SOLUBLE SUBGROUP PAIRS IN SYMMETRIC AND ALTERNATING GROUPS

QIYUE TANG

Abstract. We prove that every pair of soluble subgroups of the symmetric group S_n or the alternating group A_n has trivially intersecting conjugates whenever $n \geq 21$. This answers the second question of Anagnostopoulou-Merkouri and Burness in Problem 21.3 of the Kourovka Notebook.

hexagon:2611.00042v1

AI use and scholarly credit. The proof was developed using ChatGPT-6-Pro in a research conversation lasting approximately 157 minutes, as recorded in the research package. AI contributed to the mathematical arguments, computations, and internal review. The proof also passed an external AI-assisted check using Rethlas-OSV [13]. This revision was prepared and checked with Codex. The finite calculations use exact arithmetic and permutation and graph algorithms.

By posting this manuscript on this platform, I do not seek to assert ownership of the results or claim priority. I welcome anyone interested in preparing a finished account or checking the arguments; the eventual scholarly credit should go to those who undertake that work.

1. Introduction

For each integer $n \geq 1$, let $\Omega = \{1, \dots, n\}$, let $S_n = \mathrm{Sym}(\Omega)$ be its full permutation group, and let A_n be the subgroup of even permutations. The sign $\mathrm{sgn}(x)$ of $x \in S_n$ is 1 for an even permutation and -1 for an odd permutation. Permutations act on the right, so $v^{xy} = (v^x)^y$. A base for a faithful permutation group is a set of points whose pointwise stabilizer is the identity. In the transitive action of a finite group G on the cosets of a core-free subgroup H, the least base size is the least number of conjugates of H with trivial intersection. Here core-free means that $\bigcap_{g \in G} H^g = 1$, with $H^g = g^{-1}Hg$. This connects base-size questions with the older problem of intersecting conjugate Sylow, nilpotent, and soluble subgroups.

Two developments explain the role of solubility. Dixon's order bound [7, Theorem 3] gives $|H| \leq 24^{(n-1)/3}$ for a soluble subgroup $H \leq S_n$, with equality for suitable iterated wreath products on 4^a points. Seress [8, Theorem 1.1] proved in 1996 that every primitive soluble permutation group has a base of size at most four. The affine structure of primitive soluble groups and the recurrence of small symmetric wreath factors are central in both types of argument.

There are related intersection theorems for larger ambient groups. Baykalov [9] proved that five conjugates suffice for any soluble subgroup of an almost simple group with alternating socle: if H is such a subgroup of G, then $H \cap H^{x_1} \cap \cdots \cap H^{x_4} = 1$ for suitable $x_i \in G$. Burness [10] subsequently proved that a finite primitive group with soluble point stabilizer has base size at most five, and determined the exact values for almost simple primitive groups. These results control repeated conjugates of a single subgroup. The mixed-pair question also permits the two subgroups to belong to different conjugacy classes.

Date: November 3, 2026.

2020 Mathematics Subject Classification. Primary 20B30; Secondary 20B35, 20-08. *Keywords.* Soluble subgroup, symmetric group, alternating group, regular pair, wreath product.

A pair (H, K) of subgroups of G is called regular when $H \cap K^x = 1$ for some $x \in G$. Equivalently, the diagonal action of G on the product of the two coset spaces has a point with trivial stabilizer. Thus regular pairs extend the base-size-two question from repeated stabilizers to arbitrary pairs. Zenkov [11] proved that every pair of nilpotent subgroups in a nonsoluble finite symmetric or alternating group is regular, apart from the symmetric group S_8.

Cameron [12] considered group invariants obtained by maximizing base-size measures over permutation representations. Anagnostopoulou-Merkouri and Burness [1] extended this viewpoint to arbitrary subgroup tuples. For $k \geq 1$, a tuple $(H_1, \ldots, H_k)$ is regular if $\bigcap_{i=1}^{k} H_i^{x_i} = 1$ for some $x_1, \ldots, x_k \in G$. Their regularity number $R(G)$ is the least k for which every tuple of k core-free subgroups is regular. Write $R_{\mathrm{sol}}(G)$ for the corresponding invariant with all entries soluble. Repetitions are allowed. For S_n and A_n, $n \geq 5$, every soluble subgroup is core-free: a nonidentity normal subgroup contains the insoluble group A_n.

In [1], the authors determine $R(S_n) = n - 1$ and $R(A_n) = n - 2$, and treat soluble maximal subgroups. They conjecture that $R_{\mathrm{sol}}(S_n) = R_{\mathrm{sol}}(A_n) = 2$ for all sufficiently large n. Their example $(S_4 \wr S_4) \times S_4 \leq S_{20}$ is a nonregular pair with itself. They also find that the same subgroup, acting with one additional fixed point in degree 21, has a disjoint conjugate. This leads to the proposed threshold 21. Both the eventual question and the threshold question appear in Problem 21.3 of the Kourovka Notebook [2]; we call its second question Problem 21.3(b).

Nilradical [4] proves the eventual assertion. More precisely, the least proportion of separating conjugators, over all soluble pairs in S_n, tends to $e^{-9/2}$. The public note revised September 17, 2026 leaves the effective cutoff, including the threshold 21, open. Its proof organizes soluble groups into affine wreath forests, first separates their transposition-generated subgroups, and then controls elements outside those subgroups. We use that forest and core strategy to obtain a numerical bound valid from degree 128, followed by finite certificates and lifting to cover degrees 21 through 127.

Theorem 1.1. *Let $n \geq 21$ be an integer, and let $H, K \leq S_n$ be soluble. For each $\varepsilon \in \{1, -1\}$ there is $x \in S_n$ such that*

$$\operatorname{sgn}(x) = \varepsilon, \qquad H \cap K^x = 1.$$

Consequently, every soluble pair in either S_n or A_n is regular, and

$$R_{\mathrm{sol}}(S_n) = R_{\mathrm{sol}}(A_n) = 2.$$

The proof is computer assisted. For $n \geq 128$ the infinite range is handled by uniform inequalities, with finite exact arithmetic establishing their numerical bounds. For $21 \leq n \leq 127$ the proof uses explicit separating permutations. Section 8 describes the exhaustive coverage, the graph interpretation of these witnesses, and the finite induction. The supplementary archive specified in Appendix C contains the data and reproducible checks.

For an integer $n \geq 1$, write $Q(n)$ for the assertion that every soluble pair in S_n has separating conjugators of both prescribed signs. For a permutation g on a set Ω, $\operatorname{supp}(g) = \{v \in \Omega : v^g \neq v\}$; its support size is $|\operatorname{supp}(g)|$. A set is invariant under a group if it is preserved setwise. For $B \subseteq \Omega$, $K_B = \{g \in K : B^g = B\}$ and $K_{(B)} = \{g \in K : v^g = v \text{ for all } v \in B\}$ are its setwise and pointwise stabilizers. If C is K-invariant, $K|_C$ denotes the image of the restriction homomorphism $K \to \mathrm{Sym}(C)$. A soluble group means a finite group whose derived series terminates at the identity. We use $0! = 1$, give every empty product the value one, and set $\mathrm{GL}(0, \ell) = 1$.

2. Affine forests and lifting

For a prime ℓ, let $\mathbb{F}_\ell$ be the field with ℓ elements and $\mathrm{GL}(d, \ell)$ the group of invertible linear maps of $\mathbb{F}_\ell^d$, where $d \geq 1$. For a prime power $q = \ell^d$, put $A(q) = \mathrm{AGL}(d, \ell)$ in its

natural action on $\mathbb{F}_\ell^d$. Thus $A(q)$ consists of the maps $v \mapsto Tv + b$, where $T \in \mathrm{GL}(d, \ell)$ and $b \in \mathbb{F}_\ell^d$. A word $w = (q_1, \ldots, q_r)$, where $r \geq 0$ and each q_i is a prime power at least two, denotes the imprimitive wreath product

$$W(w) = A(q_1) \wr \cdots \wr A(q_r),$$

ordered from bottom to top, of degree $\prod_i q_i$. In $L \wr Q = L^q \rtimes Q$, where $Q \leq S_q$ and L has degree m, the q child blocks each carry a copy of the m-point action of L. The group Q permutes those blocks. Elements of L^q give their separate actions within the blocks; these are the sections. This is the imprimitive action on mq points. The empty word denotes the identity group on one point. A full affine forest is a direct product of these word groups on disjoint point sets. The associated rooted trees have leaves equal to the points; at each node the children carry a natural full affine action. These forests may be insoluble.

