Conjugate pairs with the full prime spectrum in finite groups

Charles O'Neill, Max Kirkby and Astra

25 November 2026

Abstract

For a finite group X let $\pi(X)$ be the set of primes dividing $|X|$. We prove that every finite group G contains two conjugate elements a and b with $\pi(\langle a, b\rangle) = \pi(G)$. This answers Question 17.125 of the Kourovka Notebook, a conjecture of Shumyatsky. Equivalently, every finite group in which no proper subgroup has the same prime spectrum is generated by two conjugate elements. Maslova and Revin proved this for groups whose maximal subgroups are all Hall subgroups. We study a minimal counterexample. A lifting argument through an abelian minimal normal subgroup shows that its soluble radical is trivial. For each minimal normal subgroup S^k we then lift a conjugate generating pair of the quotient by the socle so that the subgroup it generates has order divisible by $|S|$. When $k = 1$ this uses the theorem of Burness, Guralnick and Harper that a finite group whose proper quotients are all cyclic is generated by two conjugate elements. When $k \geq 2$ it uses a choice of automorphism labels along a spanning tree of the permutation action, together with the theorems of Gaschütz and of Lucchini and Menegazzo. The proof depends on the classification of finite simple groups. We have also checked in Lean 4 that the theorem follows from four of the cited published results.

2020 Mathematics Subject Classification. 20D60; 20F05, 20D06, 20E22
Keywords. prime spectrum, conjugate elements, generation of finite groups, Kourovka Notebook, minimal normal subgroups, wreath products

AI use and author contributions

The argument in this paper was developed by Astra (GPT-6.2 Astra, OpenAI) from Charles O'Neill's instructions. The manuscript was prepared from the project's research records with Claude (Anthropic). The paper contains no computations.

Charles O'Neill proposed the problem and asked for it to be answered. Charles O'Neill has checked the arguments and takes full responsibility for the correctness of the results.

1 Introduction

For a finite group X write $\pi(X)$ for the set of prime divisors of $|X|$, the *prime spectrum* of X. Shumyatsky conjectured that every finite group G contains a pair of conjugate elements a, b with $\pi(\langle a, b\rangle) = \pi(G)$. The conjecture appears as Question 17.125 in the Kourovka Notebook [5]; see [10].

Following Maslova and Revin, call a finite group P *prime-spectrum minimal* if $\pi(U) \neq \pi(P)$ for every proper subgroup $U < P$. Every finite group contains a prime-spectrum-minimal subgroup with the same prime spectrum, namely a subgroup of least order with that spectrum, and a pair of elements of a prime-spectrum-minimal group whose subgroup has the full spectrum must generate the group (Lemma 3). So Shumyatsky's conjecture is equivalent to the statement that every prime-spectrum-minimal group is generated by two conjugate elements. Maslova and Revin [10] proved this for groups all of whose maximal subgroups are Hall subgroups, and Maslova [8] proved it for prime-spectrum-minimal groups whose nonabelian composition factors all lie in $\{\mathrm{PSL}_2(7), \mathrm{PSL}_2(11), \mathrm{PSL}_5(2)\}$. We prove the conjecture in general.

Theorem 1. *Every finite group G contains two conjugate elements a and b with $\pi(\langle a, b\rangle) = \pi(G)$.*

Corollary 2. *Every prime-spectrum-minimal finite group is generated by two conjugate elements.*

Outline. By Lemma 3 it suffices to prove Corollary 2, and we consider a counterexample G of least order. Prime-spectrum minimality passes to quotients, so every proper quotient of G is generated by two conjugate elements. Section 3 shows that the soluble radical of G is trivial: lifting a conjugate generating pair through an abelian minimal normal subgroup N either generates G or produces a complement to N, and in the second case the pair can be modified so that it generates G. Then the socle M of G is a direct product of minimal normal subgroups $N_i \cong S_i^{k_i}$ with S_i nonabelian simple. We fix a conjugate generating pair of G/M and choose its lifts block by block. Since G is prime-spectrum minimal, it is enough that the subgroup generated by the lifts has order divisible by $|G/M|$ and by every $|S_i|$; we never need to show directly that it is all of G.

For a block with $k_i = 1$ (Section 5) the image of G in $\mathrm{Aut}(S_i)$ is an almost simple prime-spectrum-minimal group. Its outer part has order prime to $|S_i|$ and is therefore cyclic, so every proper quotient is cyclic and the theorem of

Burness, Guralnick and Harper [1] gives a conjugate generating pair, which we adjust to have the prescribed images. For a block with $k_i \geq 2$ (Section 6) we work in $\mathrm{Aut}(S^k) = \mathrm{Aut}(S) \wr \mathrm{Sym}(k)$. The equation $y = gxg^{-1}$ can be solved for g after the labels of x and of all but one edge on each cycle of y have been chosen freely. Two of the free labels lie off a spanning tree of the permutation action, so the automorphisms of the first factor induced by two closed walks can be prescribed independently within their cosets of $\mathrm{Inn}(S)$. The lifting lemma of Gaschütz [2], together with the theorem of Lucchini and Menegazzo [7], lets us choose these two automorphisms to generate a group containing $\mathrm{Inn}(S)$. Section 7 assembles the blocks.

