Blocking sets of PG(2, 13) invariant under a fixed-point-free Singer subgroup meet some line in five points

Dev D. Goyal

31 October 2026; revised 1 November 2026

Abstract

Let H be the subgroup of order three of a Singer cycle group of the projective plane $\mathrm{PG}(2,13)$; it fixes no point. We show that every H-invariant blocking set of $\mathrm{PG}(2,13)$ meets some line in at least five points. The 21-point blocking set of Blokhuis, Brouwer and Wilbrink [1] is invariant under a conjugate of H and meets every line in at most five points, so five is the least possible largest line intersection of an H-invariant blocking set. Every fixed-point-free collineation of order three of $\mathrm{PG}(2,13)$ generates a conjugate of H, so the statement holds for all of them. This settles one symmetric case of the plane of order 13 in Erdős Problem 1159 [2], which asks whether every finite projective plane has a point set meeting each line in at least one and at most C points; a public computational campaign [4] had recorded this case as unresolved. The proof reduces the question to 61 weighted line conditions on the orbits of H and shows by exhaustive search that they have no solution with intersections at most four. A Lean 4 project proves the theorem for the specified subgroup, with $\mathrm{PG}(2,13)$ modelled by Mathlib's projectivization of $\mathbb{F}_{13}^3$; the search runs in the Lean kernel and is covered by a soundness proof. An independent Python program repeats the geometry, the witness checks and the search.

1 Introduction and result

A *blocking set* of a projective plane is a set of points meeting every line. Erdős asked whether there is a constant C such that every finite projective plane has a point set S with $1 \le |S \cap \ell| \le C$ for all lines ℓ [2]; Erdős, Silverman and Stein proved that $|S \cap \ell| = O(\log n)$ can be achieved in a plane of order n [3]. For a particular plane the question becomes the computation of

$$c(\Pi) = \min_{B} \max_{\ell} |B \cap \ell|,$$

the minimum over blocking sets B of the largest line intersection. For the Desarguesian plane $\mathrm{PG}(2,13)$ of order 13 the 21-point blocking set of Blokhuis, Brouwer and Wilbrink [1] shows $c(\mathrm{PG}(2,13)) \le 5$. A public computational campaign on this problem [4] searched for blocking sets of $\mathrm{PG}(2,13)$ with all line intersections at most four that are invariant under various collineation groups; for the subgroup of order three of a Singer group, whose 61 point orbits all have size three, its solver run ended with status UNKNOWN after 90 seconds. We settle that case.

Let $\mathbb{F} = \mathbb{F}_{13}[\theta]/(\theta^3 + \theta + 6)$. The powers of θ are pairwise distinct up to $\theta^{2196} = 1$, so $\mathbb{F}$ is the field with 13^3 elements and θ is primitive. We identify the points of $\mathrm{PG}(2,13)$ with the one-dimensional $\mathbb{F}_{13}$-subspaces of $\mathbb{F}$, written in the basis $1, \theta, \theta^2$, and the lines with the two-dimensional subspaces. Multiplication by θ induces a collineation σ of order $183 = 13^2 + 13 + 1$, a *Singer cycle*; let $H = \langle \sigma^{61} \rangle$, of order three. Since σ^{61} maps the point $\langle \theta^i \rangle$ to $\langle \theta^{i+61} \rangle \neq \langle \theta^i \rangle$, H fixes no point.

Theorem 1. *Every H-invariant blocking set of* $\mathrm{PG}(2,13)$ *meets some line in at least five points. There is an H-invariant minimal blocking set of* 21 *points that meets every line in at most five points. Hence*

$$\min\{\max_{\ell} |B \cap \ell| : B \text{ an } H\text{-invariant blocking set of } \mathrm{PG}(2,13)\} = 5.$$

The lower bound has no size or minimality assumption on B. The upper bound is the known example of [1] (Section 4). Since 13 is prime, every collineation of $\mathrm{PG}(2,13)$ is a projectivity.

Corollary 2. *Let g be a collineation of* $\mathrm{PG}(2,13)$ *of order three without fixed points. Then every $\langle g\rangle$-invariant blocking set meets some line in at least five points, and five is attained.*

The corollary follows from Theorem 1 and the conjugacy argument of Section 5. It does not decide whether $c(\mathrm{PG}(2,13))$ is 4 or 5: blocking sets without this symmetry are not covered.

