WHEN IS THE ASGARLI–GHIOCA–YIP CURVE BLOCKING? A SHARPNESS BELIEF THAT FAILS AT $q = 41$, AND THE EXACT RANGES FOR $r \leq 5$

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $r \geq 2$, let $q \equiv 1 \pmod r$ be a prime power with $p \nmid (r^2 - 1)$, put $m = (q-1)/r$, and let $k \in \mathbb{F}_q^*$ be such that $-k$ is not an r-th power. Asgarli, Ghioca and Yip proved that the plane curve $-(ky+z)x^m + zy^m + kyz^m = 0$ is smooth and nontrivially blocking as soon as $q > r^4$, and remarked on the sharpness of that hypothesis: for $r = 4$ they wrote that they believe the conclusion holds for all $q \geq 37$, and for $r = 5$ that they believe it holds for all $q \geq 131$. We show that the first belief is false and the second is true. At $q = 41$ — a prime with $41 \geq 37$, $41 \equiv 1 \pmod 4$ and $41 \nmid 15$ — the line $x + y + z = 0$ carries none of the 104 points of the curve with $k = 2$, and in fact the curve is blocking for no admissible k; $q = 41$ is the only prime power of the range $37 \leq q \leq 256$ admitted by the remaining hypotheses where this happens, so the sharp threshold at $r = 4$ is $q \geq 49$ and not $q \geq 37$. At $r = 5$ the conclusion does hold at every admitted prime power of the declared range $131 \leq q \leq 625$, and indeed already from $q \geq 121$. The mechanism is classical: the hypothesis $q > r^4$ enters the proof only through a corollary asserting that -1 is a sum $by + cz$ of prescribed power residues, and the failure of that corollary is the vanishing of a cyclotomic number; for $r = 4$ the classical formula $16(0,0)_4 = p - 11 - 6a$ leaves exactly $p = 17$ and $p = 41$. We determine the exact set of prime powers where the corollary fails for every $r \leq 5$. Every theorem and proposition below is machine-checked in Lean 4, with the scope limitation recorded in Remark 3.2; the computations outside that development are labelled where they appear.

1. Introduction

Let $q = p^n$ be a prime power. A set $B \subseteq \mathbb{P}^2(\mathbb{F}_q)$ is a *blocking set* if every $\mathbb{F}_q$-line meets it, and a blocking set is *nontrivial* if it does not contain all $q+1$ $\mathbb{F}_q$-points of any $\mathbb{F}_q$-line. A plane curve $C = \{F = 0\}$ is a *blocking curve* if $C(\mathbb{F}_q)$ is a blocking set, and *nontrivially blocking* if $C(\mathbb{F}_q)$ is a nontrivial blocking set. Which curves — and, above all, curves of which degree — can be blocking is a question with a long history on the combinatorial side, where Blokhuis' bound $|B| \geq \frac{3}{2}(p+1)$ for nontrivial blocking sets in $\mathbb{P}^2(\mathbb{F}_p)$ [3] is the benchmark; on the algebraic side it was taken up systematically by Asgarli, Ghioca and Yip [1].

The source and its construction. Section 6 of [1] constructs blocking curves out of power residues. We quote its central statement verbatim, in its own notation and under its own numbering.

> **Theorem 6.3** ([1, Thm. 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.*

The curve has degree $m+1 = \frac{q-1}{r} + 1$, which for fixed r is far below the degrees reachable by earlier constructions; that is the point of the theorem. The hypothesis $q > r^4$, however, is an artefact of the analytic input, and [1] says so. The remark that follows the theorem is the subject of this paper; we quote its third and fourth paragraphs and its closing sentence verbatim.

> **Remark 6.4** ([1, Rmk. 6.4]). *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*

Date: 3 September 2026.

> *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.*

For $r = 2$ and $r = 3$ the same remark reports computer checks that already reach r^4, so those two cases are closed and no belief is needed. For $r = 4$ and $r = 5$ the checks stop short, at $q = 37$ and $q = 131$ respectively, and each of those two paragraphs ends instead with a sentence beginning "We believe". They have stood unexamined: none of the six works citing [1] that we could find, the most recent of them [2] by the same three authors, returns to Remark 6.4.

What is settled here. The two beliefs have opposite truth values.

- **The $r = 4$ belief is false**, at exactly one prime power. At $q = 41$ — a prime, $41 \geq 37$, $41 \equiv 1 \pmod 4$ and $41 \nmid 15 = 4^2 - 1$, so that every hypothesis of Theorem 6.3 except $q > 256$ is met — the curve of Theorem 6.3 is not blocking, for any admissible k (Theorems 4.3 and 4.5, Corollary 4.4). For $k = 2$ the witness is a single line, $x + y + z = 0$.
- **At $r = 4$, $q = 41$ is the only counterexample**: at all nineteen other primes of the range $37 \leq q \leq 256$ the curve is blocking for every k (Theorem 5.1), and so it is at the three prime powers of that range, by a computation outside the formal development. Above 256 the conclusion is Theorem 6.3 itself, so nothing is left over: the sharp threshold at $r = 4$ is $q \geq 49$, and $q = 41$ is the single prime power that separates it from the 37 of the belief.
- **The $r = 5$ belief is true**, over the whole range it asserts and Theorem 6.3 does not already prove (Theorem 5.4), and it is slightly conservative: the sharp threshold there is $q \geq 121$.