The proof uses the classification of finite simple groups through Schreier's conjecture, the theorem on coprime automorphisms of simple groups [11, Theorem 5.1] and the results of [1]. It contains no computations. Section 8 describes a Lean 4 proof that Theorem 1 follows from four of the published results we cite.

Notation. All groups are finite. For elements g, x of a group we write gxg^{-1} for the conjugate of x by g, and $\langle X \rangle$ for the subgroup generated by X. We write $|x|$ for the order of x, $C_X(Y)$ for a centralizer, $d(X)$ for the least number of generators of X, and $R(X)$ for the soluble radical of X, its largest soluble normal subgroup.

2 Preliminaries

2.1 Prime-spectrum-minimal groups

Lemma 3. *1. Let F be a finite group and let $P \leq F$ be a subgroup of least order with $\pi(P) = \pi(F)$. Then P is prime-spectrum minimal.*

2. If P is prime-spectrum minimal and $a, b \in P$ satisfy $\pi(\langle a, b \rangle) = \pi(P)$, then $\langle a, b \rangle = P$.

3. If P is prime-spectrum minimal and $K \lhd P$, then P/K is prime-spectrum minimal.

In particular, Theorem 1 is equivalent to Corollary 2.

Proof. (a) A proper subgroup $U < P$ with $\pi(U) = \pi(P) = \pi(F)$ would have smaller order than P.

(b) This is the definition, applied to $U = \langle a, b \rangle$.

(c) Let $K \leq U \leq P$ with $\pi(U/K) = \pi(P/K)$. Then

$$\pi(U) = \pi(K) \cup \pi(U/K) = \pi(K) \cup \pi(P/K) = \pi(P),$$

so $U = P$ and $U/K = P/K$.

For the last assertion, suppose Corollary 2 holds and let F be finite. Choose P as in (a). Then $P = \langle a, gag^{-1}\rangle$ for some $a, g \in P$, and a and gag^{-1} are conjugate in F with $\pi(\langle a, gag^{-1}\rangle) = \pi(P) = \pi(F)$. Conversely, if Theorem 1 holds and P is prime-spectrum minimal, it gives $a, g \in P$ with $\pi(\langle a, gag^{-1}\rangle) = \pi(P)$, and $\langle a, gag^{-1}\rangle = P$ by (b). □

2.2 Results from the literature

We use the following facts.

Theorem 4 (Schur–Zassenhaus; see [4, Chapter 3])**.** *Let N be a normal subgroup of G with $\gcd(|N|, |G/N|) = 1$. Then N has a complement in G. If N or G/N is soluble, all complements of N are conjugate in G.*

Theorem 5 (Schreier's conjecture; see [3])**.** *If S is a nonabelian finite simple group, then $\mathrm{Out}(S)$ is soluble.*

Theorem 6 ([11, Theorem 5.1])**.** *Let S be a nonabelian simple group and let C be a group acting faithfully on S with $\gcd(|C|, |S|) = 1$. Then C is cyclic.*

Theorem 7 (Gaschütz [2])**.** *Let $N \lhd L$ and $r \geq d(L)$. For every r-tuple $(\bar{l}_1, \ldots, \bar{l}_r)$ generating L/N there are $l_j \in \bar{l}_j$ such that $L = \langle l_1, \ldots, l_r\rangle$.*

Theorem 8 (Lucchini–Menegazzo [7, Theorem 1.1])**.** *If L is a noncyclic finite group with a unique minimal normal subgroup N, then $d(L) = \max\{2, d(L/N)\}$.*

Theorem 9 (Burness–Guralnick–Harper [1, Corollary 4(ii)])**.** *Let L be a finite group such that every proper quotient of L is cyclic. If L is not isomorphic to $C_p \times C_p$ for a prime p, then L is generated by two conjugate elements.*

2.3 Almost simple groups

Let S be a nonabelian simple group and identify S with $I = \mathrm{Inn}(S) \lhd \mathrm{Aut}(S)$.

Lemma 10. *1. $C_{\mathrm{Aut}(S)}(I) = 1$.*

2. If $I \leq L \leq \mathrm{Aut}(S)$, then every nontrivial normal subgroup of L contains I. In particular I is the unique minimal normal subgroup of L.

Proof. (a) Let $\alpha \in \mathrm{Aut}(S)$ commute with every inner automorphism. For $s \in S$ write ι_s for conjugation by s; then $\alpha\iota_s\alpha^{-1} = \iota_{\alpha(s)}$, so $\iota_{\alpha(s)} = \iota_s$ and $\alpha(s)s^{-1}$ lies in the centre of S, which is trivial. Thus $\alpha = 1$.