Lemma 2.1. *Every soluble subgroup of S_n is contained, after relabelling, in a full affine forest of degree n.*

Proof. Let P be a faithful primitive soluble group of degree greater than one, and choose a minimal nonidentity normal subgroup V. The last nonidentity term of the derived series of V is characteristic in V and normal in P, so minimality makes V abelian. A Sylow subgroup of V and its subgroup of elements killed by the corresponding prime are characteristic; minimality therefore makes V elementary abelian. Its orbits form a block system. Primitivity makes this either one orbit or the singleton partition; the latter would make V act trivially, contrary to faithfulness. Thus V is transitive. An abelian transitive faithful group is regular: its point stabilizers coincide and their intersection is the kernel. Choose an origin in its regular orbit and identify that orbit with $V \cong \mathbb{F}_\ell^d$. The origin stabilizer acts by conjugation as a subgroup of $\mathrm{GL}(d, \ell)$. Its kernel centralizes the regular group V and fixes the origin, hence fixes every point and is trivial. Thus $P \leq V \rtimes \mathrm{GL}(d, \ell) = A(\ell^d)$.

For a transitive imprimitive soluble group, choose a minimal nonsingleton block B. The induced setwise-stabilizer action on B is primitive. Indeed, a smaller nontrivial block for this action is a block for the whole group: an element moving B gives a disjoint translate, and one stabilizing B preserves the smaller block relation. This contradicts minimality. The induced action on the translates of B is soluble. Write the blocks as $B_1 = B, \ldots, B_k$, and choose t_i with $B^{t_i} = B_i$. Define i^g by $B_i^g = B_{i^g}$. The section of g at i is $(t_i g t_{i^g}^{-1})|_B$, which belongs to the induced block stabilizer. For g, h, the section at i of gh is the product of the section of g at i and that of h at i^g, since the middle transporting elements cancel. This is the multiplication rule in the imprimitive wreath product. The block permutation and these sections therefore give a homomorphism into the wreath product of the two induced groups. Its kernel fixes each block and acts identically on it, so is trivial. Induction on the degree gives a word group. Finally the restriction map to the product of the actions on all orbits is injective; apply the transitive conclusion to each orbit. □

Lemma 2.2. *If $K \leq S_n$ is soluble, there is a subset B_0 of size at least $\lceil n/4 \rceil$ such that $K_{(\Omega \setminus B_0)} = 1$.*

Proof. Place K in an affine forest. In each bottom affine block of degree $q = \ell^d \geq 3$, fix an affine frame $v_0, v_0 + e_1, \ldots, v_0 + e_d$, where $e_1, \ldots, e_d$ is a vector-space basis. An affine map fixing these points has zero translation after using v_0 as origin and fixes each basis vector, so is the identity. In a degree-two block fix one point. Singleton components require no fixed point. Fixing a point in each bottom block prevents movement of these blocks, and hence movement at every higher tree level. Each affine frame then kills the action within its block. This is a base for the forest and therefore for K.

For $q \geq 3$, $d + 1 \leq 3q/4$. For $d = 1$ this follows from $q \geq 3$; for $d \geq 2$ use $d + 1 \leq 3 \cdot 2^d/4$, proved by induction from $d = 2$. The degree-two cost is also at most $3q/4$. Thus the base has size at most $\lfloor 3n/4 \rfloor$, and its complement is suitable. □

Lemma 2.3. *Suppose $H, K \le S_n$ are soluble and H has a nonempty proper invariant subset A of size b.*

(1) *If $b \le \lceil n/4 \rceil$ and $Q(n-b)$ holds, the pair has separating conjugators of both signs.*
(2) *If $Q(b)$ and $Q(n-b)$ hold, the same conclusion follows.*

Proof. Fix $\varepsilon \in \{1, -1\}$. For the first assertion take $B \subseteq B_0$ of size b from Lemma 2.2, and choose z with $B^z = A$. Set $C = \Omega \setminus A$ and $L = (K_B)^z$. The action of L on C is faithful: an element in its kernel pulls back to an element of K supported inside B, which is trivial by the choice of B.

Apply $Q(n-b)$ to the soluble restriction images $H|_C$ and $L|_C$, obtaining $y \in \mathrm{Sym}(C)$, extended by the identity on A, with these images separated. A common element of H and K^{zy} preserves A and therefore belongs to $H \cap L^y$. It fixes C pointwise, so faithfulness of L^y makes it trivial. Prescribe $\mathrm{sgn}(y) = \varepsilon \,\mathrm{sgn}(z)$.

For the second assertion choose any b-set B, align it with A, and take the same setwise stabilizer L. Apply $Q(b)$ and $Q(n-b)$ separately to its restriction images and those of H. Their product separates the images on both parts, so the common element fixes all points. Choose sign 1 on A and sign $\varepsilon \,\mathrm{sgn}(z)$ on its complement. Their product, after the alignment z, has sign ε. □

3. Orders, supports, and prime-order atoms

Put $D = 24^{1/3}$, and write log for the natural logarithm. For a polynomial or formal power series $P(z) = \sum_{i \ge 0} a_i z^i$, $[z^i]P = a_i$, with absent coefficients equal to zero. Write $P \le_{\mathrm{c}} R$ when every coefficient of $R - P$ is nonnegative. All formal exponentials below have constant term one; coefficient extraction at a fixed degree involves only finitely many terms. We use $(n)_s = n(n-1)\cdots(n-s+1)$ for $0 \le s \le n$, with $(n)_0 = 1$.

Lemma 3.1. *For every natural full affine group $A(q)$,*

$$|A(q)| \le D^{q-1}, \qquad |\{g \in A(q) : |\mathrm{supp}(g)| = j\}| \le D^j \quad (j \ge 1).$$

Every forest on $n \ge 1$ leaves has order at most D^{n-1}.

Proof. Writing $q = \ell^d$, the affine order is

$$q \prod_{i=0}^{d-1} (q - \ell^i) < q^{d+1} \le q^{\log_2 q + 1}.$$

For $q \ge 16$, the logarithm of the last expression has derivative $(2\log_2 q + 1)/q$, decreasing from $9/16 < \log D$. The endpoint inequality at 16 follows from $16^5 < 24^5$. This gives the order bound. For $q < 16$ the prime powers are $2, 3, 4, 5, 7, 8, 9, 11, 13$ and the corresponding orders are $2, 6, 24, 20, 42, 1344, 432, 110, 156$; cubing verifies the claim.

A nonidentity affine map fixes either no points or a proper affine subspace, so moves at least $q/2$ points. For $q \ge 64$, $q^{\log_2 q + 1} \le D^{q/2}$. At 64, cubing reduces this to $2^{30} \le 3^{32}$; the logarithmic derivative is $13/64 < \log D/2$ and decreases thereafter. For prime $q < 64$, the minimum support is $q - 1$, so the order bound suffices. The nonprime prime powers below 64 are $4, 8, 9, 16, 25, 27, 32, 49$. At 4 the support counts are $6, 8, 9$ for supports $2, 3, 4$; at 8 they are $42, 392, 384, 525$ for supports $4, 6, 7, 8$. At 16 the support-eight count is 210 and all other nonzero supports are at least 12; at 32 the support-sixteen count is 930 and the others are at least 24. Direct cubing checks these rows. At $9, 25, 27, 49$ the minimum supports $6, 20, 18, 42$ and the orders $432, 12000, 303264, 98784$ suffice.