We stress what kind of statement is being corrected. Remark 6.4 is a remark about the sharpness of a hypothesis, not a theorem and not a conjecture that any result of [1] rests on: Theorem 6.3 is applied elsewhere in [1] only with $q > r^4$, so every proved statement of that paper stands exactly as written. What changes is the threshold in one sentence of one remark. All of our claims about [1] refer to arXiv:2208.13299v2, which is also the published version; the two arXiv versions have byte-identical Section 6 sources, and Theorem 6.3, Remark 6.4 and Corollary 2.2 read word for word the same, under the same numbering, in the published paper.

The engine behind all of this is an observation about the source's own proofs, recorded as ($\star$) in §3: the hypothesis $q > r^4$ enters the proof of Theorem 6.3 only through Corollary 2.2 of [1], a statement about q^2 pairs rather than about the $q^2 + q + 1$ lines of a curve of degree $\frac{q-1}{r} + 1$. Replacing the hypothesis by what it is used for turns the entire declared gap into a finite, and small, computation. It also answers the closing sentence quoted above for small r: for a *fixed* $r \leq 5$, relaxing $q > r^4$ in Corollary 2.2 is not out of reach at all, and we give the exact answer in §6. It is the uniformity in r that stays out of reach.

Organisation. Section 2 fixes notation and states the finite condition $P(q, r)$ that Corollary 2.2 of [1] amounts to. Section 3 contains the two reduction steps. Section 4 is the counterexample and its classical explanation. Section 5 is the positive half at $r = 4$ and $r = 5$. Section 6 records the exact failure set of Corollary 2.2 for $r \leq 5$ and two by-products. Section 7 describes the formal verification.

2. Preliminaries

Throughout, p is a prime and $q = p^n$. We write $\mathbb{P}^2(\mathbb{F}_q)$ for the projective plane over $\mathbb{F}_q$, whose points are the classes $[x : y : z]$ of nonzero triples modulo scaling, and whose $\mathbb{F}_q$-lines are the sets $L_{a,b,c} = \{[x : y : z] : ax + by + cz = 0\}$ with $(a, b, c) \neq (0, 0, 0)$. A line *misses* a curve C when it carries

no $\mathbb{F}_q$-point of C; thus C is blocking exactly when no $\mathbb{F}_q$-line misses it. Following [1, §2.1], a plane curve $C = \{F = 0\}$ is *smooth* if at every point of C at least one of F_x, F_y, F_z is nonzero.

Definition 2.1. Let $r \geq 2$, let $q \equiv 1 \pmod r$ be a prime power, put $m = (q-1)/r$, and let $k \in \mathbb{F}_q$. Write $C_{q,r,k}$ for the plane curve

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

the curve of Theorem 6.3 of [1], of degree $m + 1$. Call k *admissible* for (q, r) when $k \neq 0$ and $-k$ is not an r-th power in $\mathbb{F}_q^*$ — equivalently, when $k \neq 0$ and $(-k)^m \neq 1$. These are the k for which Theorem 6.3 speaks.

The r-th powers of $\mathbb{F}_q^*$ form the subgroup $\mu_m = \{y \in \mathbb{F}_q^* : y^m = 1\}$ of order m, and $\mathbb{F}_q^*/\mu_m$ has order r.

Definition 2.2. Let $q \equiv 1 \pmod r$ be a prime power and $m = (q-1)/r$. Say that (q, r) has the *power-pair property*, written $P(q, r)$, if

$$\text{for all } b, c \in \mathbb{F}_q^* \text{ there are } y, z \in \mu_m \text{ with } by + cz = -1.$$

Lemma 2.3. *$P(q, r)$ is equivalent to the conclusion of Corollary 2.2 of* [1]*, namely: for every multiplicative character χ of $\mathbb{F}_q$ of order r, all r-th roots of unity ω_1, ω_2 and all $b, c \in \mathbb{F}_q^*$ there are $y, z \in \mathbb{F}_q$ with $\chi(y) = \omega_1$, $\chi(z) = \omega_2$ and $by + cz = -1$.*

Proof. Assume $P(q, r)$ and fix $\chi, \omega_1, \omega_2, b, c$. Since χ is onto the group of r-th roots of unity, choose $y_0, z_0 \in \mathbb{F}_q^*$ with $\chi(y_0) = \omega_1$ and $\chi(z_0) = \omega_2$. Apply $P(q, r)$ to the pair (by_0, cz_0): it yields $y, z \in \mu_m$, that is r-th powers, with $b(y_0 y) + c(z_0 z) = -1$; and $\chi(y_0 y) = \omega_1$, $\chi(z_0 z) = \omega_2$ because χ kills r-th powers. Conversely, take $\omega_1 = \omega_2 = 1$: as $\chi(0) = 0$, the elements produced are nonzero with $\chi(y) = \chi(z) = 1$, hence lie in μ_m. □

Lemma 2.3 is the bridge between the source's formulation and the finite condition we work with; it is the only statement of this paper that is not part of the formal development, characters into $\mathbb{C}$ having no place there. Everything after this point is phrased in terms of $P(q, r)$.