(b) Let $1 \neq K \lhd L$. Then $K \cap I \lhd I$, so $K \cap I$ is 1 or I because $I \cong S$ is simple. If $K \cap I = 1$, then $[K, I] \leq K \cap I = 1$, so $K \leq C_{\mathrm{Aut}(S)}(I) = 1$ by (a), a contradiction. Hence $I \leq K$. □

3 The soluble radical of a minimal counterexample

Throughout the rest of the paper, G denotes a prime-spectrum-minimal group that is not generated by two conjugate elements and has least order among such groups. By Lemma 3(c) and the minimality of $|G|$, every proper quotient G/K with $K \neq 1$ is generated by two conjugate elements. Clearly $G \neq 1$.

Proposition 11. $R(G) = 1$.

Proof. Suppose $R(G) \neq 1$. The last nontrivial term of the derived series of $R(G)$ is abelian and characteristic in $R(G)$, hence normal in G. Let N be a minimal normal subgroup of G contained in it. Then N is abelian, and since its subgroup of elements of order dividing a prime $p \in \pi(N)$ is characteristic in N, the group N is an elementary abelian p-group.

By the minimality of $|G|$, there are $\bar{x}, \bar{g} \in G/N$ with $G/N = \langle \bar{x}, \bar{g}\bar{x}\bar{g}^{-1} \rangle$. Choose $x \in \bar{x}$ and $g \in \bar{g}$, put $y = gxg^{-1}$ and $H = \langle x, y \rangle$. Then $HN = G$, so $|G : H| = |N : H \cap N|$ is a power of p and $\pi(G) \setminus \pi(H) \subseteq \{p\}$. If $H = G$, then G is generated by the conjugate elements x, y, a contradiction. So $H < G$, and prime-spectrum minimality gives $\pi(H) \neq \pi(G)$, that is, $p \notin \pi(H)$. Hence $H \cap N = 1$, H is a complement to N, and $p \nmid |H| = |G/N|$. In particular N is a normal Hall subgroup of G. We obtain a contradiction in each of two cases.

Case 1: $C_N(x) \neq 1$. Choose $1 \neq v \in C_N(x)$. Since $x \in H$, the order of x is prime to p, and since x and v commute, $(xv)^{|x|} = v^{|x|} \neq 1$. Hence p divides $|xv|$. Put $H' = \langle xv,\ g(xv)g^{-1} \rangle$. As $v \in N$, the two generators of H' map to $\bar{x}$ and $\bar{g}\bar{x}\bar{g}^{-1}$, so $H'N = G$ and $|G/N|$ divides $|H'|$. Together with $p \in \pi(H')$ this gives $\pi(H') = \pi(G)$, hence $H' = G$ by prime-spectrum minimality. So G is generated by two conjugate elements, a contradiction.

Case 2: $C_N(x) = 1$. First, H is the only complement to N that contains x. Indeed, by Theorem 4 (with N abelian) every complement is conjugate to H in $G = NH$, hence equal to nHn^{-1} for some $n \in N$. If $x \in nHn^{-1}$, then $n^{-1}xn \in H$. The elements $n^{-1}xn$ and x of H have the same image in G/N, and $H \cap N = 1$, so $n^{-1}xn = x$. Thus $n \in C_N(x) = 1$ and $nHn^{-1} = H$.

Next, $C_N(y) = gC_N(x)g^{-1} = 1$ because $N \lhd G$. Choose $1 \neq n \in N$ and put $y' = nyn^{-1} = (ng)x(ng)^{-1}$. If $y' \in H$, then y' and y are elements of H with the same image in G/N, so $y' = y$ and $n \in C_N(y) = 1$, which is false. Hence $y' \notin H$. Let $K = \langle x, y' \rangle$. Its generators map to $\bar{x}$ and $\bar{g}\bar{x}\bar{g}^{-1}$, so $KN = G$. If $K < G$, the argument of the second paragraph, applied to K in place of H, shows that K is a complement to N. It contains x, so $K = H$

by the uniqueness just proved, which contradicts $y' \notin H$. Therefore $K = G$, and G is generated by the conjugate elements x and y', a contradiction. $\square$

Proposition 11 is in the spirit of the structural reductions of Maslova and Revin [10].

4 The socle and its permutation action

Let $M = \mathrm{Soc}(G)$ be the product of the minimal normal subgroups of G. Since $R(G) = 1$ by Proposition 11, every minimal normal subgroup of G is nonabelian. A nonabelian minimal normal subgroup is characteristically simple, so it is isomorphic to S^k for a nonabelian simple group S and some $k \geq 1$; its k simple direct factors are exactly its minimal normal subgroups, and they are permuted by conjugation.

Lemma 12. *Let $N_1, \dots, N_r$ be the minimal normal subgroups of G, with $N_i \cong S_i^{k_i}$.*

1. *$M = N_1 \times \cdots \times N_r$, and $|G| = |G/M| \prod_i |S_i|^{k_i}$.*
2. *For each i, G acts transitively by conjugation on the k_i simple factors of N_i, and M acts trivially on them.*

Proof. (a) For $i \neq j$ we have $[N_i, N_j] \leq N_i \cap N_j = 1$, so distinct minimal normal subgroups commute. Each N_i has trivial centre. If $N_i \cap \prod_{j \neq i} N_j \neq 1$, then this intersection, being normal in G, contains N_i by minimality, so N_i is centralized by itself and is abelian, a contradiction. Hence the product is direct.

