherwise, we would have,

$$z^\ell = -ky^\ell, z^{m-\ell} = (-k)^{-1}y^{m-\ell}.$$

This implies that

$$(-k)^{m-\ell}y^{\ell(m-\ell)} = z^{\ell(m-\ell)} = (-k)^{-\ell}y^{\ell(m-\ell)},$$

thus $(-k)^m = 1$, which implies that $-k$ is an r-th power in $\mathbb{F}_q^*$, violating the assumption.

Next, we show that C is geometrically irreducible. Since $p \nmid m = (q-1)/r$, we know that either $p \nmid \ell$ or $p \nmid (m - \ell)$. In either case, we can apply Lemma 2.4 to the polynomial

$$-(ky^\ell + z^\ell)x^m + (z^\ell y^m + ky^\ell z^m)$$

seen over the field $\overline{\mathbb{F}_q}$. Indeed, $z^\ell y^m + ky^\ell z^m$ has a non-repeated factor if $p \nmid (m - \ell)$ and $ky^\ell + z^\ell$ has a non-repeated factor if $p \nmid \ell$.

By Proposition 6.1, C is blocking. Thus, it remains to show that C is nontrivially blocking; note that since C has potentially large degree, Corollary 2.11 cannot be applied and it may still contain

all the $\mathbb{F}_q$-points of some $\mathbb{F}_q$-line despite being geometrically irreducible. However, observe that the curve C does not pass through $[1 : y : z]$ where y is an r-th power and z is not an r-th power, for otherwise $-(ky^\ell + z^\ell) + z^\ell + ky^\ell z^m = 0$, which implies that $y = 0$ since $z^m \neq 1$, a contradiction.

Now, suppose that the equation of a line L is given by $ax + by + cz = 0$ where $a, b, c \in \mathbb{F}_q$; we need to show there is an $\mathbb{F}_q$-point on L which is not on C.

If $abc \neq 0$, we can assume $a = 1$. Then any point $[1 : y : z]$ which lies on L satisfies $by + cz = -1$. We can apply Corollary 2.2 to find some r-th power y and some non-r-th power z which satisfies this relation; but such a point does not lie on the curve C by the above discussion. It remains to analyze the case $abc = 0$.

When $a = 0$, $b = 0$ and $c \neq 0$, then the line L is given by $z = 0$. In this case, $L \cap C$ only consists of two points $[1 : 0 : 0]$ and $[0 : 1 : 0]$. Similarly, when $a = 0$, $c = 0$ and $b \neq 0$, then $L = \{y = 0\}$ and $L \cap C$ only consists of $[1 : 0 : 0]$ and $[0 : 0 : 1]$.

When $a = 0$ and $bc \neq 0$, the equation of L is given by $by + cz = 0$, we get $y = (-c/b)z$. There are two cases to consider.

Case 1. $-c/b$ is not a r-th power in $\mathbb{F}_q$.
Then L contains the point $[1 : 1 : -c/b]$. Since 1 is an r-th power and $-c/b$ is a non-r-th power in $\mathbb{F}_q$, such a point is not contained in C.

Case 2. $-c/b$ is an r-th power in $\mathbb{F}_q$.
Then L contains a point $[1 : y_0 : z_0]$ with $y_0^m = z_0^m = \omega$ where $\omega \notin \{0, 1\}$. We claim that this $\mathbb{F}_q$-point is not on C. Otherwise,

$$-(ky_0^\ell + z_0^\ell) + z_0^\ell y_0^m + ky_0^\ell z_0^m = (\omega - 1)(ky_0^\ell + z_0^\ell) = 0.$$

This forces $ky_0^\ell + z_0^\ell = 0$, and also $z_0^\ell y_0^m + ky_0^\ell z_0^m = 0$. This contradicts the earlier statement that $\gcd(z^\ell + ky^\ell, z^\ell y^m + ky^\ell z^m) = 1$.

When $a \neq 0$ and $b = c = 0$, then line L is given by $x = 0$. Note that the point $[0 : 1 : 1]$ is on the line $x = 0$ but not on the curve C, since $-k$ is a non-r-th power implies that $k \neq -1$.