For integers $0 \le b \le a$, let $\begin{bmatrix} a \\ b \end{bmatrix}_\ell$ count the b-dimensional subspaces of $\mathbb{F}_\ell^a$. Counting ordered independent vectors and dividing by the number of ordered bases of a b-space gives

$$\begin{bmatrix} a \\ b \end{bmatrix}_\ell = \prod_{i=0}^{b-1} \frac{\ell^{a-i} - 1}{\ell^{b-i} - 1}.$$

For $0 \le k \le d$, let E_k count $T \in \mathrm{GL}(d,\ell)$ with $\dim\ker(T-I) = k$. Double-count pairs consisting of a k-space and an invertible map fixing it pointwise. A map with fixed-space dimension r contributes $\begin{bmatrix} r \\ k \end{bmatrix}_\ell$ pairs. For a fixed k-space, a basis extending it gives matrices with an identity k-block, an arbitrary k by $(d-k)$ off-diagonal block, and an invertible $(d-k)$-block. Therefore

$$\sum_{r=k}^{d} \begin{bmatrix} r \\ k \end{bmatrix}_\ell E_r = \begin{bmatrix} d \\ k \end{bmatrix}_\ell \ell^{k(d-k)} |\,\mathrm{GL}(d-k,\ell)|.$$

This triangular system determines $E_d, E_{d-1}, \ldots, E_0$ in that order. For a map with fixed-space dimension k, the equation $(T-I)w = -v$ is solvable for exactly ℓ^{d-k} translation vectors v. Each solution set has ℓ^k points. Thus each such T gives ℓ^{d-k} affine maps of support $q - \ell^k$ and $\ell^d - \ell^{d-k}$ of full support.

If L, Q have degrees m, q, their wreath product has order $|L|^q|Q| \le D^{q(m-1)+(q-1)} = D^{mq-1}$. A product of r nonempty components with n leaves has order at most $D^{n-r} \le D^{n-1}$. □

For a forest M, let $T(M)$ be its transposition-generated subgroup, called its core. It is exactly the product of the bottom factors $A(2) = S_2$, $A(3) = S_3$, $A(4) = S_4$. At an internal node with child size $m > 1$, any nonidentity local permutation moves at least two child blocks and hence at least $2m \ge 4$ leaves. A transposition must therefore act in a bottom primitive factor. The affine minimum-support bound forces that factor's degree to be at most four. In particular its core blocks have size at most four.

Fix a prime p. An element satisfying $g^p = 1$ has a canonical decomposition into disjoint prime-order atoms. At a node with q child subtrees of degree m and group L, retain the complete local permutation on its moved children and all its sections there as one atom. Recurse into the fixed children. If the local permutation moves j children, each nontrivial cycle has length p. Write the local permutation as j/p disjoint p-cycles. Along one such cycle, raising the wreath element to the pth power composes its p sections cyclically. Their product must be one. Choose $p-1$ sections arbitrarily and the last is uniquely determined; the cyclically shifted products are conjugate and are one as well. Different moved cycles are independent, giving $|L|^{j-j/p}$ choices. Every moved child is transported to a different block, so all its leaves move, giving support jm. At bottom S_2, S_3, S_4 nodes, further split into individual cycles, called core cycles. Extend the moved-node data by the identity on all other blocks to obtain an element of the full wreath group. At fixed children the remaining sections have pth power one and are decomposed recursively. These supports are disjoint from the moved children. At a bottom symmetric factor each individual cycle belongs to that factor. Thus all atoms themselves lie in the forest, their supports are disjoint, and their product recovers the original element. The local moved data and the fixed-child recursion also make this decomposition unique. A subcollection multiplies to another element of the forest.

Let $N_{j,p}(A(q))$ count elements of exact order p and support j in $A(q)$. Define $O(1) = 1$ and, for $m \ge 2$,

$$O(m) = \max_{\substack{q \mid m \\ q \text{ a prime power}}} |A(q)|O(m/q)^q.$$

It is the largest order of a transitive affine word of degree m: a nonempty word has a last factor $A(q)$ for some prime power $q \mid m$, and its preceding word has degree m/q; maximizing its order gives exactly this recurrence. For this maximum words are unrestricted, including adjacent $(2,2)$. For a divisible by p define

$$d_{a,p} = \max \frac{N_{j,p}(A(q))O(m)^{j-j/p}}{qm}, \tag{1}$$

where $a = jm$, $p \mid j$, $j \le q \le 2j$, and q is a prime power; omit $m = 1, q \in \{2, 3, 4\}$ and set an empty maximum to zero. The exact formulas for $N_{j,p}$ are in Appendix A.

Lemma 3.2. *The number of noncore p-atoms of support a in a forest of degree n is at most $nd_{a,p}$. If t is its number of transpositions divided by n, then $0 \le t \le 3/2$, the number of core 3-cycles is at most $2n$, and the number of noncore involution atoms of support four is at most $n(21/4 - 7t/2)$.*

Proof. A location supporting an a-atom has child size at most $a/2$. Every strict descendant has at most that many leaves, so cannot support an a-atom. These locations form an antichain with disjoint leaf sets. At a location of size qm its atom count divided by qm is bounded by (1); summing proves the first assertion.

A core block of size $b \le 4$ contains $\binom{b}{2} \le 3b/2$ transpositions and $2\binom{b}{3} \le 2b$ three-cycles. Summing over its blocks gives both core bounds. The possible noncore support-four locations have triples (leaves, transpositions, atoms)

$$(5, 0, 5), \quad (8, 0, 42), \quad (2q, q, q(q-1)) \ (q = 2, 3, 4).$$

These are respectively $A(5)$, $A(8)$, and $S_2 \wr S_q$. For $jm = 4$, either $m = 1, j = 4$ or $m = 2, j = 2$. In the first case $4 \le q \le 8$. The bottom symmetric case $q = 4$ contributes core cycles. Degree 5 contributes its five affine reflections; degree 8 contributes its 42 support-four involutions. In degree 7, an involution fixes one point and moves six, so contributes nothing here. In the second case the child group is S_2 and $2 \le q \le 4$, giving $S_2 \wr S_q$. The top transposition has $\binom{q}{2}$ choices and its two sections have two choices satisfying their product constraint, giving $q(q-1)$ atoms. Each last entry is at most $\frac{7}{2}(\frac{3}{2}\,\text{leaves} - \text{transpositions})$. The locations are disjoint, and every remaining leaf contributes nonnegative slack to this expression. Addition gives the claim. □

4. Separating the cores

Let M, N be affine forests of degree $n \ge 128$, and choose a uniform random relabelling $x \in S_n$. Let E be the event that a core block of M meets a relabelled core block of N in at most one point. This is equivalent to $T(M) \cap T(N)^x = 1$.

We use the canonical-event negative-dependency theorem of Lu and Székely [3, Theorem 1]: for uniform bijections, canonical events prescribing injections have a negative-dependency graph in which events with disjoint domains and disjoint ranges are nonadjacent. Thus an event's probability, conditioned on avoidance of any collection of its non-neighbors, is at most its unconditional probability. Their conflict graph may be enlarged to the domain-or-range-overlap graph used here.

Lemma 4.1. *The event E has positive probability. Let $0 \le s \le n$, and let A prescribe an injection from an s-element subset of Ω to Ω. Then*

$$\mathbb{P}(A \mid E) \le \frac{\min\{(5/4)^s, 2048\}}{(n)_s}. \tag{2}$$

Proof. A bad event prescribes a two-point injection between two pairs lying in core blocks. A core block of size $b \le 4$ contains $\binom{b}{2} \le 3b/2$ pairs, so each forest supplies at most $3n/2$ pairs. Each domain pair and range pair give two injections. There are therefore at most $2(3n/2)^2 = 9n^2/2$ bad events, each of probability $1/[n(n-1)]$. A given domain point lies in at most three core pairs; each has at most $3n/2$ range pairs and two injections. Thus each point occurs in at most $9n$ domains, and likewise in at most $9n$ ranges. A two-point event consequently has at most $4(9n) = 36n$ neighbors.