(b) The product of the simple factors of N_i in one G-orbit is a nontrivial normal subgroup of G contained in N_i, so by minimality it is N_i and the orbit contains all the factors. An element of N_i normalizes each simple factor of N_i, since the factors are normal in N_i, and N_j centralizes N_i for $j \neq i$. So M fixes every factor. $\square$

Since $M \neq 1$, the quotient G/M is prime-spectrum minimal of smaller order, so there are $x_0, g_0 \in G$ with

$$G/M = \langle x_0 M,\ y_0 M \rangle, \qquad y_0 = g_0 x_0 g_0^{-1}. \tag{1}$$

We fix them for the rest of the paper. For each i let $\rho_i \colon G \to \mathrm{Aut}(N_i)$ be the conjugation action. Then $\rho_i(N_i) = \mathrm{Inn}(N_i)$ and $\rho_i(N_j) = 1$ for $j \neq i$, so $\rho_i(M) = \mathrm{Inn}(N_i)$.

Lemma 13. *Let $x \in x_0M$ and $g \in g_0M$, and put $y = gxg^{-1}$. Then $y \in y_0M$, and for each i the permutations induced by x and y on the simple factors of N_i generate a transitive group.*

Proof. As $M \lhd G$, $gxg^{-1} \in g_0x_0g_0^{-1}M$. By Lemma 12(b) the permutation action of G on the factors of N_i factors through G/M, which is generated by the images of x and y, and it is transitive. □

5 Blocks with one simple factor

Proposition 14. *Let S be a nonabelian simple group, identified with $\mathrm{Inn}(S)$, and let $S \le L \le \mathrm{Aut}(S)$ with L prime-spectrum minimal. Then L/S is cyclic. Moreover, if $c, d \in L/S$ and c generates L/S, then there are $a \in c$ and $h \in d$ with $L = \langle a, hah^{-1}\rangle$.*

Proof. By Theorem 5, $L/S \le \mathrm{Out}(S)$ is soluble. By Hall's theorem (see [4, Chapter 3]), L/S has a Hall subgroup K/S for the set of primes outside $\pi(S)$. Then

$$\pi(K) = \pi(S) \cup \pi(K/S) \supseteq \pi(S) \cup \big(\pi(L/S) \setminus \pi(S)\big) = \pi(L),$$

so $K = L$ by prime-spectrum minimality, and $\gcd(|L/S|, |S|) = 1$. By Theorem 4, S has a complement C in L. As a subgroup of $\mathrm{Aut}(S)$, the group C acts faithfully on S, and its order is prime to $|S|$. By Theorem 6, C is cyclic, and so is $L/S \cong C$.

By Lemma 10(b), every nontrivial normal subgroup of L contains S, so every proper quotient of L is a quotient of L/S and is cyclic. Since L contains the nonabelian group S, it is not isomorphic to $C_p \times C_p$. By Theorem 9 there are $a_1, g_1 \in L$ with $L = \langle a_1, b_1\rangle$, where $b_1 = g_1a_1g_1^{-1}$.

It remains to adjust the cosets. Since L/S is abelian, $b_1S = a_1S$, so a_1S generates L/S. Put $q = |L/S|$ and $n = |a_1|$. As c also generates the cyclic group L/S of order q, we have $c = (a_1S)^r$ for some integer r prime to q. By the Chinese remainder theorem choose an integer e with

$$e \equiv r \pmod{q}, \qquad e \equiv 1 \pmod{\ell} \text{ for every prime } \ell \mid n \text{ with } \ell \nmid q.$$

Every prime divisor of n either divides q, and then does not divide e because $\gcd(r, q) = 1$, or does not divide q, and then does not divide e by construction. Hence $\gcd(e, n) = 1$. (When $q = 1$ the first congruence is empty.) Put $a = a_1^e$. Then $\langle a\rangle = \langle a_1\rangle$ and $\langle b_1^e\rangle = \langle b_1\rangle$, because $|b_1| = n$ as well, so $L = \langle a, b_1^e\rangle$. Also $aS = (a_1S)^e = (a_1S)^r = c$ and $b_1^e = g_1ag_1^{-1}$.

Finally choose an integer j with $c^j = (g_1 S)^{-1} d$, which is possible because c generates L/S, and put $h = g_1 a^j$. Then $hS = (g_1 S) c^j = d$ and $hah^{-1} = g_1 a g_1^{-1} = b_1^e$. Hence $L = \langle a, hah^{-1} \rangle$ with $a \in c$ and $h \in d$. □

6 Blocks with several simple factors

In this section S is a nonabelian simple group, $k \geq 2$, $I = \mathrm{Inn}(S)$, and $W = \mathrm{Aut}(S^k)$. We write $B = \mathrm{Inn}(S^k) \lhd W$.