Finally we consider the case $a \neq 0$, and exactly one of $b = 0$ or $c = 0$ holds. Observe that the curve does not pass through $[1 : y : 0]$ for $y \neq 0$ and $[1 : 0 : z]$ for $z \neq 0$. If $b = 0$, then L contains $[1 : 0 : z_0]$ for some nonzero z_0 and if $c = 0$ then L contains $[1 : y_0 : 0]$ for some nonzero y_0. □

One can check that when $\ell \geq 2$, the curve in Theorem 6.2 is singular at the points $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$. Next, we will show that when $\ell = 1$, the above construction in fact gives a smooth blocking curve.

Theorem 6.3. *Let $r \geq 2$ be a positive integer. Let $q \equiv 1 \pmod{r}$ be a prime power such that $q > r^4$ and $p \nmid (r^2 - 1)$. Let $k \in \mathbb{F}_q^*$ such that $-k$ is not an r-th power in $\mathbb{F}_q^*$, and set $m = \frac{q-1}{r}$. Then the curve C defined by*

$$F(x, y, z) = -(ky + z)x^m + zy^m + kyz^m = 0$$

is smooth and nontrivially blocking.

Proof. We have shown in Theorem 6.2 that C is nontrivially blocking. It suffices to show that C is smooth.

Suppose $P = [x : y : z]$ is a singular point of C. The conditions $F_x(P) = 0$, $F_y(P) = 0$ and $F_z(P) = 0$ become, after multiplying both sides by r,

$$(ky + z)x^{m-1} = 0,$$
$$-rkx^m - zy^{m-1} + rkz^m = 0,$$

$$-rx^m + ry^m - kyz^{m-1} = 0.$$

We can rewrite the system of equations in the matrix form $M\mathbf{v} = \mathbf{0}$ where

$$M = \begin{pmatrix} ky+z & 0 & 0 \\ -rkx & -z & rkz \\ -rx & ry & -ky \end{pmatrix} \text{ and } \mathbf{v} = \begin{pmatrix} x^{m-1} \\ y^{m-1} \\ z^{m-1} \end{pmatrix}.$$

Since $\mathbf{v} \neq \mathbf{0}$ by assumption, it follows that $\det(M) = 0$:

$$(r^2-1)k(ky+z)yz = 0.$$

Also note that $F_x = 0$ implies that $(ky+z)x^{m-1} = 0$.

Case 1: $x \neq 0$. Then we must have $ky + z = 0$. Since $F = 0$, we have

$$0 = zy^m + kyz^m = z(y^m - z^m).$$

If $z = 0$, then $y = 0$ and thus $F_y = -rkx^m \neq 0$ since $p \nmid r$, a contradiction. Thus, $z \neq 0$ and $y \neq 0$, and we must have

$$y^m = z^m = (-ky)^m = (-k)^m y^m,$$

which implies that $-k$ is an r-th power, violating our assumption.

Case 2: $x = 0$. Since $F_y = F_z = 0$, we have

$$rkz^m = zy^{m-1}, ry^m = kyz^{m-1}.$$

Thus, $y \neq 0, z \neq 0$. It follows that $ky + z = 0$ since $\det(M) = 0$. We can now argue in the same way as we did in **Case 1** to deduce that $-k$ is an r-th power, which is a contradiction.

We conclude that C is a smooth curve. □

We discuss the sharpness of the assumption $q > r^4$ in the statement of Theorem 6.3 for small values of r below.

Remark 6.4. When $r = 2$, the hypothesis requires $q > 16$. However, one can show that $q \geq 7$ is already sufficient by analyzing the cases $q \in \{7, 11, 13\}$ in a computer. On other hand, the conclusion fails when $q = 5$, because the degree is $d = \frac{q-1}{r} + 1 = 3$, and an irreducible cubic curve over $\mathbb{F}_5$ cannot be blocking by Theorem 1.3.

When $r = 3$, the hypothesis requires $q > 3^4 = 81$. It turns out that the conclusion fails when $q = 13$. However, we checked with a computer that the conclusion of the theorem holds for all $19 \leq q \leq 81$.