Put $q_n = (39/25)/[n(n-1)]$. At $n = 128$,

$$\frac{36nq_n}{1 - q_n} = \frac{179712}{406361} < \frac{21847}{49152} \le \log(39/25).$$

The last lower bound follows by retaining the first two terms of $\log u = 2\sum_{j\ge0}((u-1)/(u+1))^{2j+1}/(2j+1)$. The left side is $(1404/25)n/(n^2-n-39/25)$; its derivative has numerator $-(1404/25)(n^2+39/25)<0$. Since $-\log(1-q_n)\le q_n/(1-q_n)$, we obtain

$$\frac{1}{n(n-1)} < q_n(1-q_n)^{36n}.$$

Let B be a bad event and let $\mathcal{S}$ be a subfamily of other bad events. We prove by induction on $|\mathcal{S}|$ that their joint avoidance has positive probability and that

$$\mathbb{P}\left(B \,\middle|\, \bigcap_{C\in\mathcal{S}} C^c\right) \le q_n.$$

For nonempty $\mathcal{S}$, remove one event. The induction hypothesis bounds its conditional probability, given avoidance of the others, by $q_n<1$, so the joint avoidance has positive probability. Split $\mathcal{S}$ into the nonneighbors of B and its $k\le 36n$ neighbors. Conditional on avoiding the nonneighbors, negative dependency bounds the probability of B by $\mathbb{P}(B)$. Avoid the neighbors one at a time. Every conditional probability encountered has a smaller conditioning family, so the induction hypothesis bounds it by q_n. The probability of avoiding all k neighbors is at least $(1-q_n)^k$. Consequently

$$\mathbb{P}\left(B \,\middle|\, \bigcap_{C\in\mathcal{S}} C^c\right) \le \frac{1/[n(n-1)]}{(1-q_n)^k} \le q_n.$$

The empty conditioning family starts the induction. The same successive-avoidance product gives $\mathbb{P}(E)\ge(1-q_n)^{9n^2/2}>0$.

The event A has at most $18ns$ bad neighbors. Split the avoidance condition into its neighbors and nonneighbors. Negative dependency bounds the numerator by $\mathbb{P}(A)$, and the conditional induction just proved bounds the denominator below by $(1-q_n)^{18ns}$. For this application include A in the canonical-event family when invoking the negative-dependency theorem. Thus

$$\mathbb{P}(A\mid E)\le (n)_s^{-1}(1-q_n)^{-18ns}.$$

At 128, the per-point logarithm of the inflation is at most $89856/406361 < 488/2187 \le \log(5/4)$; again it decreases thereafter. Also

$$\log\frac{1}{\mathbb{P}(E)} \le \frac{(9/2)n^2q_n}{1-q_n} \le \frac{2875392}{406361} < \frac{616}{81} \le 11\log 2.$$

For the last estimate the degree-dependent expression is $(351/50)n^2/(n^2-n-39/25)$, with negative derivative proportional to $-n^2-(78/25)n$. The positive logarithm series proves the displayed lower bounds; in particular $\log 2\ge 56/81$. Bayes' inequality gives the alternative inflation 2048, proving (2). □

5. Connected involutions

Suppose a nonidentity involution belongs to $M\cap N^x$. Decompose it into atoms on each side. Form a bipartite multigraph with these atoms as vertices and the common transposition cycles as edges. A core vertex has degree one and a noncore vertex has degree at least two. On E no edge joins two core vertices. In a connected component, include the entire atom at each of its vertices. Its incident edges are exactly the transposition cycles in that atom. Thus the product of its edge cycles is both the product of its left atoms and the product of its right atoms. These products are equal nonidentity involutions and belong to the respective forests. It is enough to bound the probability of a connected witness.

For $i=0,\dots,29$, use the density interval $[i/20,(i+1)/20]$. Define

$$\alpha_i=(i+1)/20,\qquad \beta_{i,2}=21/4-7i/40,\qquad \beta_{i,k}=d_{2k,2}\quad(k\ge3).$$

These parameters bound the core density and the noncore degree-k atom densities whenever t belongs to the ith interval. For each integer $u \geq 0$, define

$$b_{i,u}^{(n)} = [y^u] \exp\left(\sum_{k \geq 2} \beta_{i,k} n^{1-k} y^k \right).$$

For $i, j \in \{0, \ldots, 29\}$, define $Z_{ij,0}^{(n)} = 1$ and, for integers $r \geq 1$,

$$Z_{ij,r}^{(n)} = \sum_{\substack{c,d \geq 0 \\ c+d \leq r}} \frac{\alpha_i^c \alpha_j^d}{c!d!} b_{i,r-c}^{(n)} b_{j,r-d}^{(n)} \frac{(r-c)!(r-d)!}{(r-c-d)!}. \tag{3}$$

Set $C_{ij,0}^{(n)} = 0$ and

$$C_{ij,r}^{(n)} = Z_{ij,r}^{(n)} - \frac{1}{r} \sum_{k=1}^{r-1} k C_{ij,k}^{(n)} Z_{ij,r-k}^{(n)}. \tag{4}$$

Lemma 5.1. *The conditional probability of a connected common involution with at most* 24 *transposition cycles is at most*

$$\sum_{r=2}^{24} C_{ij,r}^{(128)} \frac{2^r 128^{2r}}{(128)_{2r}} \min\{(5/4)^{2r}, 2048\}, \tag{5}$$

when the two core densities lie in intervals i, j.

Proof. Consider a model whose core vertices have weights $n\alpha_i$ and whose degree-k noncore vertices have weights $n\beta_{i,k}$, with distinguished ports. Allow repeated atom labels and ignore support compatibility. Divide by the factorial of the number of vertices of each type. For r ports on each side and c, d core vertices, first send the c left core ports injectively to the $r-d$ right noncore ports. Then send the d right core ports injectively to the $r-c$ left noncore ports, and match the remaining $r-c-d$ ports arbitrarily. If $c+d \leq r$, this gives

$$(r-d)_c (r-c)_d (r-c-d)! = \frac{(r-c)!(r-d)!}{(r-c-d)!}$$

allowed bijections. There are zero allowed bijections if $c+d > r$. For $a \geq 0$, the unnormalized noncore coefficient on the left is

$$[y^a] \exp\left(n \sum_{k \geq 2} \beta_{i,k} y^k \right) = n^a b_{i,a}^{(n)}.$$

Together with the core weights, the two sides contribute $n^{r-c} n^{r-d} n^{c+d} = n^{2r}$. Dividing by this factor gives (3). The core-exclusion matching count above also occurs in the public forest approach of [4]. To justify the connected coefficients, distribute each type's ordered vertices among components, and then forget the order. The multinomial factors cancel the factorials of equal-type vertices. Dividing by the factorial of the number of components gives the exponential formula

$$1 + \sum_{r \geq 1} Z_{ij,r}^{(n)} y^r = \exp\left(\sum_{r \geq 1} C_{ij,r}^{(n)} y^r \right),$$

The factorials normalize the atom vertices, and every port retains its position within its vertex. Differentiating gives $r Z_{ij,r}^{(n)} = \sum_{k=1}^{r} k C_{ij,k}^{(n)} Z_{ij,r-k}^{(n)}$, which is (4). Connected coefficients are sums of nonnegative weights. Actual distinct compatible atom choices are included in this model; deleting compatibility conditions and enlarging the type weights increases these connected counts.

A connected graph with r edges and V vertices contains a spanning tree with $V-1$ edges, so $V \le r+1$. Every normalized monomial is proportional to n^{V-2r}, hence decreases with n for $r \ge 2$. A one-edge graph is forbidden. Also $n^{2r}/(n)_{2r} = \prod_{a=0}^{2r-1}(1-a/n)^{-1}$ decreases for $n \ge 2r$, since each factor does. For each matched pair of cycle lists, there are 2^r choices of orientations; each specifies a map on $2r$ points. Apply Lemma 4.1 and evaluate at 128 to obtain (5). □

6. Uniform prime-order tails

For a prime p and a forest M on n points define

$$F_{p,M}(z) = \sum_{g \in M,\ g^p=1} z^{|\operatorname{supp}(g)|}.$$

The identity contributes the constant term one.

Lemma 6.1. *For every prime p, every nonempty full affine forest satisfies*

$$F_{2,M}(z)^2 + 3|M|z^{2n} \le_{\mathrm{c}} (1+3z^2)^n, \tag{6}$$

$$F_{p,M}(z)^p + 3^p|M|^{p-1}z^{pn} \le_{\mathrm{c}} (1+3^pz^p)^n. \tag{7}$$

Proof. For a primitive factor of degree q, Lemma 3.1 gives

$$F_{p,A(q)}(z) \le_{\mathrm{c}} (1+3^pz^p)^{\lfloor q/p \rfloor}.$$

Indeed its support-pk coefficient is at most $D^{pk} < 3^{pk}$. Taking pth powers proves (7) except for the correction at degree pq. At that degree the correction contributes $3^p|A(q)|^{p-1}$. Since $|A(q)| \le D^{q-1} < 3^{q-1}$,

$$\frac{3^p|A(q)|^{p-1}}{3^{pq}} \le 3^{1-q}.$$

If $p \mid q$, the other contribution is the pth power of the full-support coefficient, at most $|A(q)|^p$, so its normalized value is at most 3^{-p}. Their sum is at most $3^{-p}+3^{1-q} < 1$. If $p \nmid q$, the full-support coefficient is zero.