6.1 Coordinates

The minimal normal subgroups of S^k are its k simple factors, so every automorphism of S^k permutes them. Number the factors $1, \ldots, k$ and identify each with S. Then an element $w \in W$ is given by a permutation $\hat{w}$ of $\{1, \ldots, k\}$ and labels $w_1, \ldots, w_k \in \mathrm{Aut}(S)$: it maps the element s of factor i to the element $w_i(s)$ of factor $\hat{w}(i)$. Conversely every such pair defines an automorphism. If $u, v \in W$ and v is applied first, then

$$\widehat{uv} = \hat{u}\hat{v}, \qquad (uv)_i = u_{\hat{v}(i)}\, v_i \qquad (1 \leq i \leq k), \tag{2}$$

and consequently $(w^{-1})_{\hat{w}(i)} = w_i^{-1}$. The subgroup B consists of the elements with trivial permutation and all labels in I. By (2), for $w \in W$ the coset wB consists of all elements with permutation $\hat{w}$ and labels $z_i \in w_i I$, chosen independently for each i. The stabilizer W_1 of factor 1 maps to $\mathrm{Aut}(S)$ by $w \mapsto w_1$, and this is a homomorphism by (2).

For $w \in W$ and $m \geq 1$ we write $(w^m)_i = w_{\hat{w}^{m-1}(i)} \cdots w_{\hat{w}(i)} w_i$, which agrees with (2). All statements below about images in $\mathrm{Out}(S) = \mathrm{Aut}(S)/I$ use that I is normal in $\mathrm{Aut}(S)$.

6.2 Solving the conjugacy equation

Fix $\xi, \gamma \in W$ and put $\eta = \gamma \xi \gamma^{-1}$. Write $\sigma = \hat{\xi}$, $\tau = \hat{\eta}$ and $\beta = \hat{\gamma}$, so that $\tau = \beta \sigma \beta^{-1}$ and β maps each σ-cycle onto a τ-cycle of the same length, distinct σ-cycles to distinct τ-cycles.

Lemma 15. *In each τ-cycle Z choose a position $r_Z \in Z$, called reserved. Let $x \in \xi B$, and prescribe labels $y_j \in \eta_j I$ for every j that is not reserved. Then there are labels $y_{r_Z} \in \eta_{r_Z} I$ at the reserved positions and an element $g \in \gamma B$ such that the element y with permutation τ and labels (y_j) satisfies $y = gxg^{-1}$. In particular $y \in \eta B$.*

Proof. We look for g with permutation β. Since $\beta\sigma = \tau\beta$, the equation $gx = yg$ holds for the permutations, and by (2) it holds for the labels if and only if

$$g_{\sigma(i)} = y_{\beta(i)}\, g_i\, x_i^{-1} \qquad (1 \le i \le k). \tag{3}$$

Let O be a σ-cycle of length m, choose a base point $i \in O$, and put $g_i = \gamma_i$. Using (3) to define g successively at $\sigma(i), \dots, \sigma^{m-1}(i)$, induction and $\beta\sigma^t = \tau^t\beta$ give

$$g_{\sigma^t(i)} = (y^t)_{\beta(i)}\, g_i\, (x^t)_i^{-1} \qquad (0 \le t \le m),$$

where y^t is computed from the labels y_j and the permutation τ. The relation (3) at the last point $\sigma^{m-1}(i)$ of the cycle is consistent if and only if the value for $t = m$ equals g_i, that is,

$$(y^m)_{\beta(i)} = g_i\, (x^m)_i\, g_i^{-1}. \tag{4}$$

The left-hand side is the ordered product of the m labels on the τ-cycle $Z = \beta(O)$, starting at $\beta(i)$. The reserved label y_{r_Z} occurs in it exactly once, so (4) has the form $P\, y_{r_Z}\, Q = R$, where P and Q are products of prescribed labels and R is known. Set $y_{r_Z} = P^{-1}RQ^{-1}$. Doing this for every σ-cycle defines every reserved label exactly once, since each τ-cycle is $\beta(O)$ for exactly one O. With these labels, (3) defines g consistently on every σ-cycle, and then $gx = yg$.

It remains to check the cosets. The triple (ξ, γ, η) satisfies $\gamma\xi = \eta\gamma$, so it satisfies (3) and (4) with x, g, y replaced by ξ, γ, η. Modulo I, the prescribed labels of y, the labels of x and the base values $g_i = \gamma_i$ agree with those of η, ξ and γ. Hence modulo I the reserved label y_{r_Z} and η_{r_Z} solve the same equation $\bar{P}\,\bar{z}\,\bar{Q} = \bar{R}$ in $\mathrm{Out}(S)$, whose solution is unique, so $y_{r_Z} \in \eta_{r_Z} I$. Then (3) modulo I defines the same values for g and for γ along each cycle, so $g_j \in \gamma_j I$ for every j, that is, $g \in \gamma B$. Finally $y = gxg^{-1} \in \gamma\xi\gamma^{-1}B = \eta B$. $\square$

6.3 A spanning tree and two free labels

Let Γ be the directed multigraph on $\{1, \dots, k\}$ with an *x-edge* from i to $\sigma(i)$ and a *y-edge* from j to $\tau(j)$ for every i and j. Loops and parallel edges are kept. Trees and paths below are taken in the underlying undirected multigraph. Each τ-cycle of length ℓ gives a cycle in this multigraph: a loop if $\ell = 1$, two parallel edges if $\ell = 2$, and a cycle of length ℓ if $\ell \ge 3$. The same holds for σ-cycles.