When $r = 4$, the hypothesis requires $q > 4^4 = 256$. One can check that the conclusion of Theorem 6.3 does not hold when $q = 29$. On the other hand, the conclusion holds for $q = 37$. We believe that the conclusion holds for all $q \geq 37$.

When $r = 5$, the hypothesis requires $q > 5^4 = 625$. One can check using a computer that the conclusion of Theorem 6.3 does not hold when $q = 101$. On the other hand, the conclusion of Theorem 6.3 holds for $q = 131$. We believe that the conclusion holds for all $q \geq 131$.

In general, we believe the bound $q > r^4$ is not optimal. However, to the best knowledge of the authors, relaxing the inequality $q > r^4$ in Corollary 2.2 is out of reach.

We end the section by presenting the proof of Theorem 1.6 and Theorem 1.7.

Proof of Theorem 1.6. Applying Corollary 2.7 with $\theta = 1/4$ and $A = 1/2$, we can find infinitely many primes p such that $p - 1$ has a divisor r such that $\frac{1}{4}p^{1/4} \leq r < p^{1/4}$. Note that for each such a pair (p, r), we have $p > r^4$, $p \equiv 1 \pmod{r}$, and $(p-1)/r \leq 4p^{3/4}$. For each such a pair (p, r),

Theorem 6.2 implies that there is a geometrically irreducible nontrivially blocking curve over $\mathbb{F}_p$ with degree d for each choice of $d \geq \frac{p-1}{r} + 1$. Since $(p-1)/r \leq 4p^{3/4}$, we obtain desired curves in every degree starting with $4p^{3/4} + 1$. □

Proof of Theorem 1.7. The proof is similar to the proof of Theorem 1.6. It follows from Corollary 2.7 and Theorem 6.3. When $\theta = 1/4$, the requirement $A \leq 1/2$ is imposed by the bound $q > r^4$ which appears as a hypothesis in Theorem 6.3. □

7. Smooth blocking curves with degree $(q+3)/2$ and $(q-1)/2$

7.1. **Proof of Theorem 1.8.** When $q \equiv 3 \pmod 4$, we have already proved the existence of such a curve in Theorem 5.1. So, we can assume $q \equiv 1 \pmod 4$ and $p > 3$ for the rest of the proof.

Let $m = (q-1)/2$. We consider the plane curve C defined by

$$F(x, y, z) = xy(x^m + y^m) + (xz + yz)(x^m + z^m) = 0.$$

We claim that C is smooth and nontrivially blocking.

When $q = 5, 13$, one can check C is smooth and nontrivially blocking using a computer. Next, we assume $q \geq 17$ so that Corollary 2.2 can be applied with $r = 2$. Note that we can write

$$F(x, y, z) = (xy + xz + yz)x^m + xy \cdot y^m + (xz + yz)z^m,$$

so C contains the points in

$$\{[0:0:1], [0:1:0], [1:0:0]\} \cup \{[1:y:z] |\ y \text{ and } z \text{ are non-squares in } \mathbb{F}_q^*\}.$$

We can argue as in Proposition 6.1 and Corollary 2.11 that C is nontrivially blocking. Thus, it suffices to show that C is smooth.

Suppose $P = [x : y : z]$ is a singular point of C. The conditions $F_x(P) = 0$, $F_y(P) = 0$ and $F_z(P) = 0$ become, after multiplying both sides by 2,

$$\begin{aligned} x^m y + 2y^{m+1} + x^m z + 2z^{m+1} - x^{m-1}yz &= 0, \\ 2x^{m+1} + xy^m + 2x^m z + 2z^{m+1} &= 0, \\ 2x^{m+1} + xz^m + 2x^m y + yz^m &= 0. \end{aligned}$$

We can rewrite the system of equations in the matrix form $M\mathbf{v} = \mathbf{0}$ where

$$M = \begin{pmatrix} xy + xz - yz & 2y^2 & 2z^2 \\ 2x^2 + 2xz & xy & 2z^2 \\ 2x^2 + 2xy & 0 & xz + yz \end{pmatrix} \text{ and } \mathbf{v} = \begin{pmatrix} x^{m-1} \\ y^{m-1} \\ z^{m-1} \end{pmatrix}.$$