2 The cyclic model and the reduction

For $i \in \mathbb{Z}_{183}$ let $P_i = \langle\theta^i\rangle$; these are all 183 points. The points whose coordinate vector has constant coefficient zero form a line,

$$L_0 = \{P_d : d \in D\}, \qquad D = \{1,2,4,17,24,29,43,77,83,87,120,138,155,176\},$$

and the lines of $\mathrm{PG}(2,13)$ are exactly $L_t = \sigma^t(L_0) = \{P_{d+t} : d \in D\}$ for $t \in \mathbb{Z}_{183}$; D is a planar difference set modulo 183. The subgroup H acts by $i \mapsto i+61$, with the 61 orbits $O_j = \{P_j, P_{j+61}, P_{j+122}\}$, $j \in \mathbb{Z}_{61}$. An H-invariant set is $B_S = \bigcup_{j\in S} O_j$ for a unique $S \subseteq \mathbb{Z}_{61}$, and

$$|B_S \cap L_t| = r_S(t) := \#\{d \in D : d + t \bmod 61 \in S\},$$

which depends only on t mod 61. Modulo 61 the elements of D are

$$1,2,4,16,16,17,22,24,26,29,33,43,54,59,$$

with 16 twice (77 and 138) and the others once. Thus each of the 61 conditions involves twelve orbits with weight one and one orbit, the *doubled* orbit $t+16$, with weight two. The 61×61 weight matrix M is circulant and satisfies $MM^{\mathsf{T}} = 13I + 3J$.

Lemma 3. *For $c \geq 1$ there is an H-invariant blocking set with all line intersections at most c if and only if there is $S \subseteq \mathbb{Z}_{61}$ with $0 \in S$ and $1 \leq r_S(t) \leq c$ for all $t \in \mathbb{Z}_{61}$.*

Proof. The first condition holds for B_S exactly when $1 \leq r_S(t) \leq c$ for all t. A blocking set is nonempty, so some $j \in S$. The collineation σ^{-j} commutes with H, maps B_S to B_{S-j} and permutes the lines, so $S - j$ is again a solution, and it contains 0. □

Remark 4. Since $\sum_t r_S(t) = 14|S|$ and, by $M^{\mathsf{T}}M = 13I + 3J$, $\sum_t r_S(t)^2 = 3|S|^2 + 13|S|$, summing $(r_S(t)-1)(r_S(t)-4) \leq 0$ shows that a solution for $c = 4$ would have $7 \leq |S| \leq 12$. This is not used below.

3 No solution with intersections at most four

Proposition 5. *There is no $S \subseteq \mathbb{Z}_{61}$ with $0 \in S$ and $1 \leq r_S(t) \leq 4$ for all $t \in \mathbb{Z}_{61}$.*

Proof. We search over partial assignments, which fix some orbits as chosen and some as excluded; orbit 0 is chosen at the start. A node is closed when some condition t already has weight at least five on the chosen orbits, or all its orbits are excluded. Before branching we apply the forced steps: if a condition with no chosen orbit has exactly one orbit that is not excluded, that orbit is

chosen; if a condition has weight four, its other orbits are excluded; if it has weight three, its doubled orbit is excluded. Each step is valid for every solution extending the node. If no node is closed and no step applies, we pick a condition with no chosen orbit and fewest available orbits and branch on which of them is the first chosen one. Every branch of this finite search closes, so no solution exists. The Python implementation described in Section 6 visits 156,717 nodes. □

The lower bound of Theorem 1 follows from Lemma 3 with $c = 4$ and Proposition 5.

4 The matching example

Let $S_0 = \{0, 1, 13, 14, 47, 48, 60\} \subseteq \mathbb{Z}_{61}$. The 21-point set B_{S_0} meets 126 lines in one point, 36 lines in two points, 9 lines in four points and 12 lines in five points; every point of B_{S_0} lies on a tangent line, so B_{S_0} is a minimal blocking set. This proves the upper bound in Theorem 1.

The set is the sporadic example of [1, Section 5.3]. In the coordinates of that paper it consists of the three vertices of the reference triangle, the points $(1, a, 0)$, $(0, 1, a)$, $(a, 0, 1)$ with $a^3 = -1$, and the points $(b, c, 1)$ with $b^3 = c^3 = 1$. It is invariant under the projectivity of

$$A = \begin{pmatrix} 0 & 12 & 0 \\ 0 & 0 & 4 \\ 12 & 0 & 0 \end{pmatrix}, \qquad A^3 = 4I,$$

which has no fixed point because 4 is not a cube in $\mathbb{F}_{13}$. With

$$K = \begin{pmatrix} 1 & 7 & 8 \\ 0 & 10 & 1 \\ 0 & 4 & 12 \end{pmatrix}$$

one has $K(7A) = TK$, where T is the matrix of multiplication by θ^{61}, and K maps the set of [1] onto B_{S_0}. No new construction is claimed.