Lemma 16. *Suppose that $\langle \sigma, \tau \rangle$ is transitive on $\{1, \dots, k\}$. Then there are a spanning tree T of Γ, a set $\mathcal{R}$ of y-edges containing exactly one edge of each τ-cycle and no edge of T, and two distinct edges e_1, e_2 of Γ that lie neither in T nor in $\mathcal{R}$.*

Proof. Transitivity means that Γ is connected. Let c be the number of σ-cycles. Delete one x-edge from each σ-cycle (the loop, for a fixed point). The remaining x-edges form a forest F whose components are the c cycles, each with an edge removed. Each deleted x-edge joins two vertices of one component of F, so a spanning tree $T \supseteq F$ of the connected multigraph Γ consists of F together with $c-1$ y-edges. Since a tree contains no cycle, every τ-cycle has an edge outside T; let $\mathcal{R}$ contain one such edge from each τ-cycle.

If $c \geq 2$, let e_1, e_2 be two of the deleted x-edges. If $c = 1$, then $T = F$ contains no y-edge, and τ, being conjugate to σ, is also a single k-cycle. Its k edges are not in T and exactly one of them is in $\mathcal{R}$, so since $k \geq 2$ at least one y-edge e_2 lies outside $T \cup \mathcal{R}$; let e_1 be the deleted x-edge. □

When $k = 2$ and $c = 1$, both σ and τ are the transposition, and the two y-edges $1 \to 2$ and $2 \to 1$ are distinct parallel edges; the lemma then takes one as the reserved edge and the other as e_2.

For $x, y \in W$ with $\hat{x} = \sigma$ and $\hat{y} = \tau$, call x_i the label of the x-edge from i and y_j the label of the y-edge from j. A walk in the undirected multigraph from v_0 to v_n that traverses edges $f_1, \dots, f_n$ determines a word $\omega = \lambda_n \cdots \lambda_1$, where λ_t is x or y if f_t is an x- or y-edge traversed forwards, and x^{-1} or y^{-1} if it is traversed backwards. By (2) the element $\omega(x, y)$ maps factor v_0 to factor v_n with label

$$\omega(x, y)_{v_0} = \mu_n \cdots \mu_1, \tag{5}$$

where μ_t is the label of f_t if f_t is traversed forwards and its inverse otherwise. Indeed $(x^{-1})_v = x^{-1}_{\sigma^{-1}(v)}$, which is the inverse of the label of the x-edge entering v, and similarly for y.

For an edge e from s to t, let ω_e be the word of the closed walk that goes from 1 to s along T, traverses e forwards, and returns from t to 1 along T. Then $\omega_e(x, y) \in W_1$, and by (5)

$$\omega_e(x, y)_1 = A_e \, z_e \, D_e, \tag{6}$$

where z_e is the label of e and A_e, D_e are products of labels of edges of T and their inverses. In particular, if $e \notin T$, then $\omega_e(x, y)_1$ depends only on the labels of T and on z_e.

6.4 The block lift

Proposition 17. *Let $\xi, \gamma \in W$, put $\eta = \gamma\xi\gamma^{-1}$, and suppose that $\langle \hat{\xi}, \hat{\eta} \rangle$ is transitive on $\{1, \dots, k\}$. Then there are $x \in \xi B$ and $g \in \gamma B$ such that, with*

$y = gxg^{-1}$, the order of $\langle x, y\rangle$ is divisible by $|S|$. More precisely, the image of $\langle x, y\rangle \cap W_1$ under $w \mapsto w_1$ contains I.

Proof. Choose T, $\mathcal{R}$, e_1 and e_2 by Lemma 16, and take the reserved positions of Lemma 15 to be the sources of the edges in $\mathcal{R}$. Give every x-edge and every y-edge outside $\mathcal{R}\cup\{e_1, e_2\}$ the label of ξ or η at its source. In particular all labels of T are now fixed. For $r = 1, 2$ let A_r, D_r be the products in (6) for e_r, and let ζ_r be the label of ξ or η on e_r. Let $\bar{l}_r \in \mathrm{Out}(S)$ be the image of $A_r\zeta_r D_r$. Since $I \lhd \mathrm{Aut}(S)$, the map $z \mapsto A_r z D_r$ is a bijection from $\zeta_r I$ onto the coset $\bar{l}_r$.

Let $E = \langle \bar{l}_1, \bar{l}_2\rangle \leq \mathrm{Out}(S)$ and let $L \leq \mathrm{Aut}(S)$ be its preimage, so that $I \leq L$ and $L/I = E$. By Lemma 10(b), I is the unique minimal normal subgroup of L, and L is not cyclic because it contains $I \cong S$. By Theorem 8, $d(L) = \max\{2, d(E)\} = 2$. By Theorem 7 there are $l_1 \in \bar{l}_1$ and $l_2 \in \bar{l}_2$ with $L = \langle l_1, l_2\rangle$. (This includes the cases where $\bar{l}_1 = \bar{l}_2$ or where one of them is trivial.) Give e_r the label $z_r = A_r^{-1} l_r D_r^{-1} \in \zeta_r I$, for $r = 1, 2$.