3. The reduction

Where $q > r^4$ is used. Reading the proofs of [1, §6]: the hypothesis $q > r^4$ is used in the proof of Proposition 6.1 (blocking) in exactly one line, "This is guaranteed by Corollary 2.2", and in the proof of Theorem 6.2 (geometric irreducibility and nontriviality) in exactly one line, "We can apply Corollary 2.2 to find some r-th power y and some non-r-th power z which satisfies this relation". The smoothness argument of Theorem 6.3 uses only $p \nmid (r^2 - 1)$, $p \nmid r$ (automatic from $q \equiv 1 \pmod r$) and the admissibility of k; it does not use $q > r^4$ at all. Hence, with Lemma 2.3,

$$(\star) \qquad \begin{array}{l} P(q, r) \text{ together with the remaining hypotheses of Theorem 6.3} \\ \qquad \Longrightarrow \text{ the conclusion of Theorem 6.3, for every admissible } k. \end{array}$$

This is the source's own argument with one hypothesis swapped for the statement it is used to reach. The blocking half of $(\star)$ is the following proposition, which is [1, Prop. 6.1] specialised to the polynomials of Theorem 6.3, and which we have verified formally.

Proposition 3.1. *Let q be a prime power and let $m \geq 0$ be an integer — no relation between m and q is assumed. Suppose that for all $b, c \in \mathbb{F}_q^*$ there are $y, z \in \mathbb{F}_q$ with $y^m = z^m = 1$ and $by + cz = -1$. Then for* every *$k \in \mathbb{F}_q$ — admissible or not — the curve $-(ky + z)x^m + zy^m + kyz^m = 0$ is blocking. In particular, if $q \equiv 1 \pmod r$ and $P(q, r)$ holds, then $C_{q,r,k}$ is blocking for every $k \in \mathbb{F}_q$.*

Proof. The three coordinate points lie on the curve, since $F_k(1, 0, 0) = F_k(0, 1, 0) = F_k(0, 0, 1) = 0$ identically in q, m, k; and $F_k(1, y, z) = -(ky + z) + z + ky = 0$ whenever $y^m = z^m = 1$. So the set $B = \{[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]\} \cup \{[1 : y : z] : y^m = z^m = 1\}$ lies on the curve, and it suffices to block every line with B. A line $ax + by + cz = 0$ with $abc = 0$ contains one of the three coordinate

points. If $abc \neq 0$, normalise $a = 1$ and apply the hypothesis to (b, c): the resulting point $[1 : y : z]$ lies on the line and in B. □

Remark 3.2. Proposition 3.1, and every later statement, is formalised over $\mathbb{F}_q$ for *prime* q, where $\mathbb{F}_q$ is the residue ring $\mathbb{Z}/q\mathbb{Z}$; the prime powers in range are handled by the enumeration described in §7 and are labelled as such wherever they are used. Furthermore, the formal development certifies the *blocking* half of the conclusion of Theorem 6.3 and not the conjunction "smooth and nontrivially blocking". For the refutations of §4 this costs nothing: a nontrivially blocking curve is in particular blocking, so refuting blocking refutes the conjunction a fortiori. For the positive results of §5 the two remaining halves are supplied by $(\star)$, that is by the source's own proofs, which is a step we have not formalised; the enumeration found no non-smooth $\mathbb{F}_q$-point and no trivially blocking curve anywhere in its sweep.

The coset reduction. Deciding $P(q, r)$ as it stands means scanning the $(q-1)^2$ pairs (b, c) and, for each, a subset of $\mu_m \times \mu_m$. The condition, however, only depends on the classes of b and c modulo r-th powers: replacing (b, c) by (bu, cu') with $u, u' \in \mu_m$ and y, z by yu^{-1}, zu'^{-1} leaves it unchanged. So r^2 representative pairs suffice, provided one also certifies that the chosen representatives really do meet every coset.

Lemma 3.3. *Let q be prime, $m \geq 1$, and let $w_1, \dots, w_s \in \mathbb{F}_q$. Suppose*

(i) *every $b \in \mathbb{F}_q^*$ can be written $b = w_i u$ with $1 \leq i \leq s$ and $u \in \mu_m$; and*
(ii) *for every pair (i, j) there are $y, z \in \mu_m$ with $w_i y + w_j z = -1$.*

Then for all $b, c \in \mathbb{F}_q^*$ there are $y, z \in \mathbb{F}_q$ with $y^m = z^m = 1$ and $by + cz = -1$; in particular, if $q \equiv 1 \pmod r$ and $m = (q-1)/r$, then $P(q, r)$ holds.