5 All fixed-point-free subgroups of order three

Let g be a collineation of order three without fixed points and let A be a matrix inducing it, so $A^3 = aI$ with $a \in \mathbb{F}_{13}^{\times}$. If $a = b^3$, then $(b^{-1}A)^3 = I$; since $13 \equiv 1 \pmod 3$, the polynomial $X^3 - 1$ splits into distinct linear factors over $\mathbb{F}_{13}$, so $b^{-1}A$ is diagonalizable and has an eigenvector, a fixed point of g. Hence a is not a cube, $X^3 - a$ has no root and is irreducible, and it is the minimal polynomial of the nonscalar matrix A. Then $E = \mathbb{F}_{13}[A]$ is a field with 13^3 elements and $\mathbb{F}_{13}^3$ is a one-dimensional E-vector space, so g lies in the image of $E^{\times}$ in $\mathrm{PGL}(3, 13)$, a Singer group. Any two subfields of the matrix algebra isomorphic to $\mathbb{F}_{13^3}$ are conjugate under $\mathrm{GL}(3, 13)$ (identify $\mathbb{F}_{13}^3$ with either field), so all Singer groups are conjugate, and a cyclic group of order 183 has exactly one subgroup of order three. Therefore $\langle g \rangle$ is conjugate to H. A projectivity carrying H to $\langle g \rangle$ carries H-invariant blocking sets to $\langle g \rangle$-invariant ones and preserves line intersections, which gives Corollary 2. This section is a conventional argument and is not part of the Lean proof.

6 Verification

Lean. The package contains a Lean 4.35.0 project using Mathlib revision `56a0058`. Points and lines of $\mathrm{PG}(2, 13)$ are both elements of Mathlib's `Projectivization (ZMod 13) (Fin 3 → ZMod 13)`, and a point lies on a line when the dot product of representatives vanishes. The Singer cycle is the projectivity of the matrix of multiplication by θ, and H is generated by its 61st iterate. The project proves that the cycle has order exactly 183, that its 61st iterate has order

three and fixes no point, the properties of the 21-point witness, the reduction of Lemma 3 for arbitrary point sets, Proposition 5, and the final statement `SingerC3.isLeast_admissibleCaps`: 5 is the least c for which an H-invariant blocking set with all line intersections at most c exists.

The search of Proposition 5 is a Lean function `go` that is evaluated by the kernel with `decide +kernel`. It takes only five kinds of steps, each checked against the actual line counts r_S: closing a node, excluding an orbit after checking that choosing it would close the node, choosing an orbit after checking that excluding it would close the node, excluding the available orbits of a condition of weight four, and splitting on an orbit. A separate heuristic on packed line counts decides which step to take. The soundness theorem `go_sound` holds for every value of the heuristic, so its correctness is not needed. The search is split into a top search from the root and 342 subsearches with at most 4,961 steps each; together they take 771,752 steps. Finite facts about the coordinate model are also decided by the kernel. There is no `native_decide`, no compiled-code evaluation and no added axiom, and every declaration of the project depends only on `propext`, `Classical.choice` and `Quot.sound`. The kernel search takes about an hour of processor time in total.

Python. The program `certificate/check_singer.py` uses only the Python standard library. It recomputes the field, the 183 points, all lines from their coordinate equations, the difference set D, the 61 conditions and the identity $MM^{\mathsf{T}} = 13I + 3J$; it checks the witness, its intersection numbers, its tangents and the conjugacy to the set of [1]; and it runs the search of Proposition 5.

7 Limitations

The result concerns one conjugacy class of subgroups. Whether $\mathrm{PG}(2, 13)$ has a blocking set with all line intersections at most four, without symmetry, is not decided here. The identification of D as the line set is checked by computation and in Lean; the conjugacy statement of Section 5 is not formalized. The literature comparison is bounded, and historical priority is not certified.

8 Research process and AI disclosure

This is fully autonomous agentic research. Dev D. Goyal is responsible for publication. The work has not been externally peer reviewed, no expert validation is claimed, and the novelty assessment is provisional.

Autonomous AI research agents selected the question, found the reduction to 61 orbit conditions, identified the witness with the example of [1], produced and checked a solver certificate for Proposition 5, wrote their own Lean proof and searched the literature in an earlier session, which also ran internal AI-assisted reviews that are not peer review. Its records describe the research and review agents as Astra agents. The same session proposed a second result, a logarithmic lower bound for the number of bounded-degree plane curves whose rational points block all lines; it is not part of this paper.

Opus 5.5 by Anthropic used with Claude Code assessed the package for this release. It wrote the Lean project used here, including the kernel search and its soundness proof, ran its fresh build and axiom audit, wrote the independent Python checker and this manuscript, and integrated the package into the repository. It also made the editorial revision of 1 November 2026, which did not change the mathematics. The solver certificate and the earlier Lean proof are not included. AI checks are not human peer review. Section 6 states the formal scope and Section 7 the remaining limits.

References

[1] A. Blokhuis, A. E. Brouwer and H. A. Wilbrink, *Blocking sets in $PG(2,p)$ for small p, and partial spreads in $PG(3,7)$*, Advances in Geometry **3** (2003), special issue, S245–S253. doi:10.1515/advg.2003.2003.s1.245.

[2] T. F. Bloom, *Erdős Problem #1159*, erdosproblems.com/1159, accessed 31 October 2026.

[3] P. Erdős, R. Silverman and A. Stein, *Intersection properties of families containing sets of nearly the same size*, Ars Combinatoria **15** (1983), 247–259.

[4] Erdős problem verification campaign, problem 1159, orbit-search log for $q = 13$, commit `7bccace`, github.com/pw/erdosproblemaday-verification, accessed 31 October 2026.