Now every x-label has been chosen, and lies in the corresponding coset of I, so this defines $x \in \xi B$. Every y-label except those on $\mathcal{R}$ has been chosen in the corresponding coset. By Lemma 15 there are labels on $\mathcal{R}$ and an element $g \in \gamma B$ with $y = gxg^{-1}$. The walks ω_{e_1} and ω_{e_2} use only edges of T and their own edge e_r, and none of these lies in $\mathcal{R}$. So by (6),

$$\omega_{e_r}(x, y)_1 = A_r z_r D_r = l_r \qquad (r = 1, 2).$$

The elements $\omega_{e_1}(x, y)$ and $\omega_{e_2}(x, y)$ lie in $\langle x, y\rangle \cap W_1$, and the homomorphism $w \mapsto w_1$ maps the subgroup they generate onto $\langle l_1, l_2\rangle = L \supseteq I$. Hence $|S| = |I|$ divides $|L|$, which divides $|\langle x, y\rangle \cap W_1|$ and therefore $|\langle x, y\rangle|$. □

7 Proof of the theorem

Proof of Theorem 1 and Corollary 2. By Lemma 3 it suffices to prove Corollary 2. Suppose it fails, and let G be a counterexample of least order, as in Section 3. Let $N_1, \ldots, N_r$, x_0, g_0, y_0 and ρ_i be as in Section 4. For each i we choose $a_i, h_i \in \mathrm{Aut}(N_i)$ with

$$\rho_i(x_0)^{-1} a_i,\ \rho_i(g_0)^{-1} h_i \in \mathrm{Inn}(N_i), \qquad |S_i| \text{ divides } \left|\langle a_i,\ h_i a_i h_i^{-1}\rangle\right|. \quad (7)$$

Blocks with $k_i = 1$. Then $N_i = S_i$ and $L_i = \rho_i(G)$ satisfies $\mathrm{Inn}(S_i) \leq L_i \leq \mathrm{Aut}(S_i)$. As a quotient of G, L_i is prime-spectrum minimal by Lemma 3(c). The composite map $G \to L_i \to L_i/\mathrm{Inn}(S_i)$ is surjective and kills M, because

$\rho_i(M) = \mathrm{Inn}(S_i)$. By Proposition 14 the group $L_i/\mathrm{Inn}(S_i)$ is cyclic, so the images of x_0 and $y_0 = g_0 x_0 g_0^{-1}$ in it coincide. By (1) these images generate it, so the image c of x_0 generates $L_i/\mathrm{Inn}(S_i)$. Let d be the image of g_0. Proposition 14 gives $a_i \in c$ and $h_i \in d$ with $\langle a_i, h_i a_i h_i^{-1}\rangle = L_i \supseteq \mathrm{Inn}(S_i)$, so (7) holds.

Blocks with $k_i \geq 2$. Identify N_i with $S_i^{k_i}$, so that $\mathrm{Aut}(N_i) = W$ and $\mathrm{Inn}(N_i) = B$ in the notation of Section 6. Put $\xi = \rho_i(x_0)$ and $\gamma = \rho_i(g_0)$, so that $\gamma\xi\gamma^{-1} = \rho_i(y_0)$. By Lemma 13 the permutations $\hat{\xi}$ and $\widehat{\rho_i(y_0)}$ generate a transitive group. Proposition 17 gives $a_i \in \xi B$ and $h_i \in \gamma B$ satisfying (7).

Assembly. Since $\rho_i(N_i) = \mathrm{Inn}(N_i)$, there are $u_i, v_i \in N_i$ with $\rho_i(u_i) = \rho_i(x_0)^{-1} a_i$ and $\rho_i(v_i) = \rho_i(g_0)^{-1} h_i$. Put

$$x = x_0\, u_1 \cdots u_r, \qquad g = g_0\, v_1 \cdots v_r, \qquad y = gxg^{-1}, \qquad H = \langle x, y\rangle.$$

Since $\rho_i(N_j) = 1$ for $j \neq i$, we get $\rho_i(x) = \rho_i(x_0)\rho_i(u_i) = a_i$ and $\rho_i(g) = h_i$, hence $\rho_i(y) = h_i a_i h_i^{-1}$ and $\rho_i(H) = \langle a_i, h_i a_i h_i^{-1}\rangle$. By (7), $|S_i|$ divides $|\rho_i(H)|$, which divides $|H|$. Also $x \in x_0 M$ and $y \in y_0 M$, so $HM = G$ by (1), and $|G/M| = |H/(H \cap M)|$ divides $|H|$. By Lemma 12(a),

$$\pi(G) = \pi(G/M) \cup \bigcup_{i=1}^{r} \pi(S_i) \subseteq \pi(H) \subseteq \pi(G).$$

So $\pi(H) = \pi(G)$, and $H = G$ by prime-spectrum minimality. Then G is generated by the conjugate elements x and y, which contradicts the choice of G. □

Remark. From each block the proof needs only that $|S_i|$ divides the order of the subgroup generated by the lifts. This is what allows the blocks with $k_i \geq 2$ to be handled by the label argument of Section 6, without determining the subgroup that the lifts generate. Prime-spectrum minimality then does the rest.