Proof. Given $b, c \in \mathbb{F}_q^*$, write $b = w_i u$ and $c = w_j u'$ by (i); note $u, u' \neq 0$ since $u^m = 1$. Take y, z from (ii) for the pair (i, j) and replace them by yu^{-1} and zu'^{-1}, which again lie in μ_m; then $by \cdot u^{-1} + cz \cdot u'^{-1} = w_i y + w_j z = -1$. □

In practice we take $s = r$ and $w_i = g^{i-1}$ for a primitive root g of $\mathbb{F}_q$; nothing about g has to be proved, because check (i) certifies the choice on its own. The two checks cost about qrm operations in place of the roughly q^3 of a direct decision — a factor of 230 at $q = 241$, measured — and this is what puts the whole of both declared gaps inside a kernel-checked computation rather than a compiled one.

4. The counterexample at $q = 41$

Corollary 2.2 fails at $q = 41$, $r = 4$.

Proposition 4.1. *$P(41, 4)$ fails. Indeed, there are no fourth powers $y, z \in \mathbb{F}_{41}^*$ with $y + z = -1$; that is, -1 is not a sum of two fourth powers of $\mathbb{F}_{41}^*$.*

Proof. Exhaustive: the $41^2 = 1681$ pairs $(y, z) \in \mathbb{F}_{41}^2$ are scanned, and no pair with $y^{10} = z^{10} = 1$ satisfies $y + z = -1$. (The fourth powers of $\mathbb{F}_{41}^*$ are $\{1, 4, 10, 16, 18, 23, 25, 31, 37, 40\}$, so 100 pairs survive the filter.) □

Remark 4.2 (the classical mechanism). Proposition 4.1 is a statement about cyclotomic numbers, and from that side it is old. Writing $u = -by$ and $v = -cz$, the condition in $P(q, r)$ says that every ordered pair of cosets (S, T) of μ_m in $\mathbb{F}_q^*$ contains a solution of $u + v = 1$ with $u \in S$ and $v \in T$; the number of such solutions is a cyclotomic number of order r, so $P(q, r)$ fails exactly when some cyclotomic number of order r vanishes. For $r = 4$ and $p \equiv 1 \pmod 8$, with $p = a^2 + b^2$ and $a \equiv 1 \pmod 4$, the classical formula reads $16\,(0, 0)_4 = p - 11 - 6a$, and

$$p - 11 - 6a = 0 \iff (a-3)^2 + b^2 = 20 \iff (a-3, b) \in \{(\pm 2, \pm 4), (\pm 4, \pm 2)\} \iff a \in \{1, 5\},$$

after imposing $a \equiv 1 \pmod 4$; that is, $p \in \{17, 41\}$. So among the primes $p \equiv 1 \pmod 8$, exactly 17 and 41 fail to write -1 as a sum of two fourth powers of $\mathbb{F}_p^*$, and 41 is the larger. That is the mechanism behind the last failure being at 41, and behind 37 — which is $\equiv 5 \pmod 8$, and governed

by different formulas — not being one. It is not by itself a proof that the list in Remark 6.1 is complete: $P(q,4)$ involves the fifteen other cyclotomic numbers of order 4 as well, and neither the prime powers nor the primes $p \equiv 5 \pmod 8$ are covered by the display above. Completeness of that list rests on the exhaustive computation recorded there, and we use the identity only as an explanation, after checking it against a direct count at $p = 17, 41, 73, 89, 97, 113$ — a computation outside the formal development. We take the identity in the shape above from [6, §5], which reports the determination of the cyclotomic numbers of order 4 in terms of the partition $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, as Gauss's, and the resolution of the residual sign ambiguity in b — which does not enter $(0,0)_4$ — as Katre and Rajwade's [5]; see also [4].

The curve at $q = 41$. Here $r = 4$, $m = (41-1)/4 = 10$, and the curve $C_{41,4,k}$ has degree 11. The fourth powers of $\mathbb{F}_{41}^*$ are closed under negation, since $-1 = g^{20}$ is a fourth power; so the admissible k are exactly the thirty non-fourth-powers of $\mathbb{F}_{41}^*$.

Theorem 4.3. *At $q = 41$, $r = 4$, $k = 2$ the $\mathbb{F}_{41}$-line $x + y + z = 0$ carries no $\mathbb{F}_{41}$-point of the curve*

$$C_{41,4,2}\colon \qquad -(2y+z)x^{10} + zy^{10} + 2yz^{10} = 0,$$

which therefore is not blocking — although 41 is prime, $41 \geq 37$, $41 \equiv 1 \pmod 4$ and $41 \nmid 15$. Moreover $k = 2$ is admissible: -2 is not a fourth power in $\mathbb{F}_{41}^*$.

