FINITE GROUPS SATISFYING THE INDEPENDENCE PROPERTY

SAUL D. FREEDMAN, ANDREA LUCCHINI, DANIELE NEMMI, AND COLVA M. RONEY-DOUGAL

Abstract. We say that a finite group G satisfies the *independence property* if, for every pair of distinct elements x and y of G, either $\{x, y\}$ is contained in a minimal generating set for G or one of x and y is a power of the other. We give a complete classification of the finite groups with this property, and in particular prove that every such group is supersoluble. A key ingredient of our proof is a theorem showing that all but three finite almost simple groups H contain an element s such that the maximal subgroups of H containing s, but not containing the socle of H, are pairwise non-conjugate.

1. Introduction

Let G be a finite group. A generating set X for G is said to be *minimal* if no proper subset of X generates G. Let $d(G)$ and $m(G)$ denote, respectively, the smallest and largest cardinality of a minimal generating set for G. A nice result in universal algebra, due to Tarski and known as the Tarski Irredundant Basis Theorem (see, for example, [10, Theorem 4.4]), implies that, for every positive integer k with $d(G) \leqslant k \leqslant m(G)$, the group G has a minimal generating set of cardinality k. However, minimal generating sets for finite groups are not well understood. In particular, while several results in the literature (e.g., [26, 42, 52]) yield good estimates for $d(G)$, very little is known about $m(G)$. An exhaustive investigation [12, 57] was carried out for the finite symmetric groups, proving that $m(\mathrm{S}_n) = n - 1$ for each n, and giving a complete description of the minimal generating sets of S_n having cardinality $n - 1$. The problem of determining $m(G)$ in general remains open, even for finite simple groups, though partial results for certain families of these groups are given in [58].

One natural related question is "which subsets of G lie in a minimal generating set?" For singletons, the answer is easy: an element belongs to some minimal generating set for G if and only if it is not contained in the Frattini subgroup of G. Therefore, the first meaningful question is "which pairs of distinct elements belong to a minimal generating set?" Similarly, we can ask "which pairs of distinct elements belong to a generating set of size $d(G)$?" A partial answer to the corresponding question about singletons is given in [1, §6], using [8, Theorem 1].

We will call two distinct elements x and y of G *independent* in G if there exists a minimal generating set X for G with $\{x, y\} \subseteq X$. Similarly, we will call

2010 *Mathematics Subject Classification.* 20D60 (primary); 20F16, 20E32 (secondary).
Key words and phrases. Generating sets, supersoluble groups, simple groups.

x and y *rank-independent* in G if there exists such an X with $|X| = d(G)$. An obvious obstruction to x and y being independent is that one of the two is a power of the other. We say that G satisfies the *independence property* if this is the unique obstruction, i.e., if two distinct elements x and y are independent whenever neither of x and y is a power of the other. Similarly, an obvious obstruction to x and y being rank-independent is that they generate a cyclic subgroup, i.e., that each of x and y is a power of some $z \in G$. We say that a non-cyclic finite group G satisfies the *rank-independence property* if $\{x, y\}$ extends to a generating set for G of size $d(G)$ whenever $\langle x, y\rangle$ is not cyclic.

Note that we can also formulate the independence and rank-independence properties in the context of certain graphs associated with G. Each graph defined here has vertex set G. In the *independence graph* of G, which was introduced and investigated in [41], two distinct vertices are adjacent if and only if they are independent, while in the *rank graph* of G, two distinct vertices are adjacent if and only if they are rank-independent. The *power graph* of G, where distinct vertices are adjacent if and only if one is a power of the other, was introduced by Kelarev and Quinn [37] and investigated by several authors (see for example [13, 14, 15, 16, 18]). Finally, the edges of the *enhanced power graph* of G are the pairs $\{x, y\}$ of distinct vertices such that $\langle x, y\rangle$ is cyclic. This graph was introduced to interpolate between the power graph and the well-known commuting graph, but has since been studied in its own right (see [17, 48, 59, 60]). The independence property of a group is equivalent to its independence graph being the complement of its power graph. Similarly, G satisfies the rank-independence property if and only if its rank graph is the complement of its enhanced power graph.