8 Formal verification in Lean

Theorem 1 has also been proved in the Lean 4 proof assistant [6] with the Mathlib library [9], from four of the published results of Section 2, which enter as explicit hypotheses. The development has about 2,000 lines, uses version 4.24.0 of Lean and the matching release of Mathlib, and is available at `https://github.com/charlieoneill11/maths-releases`.

Statements. The four hypotheses are the following statements, for every nonabelian finite simple group S and every finite group L:

1. $\mathrm{Out}(S)$ is soluble (Theorem 5);
2. a subgroup of $\mathrm{Aut}(S)$ whose order is prime to $|S|$ is cyclic (the case of Theorem 6 used in Proposition 14);
3. if L is nonabelian and every proper quotient of L is cyclic, then L is generated by two conjugate elements (Theorem 9);
4. for $\bar{u}, \bar{v} \in \mathrm{Out}(S)$, the preimage of $\langle \bar{u}, \bar{v} \rangle$ in $\mathrm{Aut}(S)$ is generated by two elements. This is Theorem 8 combined with Lemma 10, as in the proof of Proposition 17.

From these, Lean proves that every finite group G has elements x, g such that $\langle x, gxg^{-1} \rangle$ and G have the same prime divisors of their orders. This is Theorem 1 with $a = x$ and $b = gxg^{-1}$. The conclusion is also restated with the quantifiers written out, so that x and g are chosen before the prime. For soluble groups the same conclusion is proved with no hypotheses.

Proof. The development proves Gaschütz's lemma (Theorem 7) by counting generating tuples, the conjugacy of complements of an abelian normal Hall subgroup used in Proposition 11, and the part of Hall's theorem used in Proposition 14. The existence part of Theorem 4 is taken from Mathlib. The formal proof is organised slightly differently from Section 7. Instead of lifting through the whole socle, it inducts on the order of the group and lifts a conjugate generating pair through a single minimal normal subgroup N. If N is abelian it uses the argument of Proposition 11. Otherwise it uses Proposition 14 or Proposition 17, and prime-spectrum minimality finishes as in Section 7. The simultaneous choice of lifts made in Section 7 is proved as a separate lemma. In Lemma 15 the formalisation takes the base point of each cycle to be the point immediately after the reserved edge. It also keeps the two directed edges of a 2-cycle distinct, as in Lemma 16.

Trust. The main theorem, the soluble case and the two lifting steps of Proposition 17 and Section 7 depend only on the three standard axioms of Lean: propositional extensionality, the axiom of choice and the soundness of quotients. The development contains no unproved steps, declares no further axioms and uses no compiled evaluation. So the formal proof relies only on the Lean kernel and on the four inputs above. A proof in Lean without hypotheses would also need formal proofs of those inputs. The first three depend on the classification of finite simple groups.

References

[1] T. C. Burness, R. M. Guralnick and S. Harper, *The spread of a finite group*, Ann. of Math. (2) **193** (2021), no. 2, 619–687; arXiv:2006.01421.

[2] W. Gaschütz, *Zu einem von B. H. und H. Neumann gestellten Problem*, Math. Nachr. **14** (1955), 249–252.

[3] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups, Number 3*, Math. Surveys Monogr. **40.3**, Amer. Math. Soc., Providence, RI, 1998.

[4] I. M. Isaacs, *Finite Group Theory*, Grad. Stud. Math. **92**, Amer. Math. Soc., Providence, RI, 2008.

[5] E. I. Khukhro and V. D. Mazurov (eds.), *Unsolved Problems in Group Theory. The Kourovka Notebook*, Sobolev Institute of Mathematics, Novosibirsk; arXiv:1401.0300 (version 50, Question 17.125 on page 123).

[6] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635.

[7] A. Lucchini and F. Menegazzo, *Generators for finite groups with a unique minimal normal subgroup*, Rend. Sem. Mat. Univ. Padova **98** (1997), 173–191.

[8] N. V. Maslova, *On the finite prime spectrum minimal groups*, Trudy Inst. Mat. Mekh. UrO RAN **21** (2015), no. 3, 222–232; English transl. in Proc. Steklov Inst. Math. **295** (2016), suppl. 1, 109–119.

[9] 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, 367–381.

[10] N. V. Maslova and D. O. Revin, *Generation of a finite group with Hall maximal subgroups by a pair of conjugate elements*, Trudy Inst. Mat. Mekh. UrO RAN **19** (2013), no. 3, 199–206; English transl. in Proc. Steklov Inst. Math. **285** (2014), suppl. 1, S139–S145.

[11] B. Späth and C. Vallejo Rodríguez, *Brauer characters and coprime action*, J. Algebra **457** (2016), 276–311.