Proof. Admissibility is a scan of the 41 values of $u \in \mathbb{F}_{41}$, none of which has $u^4 = -2$. For the line: a point of $\mathbb{P}^2(\mathbb{F}_{41})$ on $x + y + z = 0$ has $x = -(y+z)$ with $(y,z) \neq (0,0)$, so it is enough to check that $F_2(-(y+z), y, z) \neq 0$ at every pair $(y,z) \neq (0,0)$, which is a scan of the $41^2 = 1681$ pairs of $\mathbb{F}_{41}^2$ and is what the computation does. A missed line refutes blocking by definition. □

The curve $C_{41,4,2}$ is not empty and not small: it carries 104 of the $41^2 + 41 + 1 = 1723$ points of $\mathbb{P}^2(\mathbb{F}_{41})$, while the line of Theorem 4.3 carries 42 of them. In all, 100 lines miss $C_{41,4,2}$, namely exactly the lines $x + by + cz = 0$ with b and c both fourth powers. These three counts are context, not part of the refutation: they come from the enumeration of §7 and not from the kernel-checked computation, which certifies the missed line and nothing about cardinalities.

Corollary 4.4. *The $r = 4$ belief of Remark 6.4 of* [1]*, "We believe that the conclusion holds for all $q \geq 37$", is false. Precisely, the following consequence of it fails: for every prime $q \geq 37$ with $q \equiv 1 \pmod 4$ and $q \nmid 15$, and every $k \in \mathbb{F}_q^*$ with $-k$ not a fourth power — the condition $q \nmid 15$ being the hypothesis $p \nmid (r^2 - 1)$ of Theorem 6.3, automatic in this range — the curve $C_{q,4,k}$ is blocking.*

Proof. Instantiate at $q = 41$, $k = 2$ and apply Theorem 4.3. The statement above weakens "smooth and nontrivially blocking" to "blocking" and restricts q to primes, so its failure refutes the belief a fortiori. □

Remark 6.4 does not write out the quantifier over k inside "the conclusion of Theorem 6.3", and the reading matters in principle: the conclusion could be read as asserted for all admissible k or for some. It does not matter here.

Theorem 4.5. *At $q = 41$, $r = 4$ the curve $C_{41,4,k}$ is blocking for* no *admissible k: for each of the thirty admissible values, at least one of the three lines*

$$x + y + z = 0, \qquad x + y + 4z = 0, \qquad x + y + 10z = 0$$

misses it.

Proof. Exhaustive over the 41 values of k: for each k with $k \neq 0$ and $u^4 \neq -k$ for all u, one of the three substituted conditions $F_k(-(y+cz), y, z) \neq 0$ for all $(y,z) \neq (0,0)$, $c \in \{1, 4, 10\}$, holds — $41 \times 3 \times 41^2$ evaluations in the worst case. The witness is $c = 4$ for $k \in \{11, 17, 19, 29\}$, $c = 10$ for $k \in \{13, 15\}$, and $c = 1$ for the remaining twenty-four admissible values. Each of the three conditions refutes blocking as in Theorem 4.3. □

So the belief fails under either reading of the quantifier.

The source's own data point, reproduced. Remark 6.4 asserts that the conclusion of Theorem 6.3 fails at $q = 29$ without exhibiting a witness. The same route reproduces it, and gives one.

Proposition 4.6. *At $q = 29$, $r = 4$ (so $m = 7$) the value $k = 1$ is admissible — -1 is not a fourth power in $\mathbb{F}_{29}^*$ — and the line $x + y + z = 0$ misses $C_{29,4,1}$, which therefore is not blocking.*

Proof. As in Theorem 4.3: 29 cases for admissibility and $29^2 = 841$ for the line. □

This is the source's failure, not ours; we record it because reproducing every data point of Remark 6.4 from the source's own definitions — all nineteen of them, across $r = 2, 3, 4, 5$: the failures at $q = 5$ ($r = 2$), 13 ($r = 3$), 29 ($r = 4$) and 101 ($r = 5$), and the fifteen successes $q \in \{7, 11, 13\}$ ($r = 2$), $q \in \{19, 25, 31, 37, 43, 49, 61, 67, 73, 79\}$ ($r = 3$), $q = 37$ ($r = 4$) and $q = 131$ ($r = 5$) — was the precondition under which we were willing to believe a disagreement at $q = 41$. All nineteen agreed.

Controls. A refutation by exhaustive search is only as good as the model that was searched. The following five checks are what would fail if the model above said the wrong thing.