For (6), the 69 prime-power degrees $q < 256$ are checked by the explicit involution formulas in Appendix A: 7,251 integer coefficient comparisons. The complete loop is given in Appendix B. For $q \ge 256$, the order estimate improves to $|A(q)| \le D^{q/4}$. To check it, the logarithm of $q^{\log_2 q+1}$ at 256 is $72\log 2 < (64/3)\log 24$, and its derivative there is $17/256 < \log D/4$ and decreases. At exponent $2k$, the left coefficient without the correction is zero for $0 < k < q/4$, at most $2|A(q)|$ for $q/4 \le k < q/2$, and at most $|A(q)|^2$ for $q/2 \le k$. In the middle range,

$$2D^{q/4} \le 3^{q/4} \le \binom{q}{k} 3^k;$$

the first inequality follows from $D < 29/10$ and $(30/29)^{64} > 2$. In the next range $D^{q/2} < 3^{q/2} \le 3^k$. At $k = q$, include the correction using

$$|A(q)|^2 + 3|A(q)| < 3^{q/2} + 3^{q/4+1} < 3^q.$$

For propagation put $W = L \wr Q$, where L has degree m and $Q = A(q)$. An order-p element of Q with support j moves j/p cycles of child blocks. The sections on those cycles give $|L|^{j-j/p}$ choices, while the $q-j$ fixed children contribute $F_{p,L}(z)^{q-j}$. With u a formal variable, this gives

$$F_{p,W}(z) = \sum_{\substack{0 \le j \le q \\ p \mid j}} [u^j]F_{p,Q}(u)\,|L|^{j-j/p} z^{mj} F_{p,L}(z)^{q-j}.$$

Only multiples of p occur, and the expression can be written as

$$F_{p,W}(z) = F_{p,L}(z)^q F_{p,Q}\left(\frac{|L|^{(p-1)/p} z^m}{F_{p,L}(z)}\right).$$

Use the primitive strengthened inequality with correction coefficient c, where $c = 3$ for (6) and $c = 3^p$ for (7). After substitution and multiplication by $F_{p,L}(z)^{pq}$, every degree-pk monomial becomes a nonnegative scalar times $z^{pmk} F_{p,L}(z)^{p(q-k)}$ with $0 \le k \le q$. Thus coefficientwise comparison is preserved. The left side becomes $F_{p,W}(z)^p + c|W|^{p-1} z^{pmq}$, and the right side is

$$\left(F_{p,L}(z)^p + c|L|^{p-1} z^{pm}\right)^q \le_{\mathrm{c}} (1 + cz^p)^{mq}.$$

The one-point identity group satisfies both inequalities with equality. For a direct product of forests L, Q, $F_{p,L\times Q}(z) = F_{p,L}(z) F_{p,Q}(z)$. Multiply their strengthened inequalities. Then the two correction terms have product $c^2|L \times Q|^{p-1} z^{p(m+q)}$, which dominates the required correction because $c \ge 1$; all other cross terms have nonnegative coefficients. □

Lemma 6.2. *Conditional on E, common involutions with at least 25 cycles have total probability at most*

$$2048 \frac{18^{25} 25!}{50!} \frac{1}{1 - 9/51} < \frac{31}{10^6}.$$

The sum over all odd-prime-order rows with support at least 200 is less than 10^{-36}.

Proof. For $1 \le r \le \lfloor n/2 \rfloor$, let $a_r(M)$ count involutions with support $2r$. Then the diagonal term in (6) gives $a_r(M)^2 \le \binom{n}{2r} 3^{2r}$. Therefore $a_r(M) a_r(N)$ obeys the same bound. The conjugacy class of cycle type 2^r has size $(n)_{2r}/(2^r r!)$, so its unconditional union bound is at most $18^r r!/(2r)!$. Consecutive terms have ratio $9/(2r+1)$. Multiply their geometric tail by the upper bound 2048 for $1/\mathbb{P}(E)$.

For an odd prime p, $r \ge 1$, and $s = pr \le n$, let $a_{p,r}(M)$ count the order-p elements of M with support s. The diagonal term of (7) gives

$$a_{p,r}(M)^p \le \binom{n}{s} 3^{ps}, \qquad a_{p,r}(M) a_{p,r}(N) \le \binom{n}{s}^{2/p} 9^s \le \binom{n}{s} 9^s.$$

The last inequality uses $2/p \le 1$ and $\binom{n}{s} \ge 1$. The conjugacy class of cycle type p^r has size $(n)_s/(p^r r!)$. Multiplication by its reciprocal and cancellation of $\binom{n}{s}/(n)_s = 1/s!$ bounds this row by $p^r r! 9^s/s!$. For $s \ge 200$ and $r \le s/3$, the monotonicity of $\log t$ gives

$$\int_1^u \log t \, dt \le \log(u!) \le \int_1^u \log t \, dt + \log u \quad (u \ge 1).$$

Consequently $r! \le er(r/e)^r$ and $s! \ge (s/e)^s$. Using $pr = s$, $r \le s/3$, and $s/e > 1$ gives

$$\frac{p^r r! 9^s}{s!} \le \frac{es}{3} \left(\frac{9e^{2/3}}{s^{2/3}}\right)^s < s(3/5)^s.$$

Use $e < 3$, $e^2 < 8$, and $5832/200^2 < (3/5)^3$ for the strict inequality. There are at most s possible pairs (p, r) at a fixed support s. Differentiating the geometric series gives

$$\sum_{s \ge a} s^2 x^s = x^a \left(\frac{a^2}{1-x} + \frac{2ax}{(1-x)^2} + \frac{x(1+x)}{(1-x)^3}\right) \quad (0 < x < 1).$$

Consequently the conditional tail is at most

$$2048 \sum_{s \ge 200} s^2 (3/5)^s = 2048 (3/5)^{200}\, 101515 < 10^{-36}.$$ □

7. The bound at degree 128

For $r \geq 0$ define the normalized profile coefficients

$$A_{3,r}(n) = [y^r] \exp\left(2y + \sum_{k\geq 2} d_{3k,3} n^{1-k} y^k\right),$$

$$A_{p,r}(n) = [y^r] \exp\left(\sum_{k\geq 1} d_{pk,p} n^{1-k} y^k\right) \quad (p \geq 5 \text{ prime}).$$

The number of order-p elements with r cycles in a forest is at most $n^r A_{p,r}(n)$, by the disjoint-atom decomposition: for each atom type k, selecting m_k distinct labels gives at most $(nd_{pk,p})^{m_k}/m_k!$ choices. Dropping compatibility and multiplying the type series gives the displayed exponential. For $p = 3$, core cycles supply the coefficient $2n$ instead. Dividing the support-pr count by n^r gives precisely the normalized coefficients above. These coefficients decrease with n. The factor $n^{2r}/(n)_{pr}$ decreases for $n \geq pr$ as well, since it equals

$$n^{-(p-2)r} \prod_{j=0}^{pr-1} (1 - j/n)^{-1}.$$

An atom of support three has $j = 3$, $m = 1$, and $q \in \{3, 4, 5\}$. The group $A(5)$ has order 20, so contributes no element of order three; $A(3)$ and $A(4)$ contribute core cycles. Thus a common support-three element lies within a core block on each side and contradicts E. For every other odd-prime row with $pr < 200$ put $n_0 = \max\{128, pr\}$. Lemma 4.1 gives the bound

$$V_{p,r} = A_{p,r}(n_0)^2 \frac{p^r r! n_0^{2r}}{(p-1)(n_0)_{pr}} \min\{(5/4)^{pr}, 2048\}. \tag{8}$$

Here $r \geq 2$ for $p = 3$ and $r \geq 1$ for $p \geq 5$. The factor $p - 1$ is valid because each common cyclic group contributes all its $p - 1$ nonidentity elements of the same cycle type. A map conjugating two fixed elements on their supports permutes their r cycles and chooses the image of one point in each cycle. The remaining images are forced, giving $r!p^r$ choices.