Since $\mathbf{v} \neq \mathbf{0}$ by assumption, it follows that $\det(M) = 0$. After expanding the determinant and factoring, we obtain:

$$\det(M) = (-3) \cdot xyz \cdot (x + y) \cdot (xy + xz - yz) = 0.$$

Since $\mathrm{char}(\mathbb{F}_q) > 3$ by hypothesis, we may ignore the (-3) factor. We will proceed according to which factor above vanishes.

Case 1. $xyz = 0$.

We have three subcases to consider.

Case 1.1. $z = 0$.

In this case, $xy(x^m + y^m) = 0$ using the defining equation of the curve. If $x = 0$, then $y \neq 0$ but then $F_x \neq 0$, a contradiction. If $y = 0$, then $x \neq 0$ but then $F_z \neq 0$, a contradiction.

Thus, $xy \neq 0$ which means $x^m + y^m = 0$. Now, $F_x = 0$ gives $x^m y + 2y^{m+1} = 0$. We obtain $0 = y(-y^m) + 2y^{m+1} = y^{m+1}$, which forces $y = 0$, a contradiction.

Case 1.2. $y = 0$.

In this case, $xz(x^m + z^m) = 0$ using the defining equation of the curve. If $z = 0$, then we have handled this in Case 1.1. So, we may assume that $z \neq 0$. If $x = 0$, then $F_y \neq 0$, a contradiction. We must have $xz \neq 0$, which means $x^m + z^m = 0$. From $F_x = 0$, we get $x^m z + 2z^{m+1} = 0$. Thus, $0 = x^m z + 2z^{m+1} = z(-z^m) + 2z^{m+1} = z^{m+1}$. But then $z = 0$, which has already been handled in Case 1.1.

Case 1.3. $x = 0$.

If $x = 0$, then $F_z = 0$ implies that $yz^m = 0$, and so $z = 0$ or $y = 0$. We have handled these in Case 1.1 and Case 1.2, respectively.

Case 2. $xyz \neq 0$ and $x + y = 0$.

In this case, $y = -x$ and the defining equation for the curve becomes $-x^2(x^m + (-x)^m) = 0$. Since $m = (q-1)/2$ is even by hypothesis, we get $-x^2 \cdot (2x^m) = 0$, and so $x = 0$, a contradiction.

Case 3. $xyz \neq 0$, $x + y \neq 0$, and $xy + xz - yz = 0$.

Looking at the first row of the matrix equation $M\mathbf{v} = 0$, we obtain $2y^{m+1} + 2z^{m+1} = 0$, that is, $y^{m+1} + z^{m+1} = 0$. Let us write $F = 0$ more explicitly:

$$x^{m+1}y + xy^{m+1} + x^{m+1}z + xz^{m+1} + yzx^m + yz^{m+1} = 0$$

and rearrange to get:

$$\underbrace{x^{m+1}(y+z) + yzx^m}_{=x^m(xy+xz+yz)=x^m(2yz)} + x\underbrace{(y^{m+1} + z^{m+1})}_{=0} + yz^{m+1} = 0.$$

We deduce that:

$$2x^m yz + yz^{m+1} = 0 \;\; \Rightarrow \;\; 2x^m + z^m = 0.$$

We will now combine the three relations $xy + xz = yz$, $y^{m+1} + z^{m+1} = 0$, and $2x^m + z^m = 0$. Since we are working in projective coordinates and $xyz \neq 0$, without loss of generality, we can set $z = 1$. These three relations become:

$$\begin{aligned} xy &= y - x, \\ y^{m+1} &= -1, \\ 2x^m &= -1. \end{aligned}$$

Since $y^{m+1} = -1$, we square both sides to get $y^{2m+2} = 1$. But $2m + 1 = q$ by hypothesis, and so $y^{q+1} = 1$. In particular, $y^{q^2-1} = 1$ which means y belongs to $\mathbb{F}_{q^2}$. Since x and y are related by $xy = y - x$, this means x is in $\mathbb{F}_{q^2}$ as well, and so $x^{q^2-1} = 1$ too.