In this paper, we will give a complete classification of the finite groups G satisfying the independence property and those satisfying the rank-independence property. We will see in particular that in each case G is supersoluble.

The classification of finite groups with the rank-independence property is not particularly difficult (however, our proof relies on the classification of finite simple groups). The description depends on whether $d(G) = 2$ or $d(G) \geqslant 3$.

Theorem 1. *Let G be a finite group with $d(G) = 2$. Then G satisfies the rank-independence property if and only if one of the following occurs:*

(i) $G \cong C_p \times C_p$, *with p a prime;*
(ii) $G \cong Q_8$*; or*
(iii) $G \cong C_p \rtimes C_{q^m}$, *where p and q are distinct primes, m is an arbitrary positive integer, and the action of C_{q^m} on C_p has kernel $C_{q^{m-1}}$.*

Theorem 2. *Let G be a finite group with $d(G) \geqslant 3$. Then G satisfies the rank-independence property if and only if $G = P \rtimes C$, where P is an elementary abelian p-subgroup of G and C is a cyclic group of coprime order acting on P as scalar multiplication.*

In the above result, we permit $C = 1$, and more generally, $G = P \times C$.

In a very recent paper, Harper [32] introduced the notion of k-flexible groups, for each positive integer k. A finite group G is *k-flexible* if, for all $g_1, \ldots, g_k \in G$ such that $d(\langle g_1, \ldots, g_k\rangle) = k$, there exist $g_{k+1}, \ldots, g_{d(G)} \in G$ such that

$\langle g_1, \ldots, g_{d(G)} \rangle = G$. In particular, the notions of 2-flexible groups and groups with the rank-independence property coincide. Theorems 1 and 2 above correspond to a small correction of Lemma 2.7 and a slightly more precise statement of part of Theorem 2.14 in [32], respectively, and were proved independently.

The classification of the finite groups with the independence property is much more difficult. To prove that a group satisfying the independence property is supersoluble, we require several new tools that rely on classifications of the finite simple groups and their maximal subgroups, including the following key result. For an element s of a group G, we write $\mathcal{M}_G(s)$ to denote the set of maximal subgroups of G containing s.

Theorem 3. *Let S be a non-abelian finite simple group. Then there exist non-commuting elements $s, x \in S$ such that, for each almost simple group G with socle S, the intersection $\bigcap_{M \in \mathcal{M}_G(s)} M$ contains x.*

We shall prove Theorem 3 in Section 2 as a consequence of two stronger theorems, which may be of interest in their own right: Theorem 4 below, which deals with all but three choices for S, and Theorem 2.1, which addresses the remaining groups.

For an almost simple group G with socle S, we let $\mathcal{M}'_G(s)$ denote the set of maximal subgroups M of G with $s \in M$ and $S \not\leqslant M$. A *novelty maximal* of G is a maximal subgroup M such that $M \cap S$ is a proper non-maximal subgroup of S. We shall use ATLAS notation for the names of simple groups. For example, $\mathrm{O}_8^+(3)$ denotes the simple 8-dimensional orthogonal group of plus type defined over $\mathbb{F}_3$, while $\mathrm{GO}_8^+(3)$ is the corresponding general orthogonal group.

Theorem 4. *Let S be a non-abelian finite simple group, and if $S \cong \mathrm{O}_8^+(q)$, then suppose that $q \notin \{2, 3, 5\}$. Then S contains an element s such that:*

(i) *$N_S(\langle s \rangle) > C_S(s)$; and*

(ii) *for each almost simple group G with socle S, there is at most one novelty maximal in $\mathcal{M}'_G(s)$, and no two subgroups in $\mathcal{M}'_G(s)$ are G-conjugate.*

Even once we have proved that all finite groups satisfying the independence property are supersoluble, it is not straightforward to classify these groups. Indeed, the description of these groups is neither natural nor easy, as evidenced by the following statement. Throughout, we denote the Frattini subgroup of a group G by $\Phi(G)$.