Proposition 4.7.
(1) $[1 : 1 : 1]$ *lies on $C_{q,r,k}$ for every q, r and k; in particular the curve of Theorem 4.3 is not empty.*
(2) *The line $x + y + 2z = 0$ does* not *miss $C_{41,4,2}$: the substituted condition is not vacuously true.*
(3) *Exactly* 30 *of the* 41 *values of k are admissible at $q = 41$: the hypothesis of Theorem 6.3 is not vacuous there.*
(4) *The line $x + y + z = 0$ does* not *miss $C_{41,4,11}$, although $k = 11$ is admissible: the single line of Theorem 4.3 does not work uniformly in k, so Theorem 4.5 is not a restatement of Theorem 4.3.*
(5) *None of the lines $x + y + cz = 0$, $c \in \{1, 4, 10\}$, misses $C_{37,4,2}$ — the substituted form reports no miss at $q = 37$, the source's own positive data point.*

Proof. (1) is the identity $-(k + 1) + 1 + k = 0$. (2), (4) and (5) exhibit points and are decided by the same q^2-pair scan as Theorem 4.3; (3) filters the 41 values of k against the 41 values of u. □

Items (4) and (5) are the two directions in which a refutation of this shape usually goes wrong: (4) refutes a claim that would have been too large, (5) a phrasing that would have been too small, by confirming that the machinery reports *no* miss where the source says the conclusion holds.

5. The positive half

$r = 4$: the rest of the declared range. The range in which the $r = 4$ belief asserts something that Theorem 6.3 does not already prove consists of the prime powers $q \equiv 1 \pmod 4$ with $37 \le q \le 256$ and $p \nmid 15$. There are twenty-three of them: twenty primes, and the three prime powers $49 = 7^2$, $121 = 11^2$ and $169 = 13^2$.

Theorem 5.1. *Let q be one of the nineteen primes*

$$37,\ 53,\ 61,\ 73,\ 89,\ 97,\ 101,\ 109,\ 113,\ 137,\ 149,\ 157,\ 173,\ 181,\ 193,\ 197,\ 229,\ 233,\ 241$$

— that is, one of the primes $q \equiv 1 \pmod 4$ with $37 \le q \le 256$ other than 41. Then $P(q, 4)$ holds, and the curve $C_{q,4,k}$ is blocking for every $k \in \mathbb{F}_q$.

Proof. For each such q we exhibit four representatives $w_i = g^{i-1}$, g the least primitive root of $\mathbb{F}_q$, and verify the two conditions of Lemma 3.3 by exhaustive evaluation: condition (i) over the q elements b against the $4m$ products $w_i u$ with $u \in \mu_m$, condition (ii) over the 16 representative pairs against the m^2 pairs $(y, z) \in \mu_m^2$. Proposition 3.1 then gives the blocking conclusion for every k. No case is argued by hand; every one of the nineteen is a finite computation, and each was carried out in the kernel of the proof assistant. □

Corollary 5.2. *$q = 41$ is the only prime power at which the $r = 4$ belief of Remark 6.4 fails, and the sharp threshold for the conclusion of Theorem 6.3 at $r = 4$ is $q \ge 49$.*

Proof sketch. Theorem 5.1 covers the nineteen primes of the range other than 41; Theorem 4.5 settles 41; the three prime powers 49, 121, 169 are covered by the enumeration described in §7, which verifies $P(q,4)$ there directly and, independently, walks all q^2+q+1 lines of $\mathbb{P}^2(\mathbb{F}_q)$ against $C_{q,4,k}$ for every admissible k. Above $q=256$ the conclusion is Theorem 6.3 of [1] itself, so no residual range is left. For sharpness, the same enumeration shows that the conclusion fails at $q=13,17,29,41$ and at no other prime power $q\equiv 1 \pmod 4$, $p\nmid 15$, with $13\le q\le 293$; and the least prime power above 41 that satisfies those two hypotheses is 49. The two steps outside the formal development are the prime powers and the enumeration on the curve; they are labelled again in §7. □

Proposition 5.3. *At $q=257,269,277,281,293$ — all above $4^4=256$, where Theorem 6.3 of* [1] *proves the conclusion — $P(q,4)$ holds and $C_{q,4,k}$ is blocking for every k.*

Proof. As for Theorem 5.1. □

Proposition 5.3 claims nothing new; it is a control. A failure there would have been evidence of a defect in our formalisation rather than a counterexample, since in that range the statement is a published theorem.

$r=5$: the other belief. For $r=5$ the belief asserts the conclusion from $q\ge 131$ on, while Theorem 6.3 proves it only above 625. The range in between contains twenty primes $q\equiv 1 \pmod 5$ and, after the hypothesis $p\nmid 24$ removes $q=256$, exactly one prime power, $361=19^2$.

Theorem 5.4. *Let q be one of the twenty primes*

$$131,\ 151,\ 181,\ 191,\ 211,\ 241,\ 251,\ 271,\ 281,\ 311,$$
$$331,\ 401,\ 421,\ 431,\ 461,\ 491,\ 521,\ 541,\ 571,\ 601$$

— that is, the primes $q\equiv 1 \pmod 5$ with $131\le q\le 625$. Then $P(q,5)$ holds and the curve $C_{q,5,k}$ is blocking for every $k\in\mathbb{F}_q$.