On the other hand, since $2x^m = -1$, that is, $2x^{(q-1)/2} = -1$, this would imply after squaring both sides: $4x^{q-1} = 1$, and so $4^{q+1}x^{q^2-1} = 1$. Since $x^{q^2-1} = 1$, this last equation means $4^{q+1} = 1$. From here, we can use $4^q = 4$ to get $4^2 = 1$ in $\mathbb{F}_q$, that is, $15 = 0$ holds in $\mathbb{F}_q$. Since the characteristic p is bigger than 3, we conclude $p = 5$.

In this case, $4x^{q-1} = 1$ implies $x^{q-1} = -1$. Now, $xy = y - x$ implies $x^q y^q = y^q - x^q$. Using $x^{q-1} = -1$ and $y^{q+1} = 1$, this last equation can be written as $-x/y = (1/y) + x$ or equivalently, $-x = 1 + xy$. But we know $xy = y - x$, and so $-x = 1 + y - x$ which forces $y = -1$. Substituting this back again into $xy = y - x$, we get $-x = -1 - x$, which is a contradiction. We deduce that C is smooth.

Remark 7.1. When $q \equiv 3 \pmod 4$, and $p > 3$, one can use a similar argument to show that curve C defined by

$$F(x, y, z) = -(xy + xz + yz)x^m + xy \cdot y^m + (xz + yz)z^m = 0$$

is smooth and nontrivially blocking, where $m = (q - 1)/2$.

7.2. **Proof of Theorem 1.9.** Let $q \equiv 3 \pmod 4$ such that $p > 3$ and $q \equiv 3 \pmod 4$. Let $m = (q - 1)/2$. Consider the plane curve C defined by

$$(x + y + z)^m + x^m + y^m + z^m = 0.$$

We show that C is smooth and nontrivially blocking in a series of two claims. Note that the proof of Claim 7.2 works for all prime powers $q = p^r$ with $p > 3$.

Claim 7.2. *C is smooth.*

Proof. Assume, to the contrary, that $P = [x : y : z]$ is a singular point of C. Let $F = (x+y+z)^m + x^m + y^m + z^m$ be the defining polynomial of C. The conditions $F_x(P) = F_y(P) = F_z(P) = 0$ translate to:

$$m(x + y + z)^{m-1} + mx^{m-1} = 0,$$
$$m(x + y + z)^{m-1} + my^{m-1} = 0,$$
$$m(x + y + z)^{m-1} + mz^{m-1} = 0.$$

Thus, $x^{m-1} = y^{m-1} = z^{m-1} = -(x + y + z)^{m-1}$. If $xyz = 0$, then it is clear that $x = y = z = 0$ which would be a contradiction. So, we may assume that $xyz \neq 0$. The relations tell us that there are $\alpha, \beta \in \overline{\mathbb{F}_q}$ such that $x = \alpha z$ and $y = \beta z$, where $\alpha^{m-1} = \beta^{m-1} = 1$. Since $m - 1 = \frac{q-3}{2}$, we get $\alpha^{q-3} = 1$. And so $\alpha^q = \alpha^3$. Similarly, $\beta^q = \beta^3$. Using $z^{m-1} = -(x + y + z)^{m-1}$, we obtain

$$(1 + \alpha + \beta)^{m-1} = -1 \quad \Rightarrow \quad (1 + \alpha + \beta)^{q-3} = 1.$$

Therefore,

$$1 + \alpha^q + \beta^q = (1 + \alpha + \beta)^q = (1 + \alpha + \beta)^3.$$

Consequently,

$$1 + \alpha^q + \beta^q = 1 + \alpha^3 + \beta^3 + 3(\alpha\beta + 1)(\alpha + \beta) + 3(\alpha + \beta)^2. \tag{17}$$