Proposition 7.1. *With densities defined by* (1)*, the sum of the* 267 *values in* (8) *is less than* 0.012952*. For each of the* 465 *unordered density-interval pairs,* (5) *is less than* 0.984380*. Adding both tails from Lemma 6.2 gives a bound less than* 0.999*. For the interval pair* $(0, 0)$ *the complete bound is less than* 0.052168*.*

Proof. All quantities are rational. The supplementary programs implement (1), (3), (4), (5), and (8) using integers and `Fraction`. Appendix B specifies the recurrences and the full ranges. The exact sum of the odd-prime rows has decimal expansion $0.012951415109\ldots$. The maximum connected-involution bound occurs at $(i, j) = (0, 29)$ and is $0.984379245541\ldots$. The involution tail is

$$\frac{1383272158897143899136}{45276553871414302796734375}.$$

The maximum complete bound and the $(0, 0)$ bound are respectively

$$0.997361212272\ldots, \qquad 0.052167695309\ldots.$$

The comparisons in the assertion are performed before decimal conversion. □

Theorem 7.2. *The assertion $Q(n)$ holds for every $n \geq 128$.*

Proof. Enclose the two soluble subgroups in affine forests. If their intersection after conjugation is nonidentity, it contains an element of prime order. Conditional on E, a common involution contains a connected witness; Lemma 5.1 bounds its first 24 rows, and Lemma 6.2 bounds its tail. Formula (8) and the odd-prime tail cover all other prime-order witnesses.

Proposition 7.1 makes their total conditional probability less than one. Since $\mathbb{P}(E) > 0$, some x separates the two forests.

If $m \in M$ is odd, then $M \cap N^{xm} = (M \cap N^x)^m = 1$. If $h \in N$ is odd, then $N^{hx} = N^x$. Thus either odd forest provides successful conjugators of both signs. If both forests are all even, their transposition cores are trivial, so E is the whole space. Their actual densities are zero, and interval pair $(0, 0)$ gives bad probability less than $1/2$. More than half of S_n consists of successful conjugators, and hence both sign classes contain one. Finally compose with the two original relabellings, choosing the sign that compensates for them. □

8. Finite degrees and graph certificates

A finite certificate consists of two envelope indices, a required sign, and a concrete permutation of that sign. Its acceptance test computes the subgroup intersection.

8.1. **Complete lists of envelopes.** For $n \leq 39$ enumerate all words of degree at most n without adjacent $(2, 2)$, and then all sets of distinct words whose degrees sum to n. This is a complete cover by Lemma 2.1: replace $A(2) \wr A(2)$ by $A(4)$ and merge equal word components $W(w) \times W(w)$ into $W(w) \wr S_2$. Both replacements enlarge groups and preserve degree. Each merge decreases the component count, and each adjacent $(2, 2)$ replacement decreases the total number of word entries. Iteration terminates because neither operation increases the component count and, between merges, the total word length decreases.

For $23 \leq n \leq 63$, further prune by the replacements

$$W(w) \times (W(w) \wr S_2) \leq W(w) \wr S_3, \qquad W(w) \times (W(w) \wr S_3) \leq W(w) \wr S_4.$$

They are used for literally identical prefixes w, before replacing adjacent $(2, 2)$. Iteration again decreases the component count. Thus every initial forest lies in a terminal pruned envelope. The numbers of envelopes at degrees 21 through 39 are

$$255, 315, 231, 281, 352, 424, 519, 624, 765, 927, 1123,$$
$$1347, 1632, 1950, 2349, 2800, 3362, 3996, 4775.$$

The first two degrees use the unpruned list. From degree 64 onward, all multisets of normalized words with a residual degree pattern are enumerated, including repeated words.

If k envelopes are explicitly tested and e of them are all even, the witness requirement is exactly

$$\frac{k(k+1)}{2} + \frac{e(e+1)}{2}. \tag{9}$$

There is one witness for each unordered pair, including the diagonal, and a second sign for each all-even pair. An odd element of either envelope changes the sign of any successful conjugator. If $H^a \leq M$ and $K^b \leq N$, a separating x for M, N gives bxa^{-1} for H, K. The sign is $\operatorname{sgn}(b) \operatorname{sgn}(x) \operatorname{sgn}(a)$, so the prescribed sign of x compensates for the relabellings.

8.2. **Sound graph acceptance.** Encode the word trees with distinct colors for their direct-factor roots. Leaves are the original n points and share a dedicated color. At a node of odd characteristic and degree greater than four, add, for each unordered distinct pair u, v, a midpoint gadget identifying $(u + v)/2$: a relation vertex joins the parent and the two endpoints, and a differently colored port joins it to the midpoint. At a characteristic-two node of degree at least eight, add a relation vertex for each four-element subset with vector sum zero, joined to its parent and four children. Degrees $2, 3, 4$ require only the tree because their natural affine group is symmetric.

For degrees 64 through 127, higher-dimensional affine nodes instead use incidence with all affine hyperplanes. Their normals are normalized by making the first nonzero coordinate one; a hyperplane $a \cdot v = b$ contributes a relation vertex joined to its parent and its incident children. Dimension-one nodes retain midpoint gadgets. Every affine map preserves the

relevant relations, so every envelope element extends to a color-preserving graph automorphism. The actual permutation generators are checked against the exact coordinates and graph edges.

To test $M \cap N^x$, take disjoint copies of the internal vertices, separate their colors by side, and identify leaves after moving the second leaf i to i^x. Every common permutation extends on both sides, and the extensions agree on the leaves. They therefore combine to an automorphism of the glued graph. If the computed exact automorphism orbits of all leaves are singletons, the intersection is trivial.

8.3. **The finite induction.** For degrees 21 through 39, every envelope pair is explicitly checked. At degrees 40 through 63, every soluble subgroup contained in an envelope with an orbit of size $b \le \lceil n/4 \rceil$ preserves that set. Apply Lemma 2.3(1) to this actual soluble subgroup and an arbitrary soluble partner, using the previously established $Q(n-b)$. The remaining envelopes have at most three orbits, and all their unordered pairs are checked.

For $64 \le n \le 127$, first remove envelopes with such a small orbit. If there are three remaining orbits, each has at least 17 points; some orbit has at least 21, and its complement has at least 34. Apply Lemma 2.3(2) to the soluble subgroup inside the envelope. With two orbits, apply that lemma whenever the smaller orbit has size at least 21. Thus the only residual degree patterns are

$$(n), \qquad (b, n-b) \quad \text{with } \lceil n/4 \rceil < b \le 20.$$

For $n \ge 77$ only the first pattern remains. Enumerating all normalized word combinations of these degrees gives 744 residual envelopes in degrees 64 through 127, with 14,649 unordered pairs and 14,711 witnesses. Every lifting dependency decreases the degree and remains at least 21.

Proposition 8.1. *The finite certificates establish $Q(n)$ for every $21 \le n \le 127$.*

Proof. The complete pair and sign checks, partition checks, and exact intersection checks in the supplementary archive give the following totals:

Degrees	Unordered pairs	Sign witnesses
21–26	301,055	301,061
27–39	37,550,204	37,550,224
40–63	1,106,520	1,106,590
64–127	14,649	14,711
Total	38,972,428	38,972,586

Degrees 21 through 26 use exact GAP intersections [6]. The graph witnesses for all 101 degrees 27 through 127 have complete replay records with the official nauty/Traces release 2.9.3 [5]: 38,671,525 queries, all accepted by the singleton-leaf-orbit criterion. The indexing checks enforce (9), concrete permutation validity, and sign. The complete finite degree-dependency graph contains 5,086 strictly decreasing dependencies. The preceding cover and residual classification, followed by induction on n, proves the assertion. □

Proof of Theorem 1.1. Use Proposition 8.1 for $21 \le n \le 127$ and Theorem 7.2 for $n \ge 128$. For $H, K \le A_n$, choose the positive sign. Each ambient group contains a nonidentity soluble cyclic subgroup generated by a 3-cycle, so a one-entry tuple need not be regular. Hence both soluble regularity numbers are exactly two. □

Appendix A. Exact affine counts

For an integer $d \geq 0$ and a prime power ℓ, define

$$G(d,\ell) = \prod_{i=0}^{d-1} (\ell^d - \ell^i) = |\operatorname{GL}(d,\ell)|, \qquad G(0,\ell) = 1.$$

Here $\operatorname{GL}(d,\ell)$ acts over the field of order ℓ. For each prime p, initialize all support counts $N_{a,p}(A(\ell^d))$ to zero and add the following contributions. In these affine counts ℓ is prime and $d \geq 1$.