Proof. As for Theorem 5.1, with five representatives $1,g,g^2,g^3,g^4$ and 25 representative pairs, $m=(q-1)/5$ throughout. □

Corollary 5.5. *The $r=5$ belief of Remark 6.4 of* [1] *is true over the whole of its declared range, and is slightly conservative: the sharp threshold is $q\ge 121$ rather than $q\ge 131$.*

Proof sketch. Theorem 5.4 covers the twenty primes; the enumeration of §7 verifies $P(q,5)$ at the remaining prime power $361=19^2$ of the range, and also at $121=11^2$, which lies just below the threshold of the belief. Above 625 the conclusion is Theorem 6.3, so there is no residual range. Sharpness: the same enumeration shows that $P(q,5)$ fails at $q=11,16,31,41,61,71,101$ and nowhere else, and of these only $q=16$ is removed by $p\nmid 24$; so $P(q,5)$, and with it the conclusion, holds at every prime power from $q=121$ on that satisfies the remaining hypotheses. That 121 and not something smaller is the threshold is the source's own data point $q=101$, where the conclusion genuinely fails — reproduced here on the curve. For the other five values of the list we assert only the failure of $P(q,5)$, not of the conclusion. □

6. The exact range of Corollary 2.2 for $r\le 5$

The reduction ($\star$) makes the question "for which q does Theorem 6.3 hold?" equivalent to the question "for which q does Corollary 2.2 hold?", and the second question has a complete answer for every small r, because above r^4 it is a published theorem and below r^4 it is a finite computation. The following remark records that answer. It is stated outside the formal development: it ranges over all prime powers, and a computable model of $\mathbb{F}_{p^n}$ for $n>1$ is not part of our development.

Remark 6.1 (computation outside the formal development). Over *all* prime powers $q\equiv 1 \pmod r$, the conclusion of Corollary 2.2 of [1] — equivalently, by Lemma 2.3, the property $P(q,r)$ — fails

exactly at

r	prime powers where Corollary 2.2 fails	r^4
2	3, 5	16
3	4, 7, 13, 16	81
4	5, 9, 13, 17, 25, 29, 41	256
5	11, 16, 31, 41, 61, 71, 101	625

Each list is complete, not merely searched: the searches ran over all pairs $(b, c) \in (\mathbb{F}_q^*)^2$, with no coset argument assumed, up to $q \le 199$, 289, 1193 and 691 respectively, and each of those bounds passes r^4, above which Corollary 2.2 is a theorem of [1]. Inside the formal development are the failure at $q = 41$ (Proposition 4.1) and, at $r = 4$ and $r = 5$, the positive prime cases on which the thresholds of the next display turn (Theorems 5.1 and 5.4, Proposition 5.3). Everything else here — the remaining failures, the rows $r = 2$ and $r = 3$, and every prime power $q = p^n$ with $n > 1$ — is computation outside it.

Intersecting with the remaining hypotheses of Theorem 6.3 — which drop $q = 3$ at $r = 2$, $q = 4, 16$ at $r = 3$, $q = 5, 9, 25$ at $r = 4$ and $q = 16$ at $r = 5$, since there $p \mid (r^2 - 1)$ — and applying $(\star)$ yields the thresholds

$$r = 2 :\ q \ge 7; \qquad r = 3 :\ q \ge 19; \qquad r = 4 :\ q \ge 49; \qquad r = 5 :\ q \ge 121,$$

each of them sharp, and each of them well below the r^4 of the hypothesis. For $r = 2$ and $r = 3$ these agree with what Remark 6.4 already reports. For $r = 4$ the threshold sits above the 37 of the belief, with exactly one admitted prime power, $q = 41$, in between; for $r = 5$ it sits one admitted prime power below the 131 of the belief.

Remark 6.2 (a computer check in [1] that can be dropped). The proof of [1, Thm. 1.8] reads, verbatim: "When $q = 5, 13$, one can check C is smooth and nontrivially blocking using a computer. Next, we assume $q \ge 17$ so that Corollary 2.2 can be applied with $r = 2$." The bound $q \ge 17$ there is exactly $q > 2^4 = 16$. By the $r = 2$ line of Remark 6.1, Corollary 2.2 in fact holds at every odd prime power except $q = 3$ and $q = 5$, so the general argument already covers $q = 13$ and only $q = 5$ needs a separate check. Theorem 1.8 is true as stated; its proof is one case shorter. (The passage is §7.1 of [1], the proof of its Theorem 1.8; the section and theorem numbers agree in arXiv:2208.13299v2 and in the published version.)