Using $\alpha^q = \alpha^3$ and $\beta^q = \beta^3$, the equation (17) simplifies to:

$$3(\alpha + \beta)(\alpha + 1)(\beta + 1) = 0.$$

If $\alpha = -1$, then $x = -z$, but then $y^{m-1} = -(x + y + z)^{m-1}$ implies that $y^{m-1} = -y^{m-1}$, contradicting $xyz \neq 0$. If $\beta = -1$, then a similar calculation reaches $x^{m-1} = -x^{m-1}$, a contradiction. If $\alpha + \beta = 0$, then $\alpha = -\beta$, which means $y = -x$, and the same reasoning as above shows $z^{m-1} = -z^{m-1}$, which again gives a contradiction. Therefore, C is a smooth curve. □

Claim 7.3. *C is nontrivially blocking.*

Proof. By Corollary 2.11, it suffices to show that C is blocking. When $q = 7$, the degree is $d = \frac{q-1}{2} = 3$, and the conclusion fails because an irreducible cubic curve over $\mathbb{F}_7$ cannot be blocking by Theorem 1.3. When $11 \leq q < 47$, it is easy to verify the statement using a computer. Next, we assume that $q \geq 47$ so that we can apply Corollary 2.3.

Let L be an $\mathbb{F}_q$-line $ax + by + cz = 0$ in $\mathbb{P}^2$. We consider several cases depending on the values of a, b, c. The convention for numbering different cases follows a tree structure.

Case 0. $abc = 0$. Since the equation of the curve is symmetric in x, y, z, we may assume $c = 0$. We have two subcases to consider.

Case 00. $b = 0$. In this case, L is given by $\{x = 0\}$, and $C \cap L$ contains the point $[0 : 1 : -1]$. We have used $(-1)^m = -1$ which holds due to $q \equiv 3 \pmod 4$.

Case 01. $a = 0$. In this case, L is given by $\{y = 0\}$, and $C \cap L$ contains the point $[1 : 0 : -1]$.

Case 02. $ab \neq 0$. We can assume $b = 1$ for the rest of this case.

Case 020. $a = 1$. In this case, L is given by $x + y = 0$, and $L \cap C$ contains $[1 : -1 : 0]$.

Case 021. $a \neq 1$. The equation for L is $y = -ax$. Substituting this into the equation of C, we get:

$$x^m - a^m x^m + z^m + ((1-a)x + z)^m = 0.$$

We will look for a solution with $z = 1$, in which case the equation above becomes:

$$x^m - a^m x^m + 1 + ((1-a)x + 1)^m = 0. \tag{18}$$

Case 0210. $a^m = 1$. In this case, (18) becomes $((1-a)x+1)^m = -1$. We can always find $x_0 \in \mathbb{F}_q^*$ such that $(1-a)x_0+1$ is a non-square since $a \neq 1$. Such a point satisfies $((1-a)x_0+1)^m = -1$, and therefore $[x_0 : -ax_0 : 1] \in L \cap C$.

Case 0211. $a^m = -1$. In this case, (18) becomes $2x^m + 1 + ((1-a)x + 1)^m = 0$. By Corollary 2.3, we can find a non-square $x_0 \in \mathbb{F}_q$ such that $(1-a)x_0 + 1$ is a nonzero square. Such a point satisfies $x_0^m = -1$ and $((1-a)x_0 + 1)^m = 1$. Therefore, $[x_0 : -ax_0 : 1] \in L \cap C$.

This concludes the analysis of the case $abc = 0$. We move on to the next main case.

Case 1. $abc \neq 0$.

We work under the assumption now that $c = 1$. Again, there are several cases to consider.

Case 10. $a = b = 1$. In this case, $C \cap L$ contains the point $[1 : -1 : 0]$.

Again, using the symmetry of the curve, we will proceed according to the following case.

Case 11. $b \neq 1$. There are two further sub-cases to consider:

Case 110. $a = 1$. The equation of L is $z = -(x + by)$. The intersection between L and C is thus governed by the following relation:

$$x^m + y^m - (x + by)^m + ((1-b)y)^m = 0. \tag{19}$$

Case 1100. $1 - b$ is a (nonzero) square. In this case, (19) leads to:

$$x^m + 2y^m - (x + by)^m = 0.$$

By setting $y = 1$, it suffices to find $x_0 \in \mathbb{F}_q$ such that x_0 is a non-square and $x_0 + b$ is a nonzero square. Such x_0 exists by Corollary 2.3.