If $p \neq \ell$, let f be the multiplicative order of ℓ modulo p and $h = (p-1)/f$. For every tuple of nonnegative integers $m_0, \ldots, m_h$ with

$$d = m_0 + f \sum_{i=1}^{h} m_i, \qquad \sum_{i=1}^{h} m_i > 0,$$

add

$$\frac{G(d,\ell)\ell^{d-m_0}}{G(m_0,\ell)\prod_{i=1}^{h} G(m_i,\ell^f)}$$

to $N_{\ell^d-\ell^{m_0},p}(A(\ell^d))$. Indeed, the derivative pX^{p-1} is relatively prime to $X^p - 1$, so an order-p matrix is semisimple. In an algebraic closure of $\mathbb{F}_\ell$, Frobenius acts on nonidentity pth roots by $\zeta \mapsto \zeta^\ell$; its orbits have length f. Thus $X^p - 1$ has the factor $X - 1$ and h nontrivial irreducible factors of degree f. On their multiplicity spaces the commuting invertible maps form $\operatorname{GL}(m_0,\ell) \times \prod_{i=1}^{h} \operatorname{GL}(m_i,\ell^f)$, where the latter factors act over the degree-f extension of $\mathbb{F}_\ell$. This gives the displayed linear conjugacy-class denominator. For a linear map T of this type, $I + T + \cdots + T^{p-1}$ is multiplication by p on its fixed space and zero on the other summands. Its kernel is $\operatorname{im}(T - I)$ of dimension $d - m_0$. These are precisely the translation vectors giving affine pth power one. Since $T \neq I$, each resulting affine map has exact order p and has ℓ^{m_0} fixed points.

If $p = \ell$, let λ range over partitions of d with parts at most p. For $1 \leq j \leq p$, let m_j be the multiplicity of the part j, zero when that part is absent. Put $b = \sum_{j=1}^{p} m_j$, and define the column lengths $\lambda'_i = \sum_{j=i}^{p} m_j$ for $1 \leq i \leq p$. The centralizer order of a nilpotent matrix of this type is

$$p^{\sum_i (\lambda'_i)^2 - \sum_j m_j^2} \prod_j G(m_j, p).$$

Write $V = \bigoplus_j (\mathbb{F}_p[t]/t^j)^{m_j}$ for the underlying vector space, with t acting as the nilpotent matrix. A module homomorphism from $\mathbb{F}_p[t]/t^i$ to $\mathbb{F}_p[t]/t^j$ is determined by the image of 1, which must be killed by t^i. This gives dimension $\min(i,j)$, so the total commuting-algebra dimension is

$$\sum_{i,j} m_i m_j \min(i,j) = \sum_i (\lambda'_i)^2.$$

For each block length j, take the constant coefficients of the maps between the m_j summands of that length. This gives a surjective algebra homomorphism onto $\prod_j \operatorname{Mat}_{m_j}(\mathbb{F}_p)$: composition through a different block length has zero constant coefficient, since one direction is divisible by a positive power of t. On every quotient $t^h V/t^{h+1}V$, with $0 \leq h < d$, order the summands by block length. The induced matrix is block triangular, with diagonal blocks equal to these constant-coefficient matrices for $j > h$; a map from a shorter block to a longer block has zero constant coefficient. A commuting endomorphism is therefore invertible precisely when all these diagonal matrices are invertible. Indeed, invertibility on all the successive quotients of a finite filtration implies invertibility on the whole space, and invertibility on the whole space implies it on the quotients. The kernel of the homomorphism has dimension $\sum_i (\lambda'_i)^2 - \sum_j m_j^2$, so each image has $p^{\sum_i (\lambda'_i)^2 - \sum_j m_j^2}$ lifts. Multiplying by the orders of the general linear factors gives the stated centralizer. Divide $G(d,p)$ by

this centralizer to obtain the linear class size. Per linear element add p^{d-b} affine maps to support $p^d - p^b$ and $p^{d-m_p} - p^{d-b}$ maps to full support p^d, omitting the identity. For $T = I + U$, the affine pth power is $(I, (I + T + \cdots + T^{p-1})v)$ and $I + T + \cdots + T^{p-1} = U^{p-1}$ in characteristic p. Thus the condition is $U^{p-1}v = 0$; its kernel has dimension $d - m_p$, while $\operatorname{im} U$ has dimension $d - b$ and lies in that kernel because $U^p = 0$. The equation $Uw = -v$ has a solution exactly when $v \in \operatorname{im} U$, in which case it has p^b solutions. This gives both affine support contributions, including translations for the zero nilpotent matrix.

For involutions there is a second formula. In odd characteristic, for each $1 \le r \le d$, add

$$\frac{G(d,\ell)\ell^r}{G(r,\ell)G(d-r,\ell)}$$

to support $\ell^d - \ell^{d-r}$, by the negative-eigenspace decomposition. In characteristic two, first add $2^d - 1$ translations of full support. For $1 \le r \le \lfloor d/2 \rfloor$, the number of square-zero matrices of rank r is

$$\begin{bmatrix} d \\ r \end{bmatrix}_2 \begin{bmatrix} d-r \\ r \end{bmatrix}_2 G(r,2).$$

Choose the image, an r-space, in $\begin{bmatrix} d \\ r \end{bmatrix}_2$ ways. The kernel is a $(d-r)$-space containing it; in the quotient by the image there are $\begin{bmatrix} d-r \\ d-2r \end{bmatrix}_2 = \begin{bmatrix} d-r \\ r \end{bmatrix}_2$ choices. Finally choose an isomorphism from the quotient by the kernel to the image, in $G(r,2)$ ways. These choices determine a square-zero map of rank r and recover every such map uniquely. Per matrix add 2^r maps to support $2^d - 2^{d-r}$ and $2^{d-r} - 2^r$ to full support. These independent formulas agree on all primitive rows used in (6).

Appendix B. Finite arithmetic specification

The numerical part of the proof consists of three bounded calculations. First generate $d_{a,p}$ for $a \le 200$ by (1) and Appendix A. It suffices to enumerate $q \le 400$, $m \le 100$, and primes $p \le 200$; the conditions $a = jm \le 200$ and $q \le 2j$ prove exhaustiveness.

Second, for each prime power $q < 256$, form the involution distribution f_k indexed by half the support, including $f_0 = 1$. Check, for all $0 \le r \le q$,

$$\sum_{k=0}^{r} f_k f_{r-k} + \mathbf{1}_{r=q}\, 3|A(q)| \le \binom{q}{r} 3^r.$$

The 69 degrees give $7,251$ comparisons. Here $\mathbf{1}_{r=q}$ is one if $r = q$ and zero otherwise.