Remark 6.3 (beyond $r = 5$: an extension, not a correction). Remark 6.4 of [1] stops at $r = 5$. Over primes alone — prime powers were not swept — the same enumeration gives, again completely, since the search reached $q \le 4000$, past both $6^4 = 1296$ and $7^4 = 2401$: Corollary 2.2 fails at

$$r = 6 : q = 7,\ 13,\ 19,\ 31,\ 37,\ 43,\ 61,\ 67,\ 73,\ 79,\ 97,\ 109,\ 139,\ 157,\ 223,\ 277;$$
$$r = 7 : q = 29,\ 43,\ 71,\ 113,\ 127,\ 491.$$

Restricted to primes, the largest failure is $5, 13, 41, 101, 277, 491$ for $r = 2, \dots, 7$, against $r^4 = 16, 81, 256, 625, 1296, 2401$: a ratio between 3.2 and 6.3 at each of the six points. Fitting a growth rate to six points is not a claim, and we make none; the honest statement is that the sharp thresholds are known for $r \le 5$ and that nothing here bears on the uniformity in r that [1] calls out of reach.

7. Verification

Every theorem, proposition and corollary of §§3–5 has been formally verified in Lean 4 against *Mathlib* [7, 8], with three exceptions: Lemma 2.3, whose statement quantifies over complex characters and is the bridge into the finite condition rather than part of it, and the two summarising Corollaries 5.2 and 5.5, whose proof sketches draw on the enumeration as they say. The development is seven files and about 1100 lines, and contains no `sorry` and no hand-written `axiom`: under `#print axioms` each of its 35 declarations reports a subset of the standard set `propext`, `Classical.choice`, `Quot.sound`, several of the elementary lemmas reporting only the first and third. Every exhaustive search — the 1681-pair scan of Theorem 4.3, the 41-value scan of Theorem 4.5, and the two coset checks at each of

the nineteen primes of Theorem 5.1, the five of Proposition 5.3 and the twenty of Theorem 5.4 — is decided *by the kernel* of the proof assistant (`decide` and `decide +kernel`); the compiled-evaluation escape hatch `native_decide` is used nowhere in the development, which is what the coset reduction of Lemma 3.3 buys. A full rebuild of the seven files takes 1219 seconds on a shared twenty-core machine. Outside the formal development lie exactly four things, each labelled where it appears: the equivalence of Lemma 2.3; the prime powers, which need a computable model of $\mathbb{F}_{p^n}$ that the residue ring $\mathbb{Z}/q\mathbb{Z}$ is not; the tables of Remarks 6.1 and 6.3; and the direct enumeration on the curve, a C program that builds $\mathbb{P}^2(\mathbb{F}_q)$, computes $C_{q,r,k}(\mathbb{F}_q)$ for every admissible k, walks all q^2+q+1 lines, and reports blocking, nontriviality and smoothness at the $\mathbb{F}_q$-points, run over the 32 prime powers $13 \le q \le 293$ at $r = 4$. The refutation at $q = 41$ was produced independently three times — by that C program, by a Python program which agrees on the point count 104, the 100 missed lines and the 30 admissible k, and by the proof assistant's kernel — and every data point of Remark 6.4 of [1] was reproduced before the disagreement at $q = 41$ was accepted.

Acknowledgement of the source. We are indebted to the authors of [1] for a construction stated precisely enough to be tested, for computer checks reported in enough detail to be reproduced, and for flagging the hypothesis $q > r^4$ as probably non-optimal in the first place. The correction above concerns one sentence of one remark and leaves every theorem of that paper intact. The citation lists behind the statement in §1 that no later work returns to Remark 6.4 — six citing works, every one of them fetched as an e-print and searched — were consulted on 3 September 2026.

References

[1] S. Asgarli, D. Ghioca, C. H. Yip, *Plane curves giving rise to blocking sets over finite fields*, Designs, Codes and Cryptography **91** (2023), no. 11, 3643–3669; DOI 10.1007/s10623-023-01264-y. Also arXiv:2208.13299 (v1 28 August 2022, v2 31 May 2023). The Section 6 sources of v1 and v2 are byte-identical, and Theorem 6.3, Remark 6.4 and Corollary 2.2 read word for word the same in the published version; numbering above follows the published version.

[2] S. Asgarli, D. Ghioca, C. H. Yip, *Blocking sets from a union of plane curves*, arXiv:2510.15332 (17 October 2025).

[3] A. Blokhuis, *On the size of a blocking set in* $\mathrm{PG}(2,p)$, Combinatorica **14** (1994), no. 1, 111–114; DOI 10.1007/BF01305953. Cited here for context only.

[4] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424; DOI 10.2307/2371217.

[5] S. A. Katre and A. R. Rajwade, *Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum*, Math. Scand. **60** (1987), 52–62; DOI 10.7146/math.scand.a-12171.

[6] Md. H. Ahmed and J. Tanti, *Jacobi sums and cyclotomic numbers: A survey report*, arXiv:1906.09960v1 (21 June 2019). Section numbers cited above are those of v1, the only version.

[7] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28 (A. Platzer and G. Sutcliffe, eds.), Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.

[8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381.