Case 1101. $1 - b$ is a non-square. In this case, (19) leads to:

$$x^m = (x + by)^m.$$

By setting $y = 1$, it suffices to find an $x_0 \in \mathbb{F}_q$ such that x_0 and $x_0 + b$ are both nonzero squares. Such x_0 exists by Corollary 2.3.

Case 111. $a \neq 1$ (note that we already know that $b \neq 1$). The equation of the line L is $z = -ax - by$. Substituting this into the equation of C, the points in $L \cap C$ are determined by:

$$x^m + y^m - (ax + by)^m + ((1-a)x + (1-b)y)^m = 0.$$

We look for solutions to the above equation when $x, y \in \mathbb{F}_q$. Setting $y = 1$, it suffices to analyze:

$$x^m - (ax + b)^m + ((1-a)x + 1 - b)^m = -1. \tag{20}$$

We proceed according to two subcases, depending on whether a is equal to b.

Case 1110. $a = b$. In this case, the equation (20) is satisfied when $x = -1$ because $q \equiv 3 \pmod 4$. Thus, $L \cap C$ certainly contains $\mathbb{F}_q$-points in this case.

Case 1111. $a \neq b$. In this case, in order to satisfy (20), it suffices to find $x_0 \in \mathbb{F}_q$ such that x_0 is a non-square, but $ax_0 + b$ and $(1-a)x_0 + 1 - b$ are both nonzero squares. After dividing both sides by a and $1-a$, we need to ensure that x_0 is a non-square, $x_0 + \frac{b}{a}$ and $x_0 + \frac{1-b}{1-a}$ have prescribed form (squares or non-squares depending on a and $1-a$). Such an x_0 exists by Corollary 2.3 since $a \neq b$ implies that $\frac{b}{a} \neq \frac{1-b}{1-a}$.

This concludes the proof that $C(\mathbb{F}_q)$ is a blocking set. □

Note that the condition $q \equiv 3 \pmod 4$ was used in the proof of the previous theorem. Indeed, the given curve will not be blocking when $q \equiv 1 \pmod 4$ and $p > 3$, because the line $x+y+z = 0$ is not blocked. We finish the paper by illustrating different examples for the case $q \equiv 1 \pmod 4$.

Example 7.4. Consider the following plane curves of degree $d = \frac{q-1}{2}$,

- $x^d + y^d + z^d + (x+y+z)^d + (x-3y+9z)^d + (x+2y+4z)^d = 0$ over $\mathbb{F}_q$ for $q \in \{13, 17, 29, 37, 53\}$,
- $x^d + y^d + z^d + (x+y+z)^d + (x-5y+25z)^d + (x+2y+4z)^d = 0$ over $\mathbb{F}_q$ for $q \in \{41, 61\}$.

Each of these plane curves is smooth and blocking over $\mathbb{F}_q$.

We do not know how to generalize Example 7.4 for every $q \equiv 1 \pmod 4$. Interestingly, the curve defined by

$$x^d + y^d + z^d + (x+y+z)^d + (x-3y+9z)^d + (x+2y+4z)^d = 0$$

is not a blocking curve over $\mathbb{F}_q$ for $q \in \{41, 61\}$. Moreover, it is not smooth for $q = 61$. It is reasonable to conjecture that for $q \equiv 1 \pmod 4$, there exists a smooth blocking curve of the form,

$$x^{\frac{q-1}{2}} + y^{\frac{q-1}{2}} + z^{\frac{q-1}{2}} + (x+y+z)^{\frac{q-1}{2}} + (x-ay+a^2z)^{\frac{q-1}{2}} + (x+by+b^2z)^{\frac{q-1}{2}} = 0$$

for suitable choices of $a, b \in \mathbb{F}_q$.