Third, the exponential coefficients needed for (3) and (8) use the recurrence

$$e_0 = 1, \qquad e_r = \frac{1}{r}\sum_{k=1}^{r} k u_k e_{r-k}, \quad \text{where} \quad \sum_{r \ge 0} e_r y^r = \exp\left(\sum_{k \ge 1} u_k y^k\right).$$

Run (3) and (4) through $r = 24$ for every $0 \le i \le j < 30$, and (8) for every odd prime p, $pr < 200$, excluding $(p, r) = (3, 1)$. Exact rational arithmetic then checks the comparisons of Proposition 7.1. The following is the main verification loop; the accompanying density generator and full probability verifier supply its input formulas and summands.

```
from fractions import Fraction as Q
from math import factorial, comb

def exp_coeff(u, R):
    e = [Q(1)] + [Q(0)] * R
    for r in range(1, R+1):
        e[r] = sum(k*u[k]*e[r-k]
                   for k in range(1, r+1)) / r
    return e

def connected(Z, R):
    C = [Q(0)] * (R+1)
```

```
    for r in range(1, R+1):
        C[r] = Z[r] - sum((k*C[k]*Z[r-k]
                           for k in range(1, r)), Q(0)) / r
        assert C[r] >= 0
    return C

# inv is the exact support-count dictionary from Appendix A.
def primitive_invariant(q, order, inv):
    f = [0]*(q+1)
    f[0] = 1
    for support, count in inv.items():
        assert support % 2 == 0
        f[support//2] = count
    for r in range(q+1):
        lhs = sum(f[k]*f[r-k] for k in range(r+1))
        if r == q:
            lhs += 3*order
        assert lhs <= comb(q,r)*3**r
```

The infinite tails are established in Lemma 6.2; the arithmetic loop has fixed finite limits independent of n.

Appendix C. Supplementary files and reproduction

The computational supplement is supplied as `Kourovka_21_3b_GitHub_ready.zip`, with root directory `kourovka-21-3b-certificates`. It contains the certificates and computation materials corresponding to this manuscript. Paths in this appendix are relative to that root. The supplement includes finite data, source code, stable graph software, and `MANIFEST.json` with file sizes and SHA-256 digests. The file `PROOF_CERTIFICATE_MAP.md` links every computational assertion to its inputs, verifier, and expected output. The manuscript is distributed separately.

For the degree-128 calculations use:

```
python prime_order_referee/prime_atom_densities.py
python prime_order_referee/verify_involution_invariant.py
python prime_order_referee/connected_128_certificate.py
```

The outputs are `prime_atom_densities_200.json`, `involution_polynomial_invariant_audit.json`, `connected_128_density_boxes.jsonl`, `connected_128_odd_prime_rows.json`, and `connected_128_summary.json` in the same directory. The probability verifier uses `Fraction` for all decisions; decimals are presentation only. An additional outward-interval implementation is documented in `REPRODUCE.md`. The command `python verify.py math` runs both implementations in a separate output directory.

The finite index is `CERTIFICATE_INDEX.json`. Each degree row identifies the explicit groups, concrete witness certificate, graph and permutation pool when applicable, and the complete pair and sign counts. The induction data are `computation/lifting/INDUCTION_CLOSED_THROUGH_63.json` and `computation/hyperplane_lifting/INDUCTION_CLOSED_THROUGH_127.json`. Full new intersection replays are recorded in `verification_records/graph/SUMMARY.json` and the six degree records in `verification_records/gap/`. The command `python verify.py coverage` independently checks all pair/sign slots against the actual generators; `python verify.py models` verifies the envelope partitions and affine-wreath membership of those generators.

The group files use one-based image lists: $[a_1, \dots, a_n]$ denotes the permutation $i \mapsto a_i$. Their arrays `ExplicitCoverWords`, `ExplicitGroupOrders`, and `ExplicitGenerators` give the word indices, product orders, and generators of each envelope in the same order. In a JSONL certificate each line gives degree `n`, envelope indices `i,j`, parity `parity`, and either a complete permutation `x` or a one-based `candidate` index in the permutation pool. An explicit `x` is used directly. For an indexed record, let u be its pool permutation and let

$\varepsilon \in \{1, -1\}$ be its requested parity. Decode the tested permutation by

$$x = \begin{cases} u, & \operatorname{sgn}(u) = \varepsilon, \\ u(1\ 2), & \operatorname{sgn}(u) \neq \varepsilon. \end{cases}$$

With our right-action convention, the second case interchanges the image values 1 and 2 in the list for u, and $\operatorname{sgn}(x) = \varepsilon$ in both cases. Let M_i, M_j denote the indexed envelopes. This decoded x determines the leaf identification in the glued graph and is the permutation used to test $M_i \cap M_j^x$. For example, the degree-40 record $(i, j, \varepsilon, \texttt{candidate}) = (90, 90, -1, 1)$ uses $x = u(1\ 2)$ because pool entry 1 is even. The coverage check requires exactly one positive-sign record for every unordered pair and exactly one negative-sign record when both envelopes are all even. For a pair having an odd envelope, the other sign follows by the multiplication argument in Section 7.

A graph-family file begins with `KOUROVKA_GRAPH_COVERS_V1`, then the degree and number of envelopes. Each envelope has a header giving its one-based index, vertex count, edge count, and odd-generator flag; the next line lists the vertex colors, followed by the edges as pairs of zero-based vertex indices. The first n vertices are the original points. The program `verify_graph_models.py` reconstructs these graphs from the envelope words and field coordinates and checks every actual generator on the resulting graph. The pool records give one-based permutation indices and image lists. A query file gives its record count followed by lines `i j parity candidate`; the graph engine decodes each indexed permutation by the parity rule above and checks the corresponding glued graph.

For $27 \leq n \leq 39$, the concrete witnesses are losslessly encoded in `computation/graph_n_certificates.kc4`. The decoder `computation/certificate_codec.py` reconstructs the original JSONL bytes or query stream and checks their SHA-256. For higher degrees the query and JSONL files are retained in the `lifting` or `hyperplane_lifting` directory. The command format for a new graph replay is

```
software_referee/runtime_293/graph_engine check \
    COVERS POOL QUERIES OUTPUT traces
```

Here `COVERS` is the colored graph family, `POOL` the concrete permutation pool, and `QUERIES` the exhaustive pair/sign list; the complete commands and reconstruction steps are in `REPRODUCE.md`. Each accepted query must report singleton orbits for all original point vertices. The supplied completion records include a fresh full replay of every finite witness. Hash checks establish file identity; executing the commands repeats the intersections.

References

[1] M. Anagnostopoulou-Merkouri and T. C. Burness, *On the regularity number of a finite group and other base-related invariants*, *J. London Math. Soc.* **110** (2024), no. 6, e70035, doi:10.1112/jlms.70035; author manuscript: https://seis.bristol.ac.uk/~tb13602/docs/regular_tuples_final.pdf.

[2] E. I. Khukhro and V. D. Mazurov (eds.), *The Kourovka Notebook: Unsolved Problems in Group Theory*, 21st edition, Problem 21.3, https://alglog.org/21tkt.pdf, accessed November 3, 2026.

[3] L. Lu and L. A. Székely, Using Lovász Local Lemma in the space of random injections, *Electron. J. Combin.* **14** (2007), Research Paper 63, doi:10.37236/981.

[4] Nilradical, *Soluble subgroups with trivially intersecting conjugates*, revised September 17, 2026, https://nilradical.ai/notes/kourovka-21-3/.

[5] B. D. McKay and A. Piperno, Practical graph isomorphism, II, *J. Symbolic Comput.* **60** (2014), 94–112.

[6] The GAP Group, *GAP—Groups, Algorithms, and Programming*, version 4.12.1, https://www.gap-system.org/.

[7] J. D. Dixon, The Fitting subgroup of a linear solvable group, *J. Austral. Math. Soc.* **7** (1967), 417–424, doi:10.1017/S1446788700004353.

[8] Á. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* **53** (1996), 243–255, doi:10.1112/jlms/53.2.243.

[9] A. A. Baykalov, Intersection of conjugate solvable subgroups in symmetric groups, *Algebra Logic* **56** (2017), 87–97, https://arxiv.org/abs/1701.04231.

[10] T. C. Burness, Base sizes for primitive groups with soluble stabilisers, *Algebra Number Theory* **15** (2021), 1755–1807, doi:10.2140/ant.2021.15.1755.
[11] V. I. Zenkov, On intersections of nilpotent subgroups in finite symmetric and alternating groups, *Proc. Steklov Inst. Math.* **285** (2014), suppl. 1, S203–S208, doi:10.1134/S0081543814050228.
[12] P. J. Cameron, *Some measures of finite groups related to permutation bases*, 2014, https://arxiv.org/abs/1408.0968.
[13] OSVerify contributors, *Rethlas-OSV*, software repository, 2026, https://github.com/OSVerify/Rethlas-OSV.

Zhili College, Tsinghua University, Beijing 100084, China
Email address: tangqy24@mails.tsinghua.edu.cn