ACKNOWLEDGEMENTS

The authors thank Greg Martin and József Solymosi for helpful discussions. During the preparation of this manuscript, the first author was supported by a postdoctoral research fellowship from the University of British Columbia and the NSERC PDF award. 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

[ABGP14] N. Anbar, D. Bartoli, M. Giulietti, and I. Platoni, *Small complete caps from singular cubics*, J. Combin. Des. **22** (2014), no. 10, 409–424.

[ABPG15] N. Anbar, D. Bartoli, I. Platoni, and M. Giulietti, *Small complete caps from singular cubics, II*, J. Algebraic Combin. **41** (2015), no. 1, 185–216.

[ADL22] S. Asgarli, L. Duan, and K.-W. Lai, *Frobenius nonclassical hypersurfaces*, arXiv e-prints (2022), available at https://arxiv.org/abs/2207.11981.

[AG22] S. Asgarli and D. Ghioca, *Smoothness in pencils of hypersurfaces over finite fields*, Bull. Aust. Math. Soc (2022). https://doi.org/10.1017/S0004972722000776.

[AGW11] A. Akbary, D. Ghioca, and Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17** (2011), no. 1, 51–67.

[AGY22] S. Asgarli, D. Ghioca, and C. H. Yip, *Most plane curves over finite fields are not blocking* (2022). In preparation.

[AP96] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, Arithmetic, geometry and coding theory (Luminy, 1993), 1996, pp. 1–7.

[BH17] H. Borges and M. Homma, *Points on singular Frobenius nonclassical curves*, Bull. Braz. Math. Soc. (N.S.) **48** (2017), no. 1, 93–101.

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

[BM22] D. Bartoli and G. Micheli, *Algebraic constructions of complete m-arcs* (2022). Combinatorica, in press.

[BMP17] D. Bartoli, S. Marcugini, and F. Pambianco, *On the completeness of plane cubic curves over finite fields*, Des. Codes Cryptogr. **83** (2017), no. 2, 233–267.

[BMT14] H. Borges, B. Motta, and F. Torres, *Complete arcs arising from a generalization of the Hermitian curve*, Acta Arith. **164** (2014), no. 2, 101–118.

[Bom65] E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.

[Bor09] H. Borges, *On complete (N,d)-arcs derived from plane curves*, Finite Fields Appl. **15** (2009), no. 1, 82–96.

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

[Gác03] A. Gács, *On a generalization of Rédei's theorem*, Combinatorica **23** (2003), no. 4, 585–598.

[Gao01] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, J. Algebra **237** (2001), no. 2, 501–520.

[Giu02] M. Giulietti, *On plane arcs contained in cubic curves*, Finite Fields Appl. **8** (2002), no. 1, 69–90.

[GPTU02] M. Giulietti, F. Pambianco, F. Torres, and E. Ughi, *On complete arcs arising from plane curves*, Des. Codes Cryptogr. **25** (2002), no. 3, 237–246.

[HV88] J. W. P. Hirschfeld and J. F. Voloch, *The characterization of elliptic curves over finite fields*, J. Austral. Math. Soc. Ser. A **45** (1988), no. 2, 275–286.

[HV90] A. Hefez and J. F. Voloch, *Frobenius nonclassical curves*, Arch. Math. (Basel) **54** (1990), no. 3, 263–273.

[Lin44a] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 139–178.

[Lin44b] ———, *On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon*, Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 347–368.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, Second, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[LP20] S. Li and A. Pott, *Intersection distribution, non-hitting index and Kakeya sets in affine planes*, Finite Fields Appl. **66** (2020), 101691, 38.

[MV73] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

[Par86] R. Pardini, *Some remarks on plane curves over fields of finite characteristic*, Compositio Math. **60** (1986), no. 1, 3–17.

[Seg67] B. Segre, *Introduction to Galois geometries*, Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. Ia (8) **8** (1967), 133–236.

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

[SV86] K. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19.

[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.

[Xyl11] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, Bonner Mathematische Schriften [Bonn Mathematical Publications], vol. 404, Universität Bonn, Mathematisches Institut, Bonn, 2011. Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

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