Theorem 5. *A finite group G satisfies the independence property if and only if one of the following occurs:*

(i) *G is a cyclic group of prime power order;*

(ii) *G is the quaternion group Q_8 of order 8; or*

(iii) *$G \cong (V_1^{\delta_1} \times \cdots \times V_r^{\delta_r}) \rtimes H$, where H is abelian, $\delta_1, \ldots, \delta_r$ are positive integers for some $r \geqslant 0$, $V_1, \ldots, V_r$ are irreducible H-modules on which H acts non-trivially, and the following statements hold. Here, for $h \in H$, we write $I_h := \{i \in \{1, \ldots, r\} \mid h \in C_H(V_i)\}$.*

  (a) If $\delta_i = 1$, then $|H/C_H(V_i)|$ is prime.

  (b) If $|V_i| = |V_j|$, then $i = j$.

  (c) $(|H|, |V_i|) = 1$ for all $i \in \{1, \ldots, r\}$.

(d) *For all $x, y \in H$, if $y \in \langle x \rangle \Phi(H)$ and $I_x \subseteq I_y$, then one of x and y is a power of the other. If in addition $I_x \neq \varnothing$, then $y \in \langle x \rangle$.*

In part (iii), notice that if G is abelian, then $G = H$ and $r = 0$, hence (d) implies that $\Phi(H) = 1$.

The structure of the paper is as follows. Theorems 3 and 4 are proved in Section 2. In Section 3, we prove that a finite group G satisfying the independence property is supersoluble. The structure of the finite supersoluble groups satisfying the independence property is investigated in Section 4, where Theorem 5 is proved. Finally, finite groups with the rank-independence property are studied in Section 5, where we prove Theorems 1 and 2.

2. Non-conjugate maximal subgroups of almost simple groups

In this section, we prove Theorem 3. To do so, we shall first prove several elementary lemmas and show how Theorem 3 follows from Theorems 4 and 2.1. We then work through the families of finite simple groups, proving Theorems 4 and 2.1: for most families, Theorem 4 follows easily from known results on elements of S that lie in few maximal subgroups. However, significantly more work is required in the case where S is orthogonal of plus type.

2.1. **Preliminary results, and statement of Theorem 2.1.** Recall the notation $\mathcal{M}_G(s)$ and $\mathcal{M'}_G(s)$ from just before Theorems 3 and 4, respectively.

Theorem 2.1. *Let $S := \mathrm{O}_8^+(q)$, with $q \in \{2, 3, 5\}$. Then S contains an element s such that, for any almost simple group G with socle S, the following statements hold.*

(i) *$\bigcap_{M \in \mathcal{M}_G(s)} M$ contains an element of $N_S(\langle s \rangle) \setminus C_S(s)$.*
(ii) *If $G > S$, then there exists an $\alpha_G \in \mathrm{Aut}(S)$ such that $\mathcal{M}'_G(s^{\alpha_G})$ contains at most one novelty maximal, and no two subgroups in $\mathcal{M}'_G(s^{\alpha_G})$ are conjugate in G.*

On the other hand, for each $r \in S$, the set $\mathcal{M}_S(r)$ contains two S-conjugate subgroups, and there exists a group R with $S < R \leqslant \mathrm{Aut}(S)$ such that $\mathcal{M}'_R(r)$ contains two R-conjugate subgroups.

This theorem suggests that the statements about the group $\Omega_8^+(5)$ from [30, p. 767] and [6, Lemma 5.15(b)] are not quite correct. We also note that Theorem 4 implies that, when S is as in that theorem, G-conjugate subgroups in $\mathcal{M}_G(s)$ correspond to conjugate maximal subgroups of G/S, and vice versa. On the other hand, the final part of Theorem 2.1 shows that Theorem 4 does not hold when $S = \mathrm{O}_8^+(q)$ with $q \in \{2, 3, 5\}$. In particular, there is no $s \in S$ such that we may set $\alpha_G = 1$ for all $G > S$.

We now state several elementary but useful results. The first of these follows readily from the Orbit-Stabiliser Theorem, and is well known; for example, see [30, Lemma 2.4] and the proof of [6, Lemma 5.9]. We will usually apply this result in the special case where H is a (non-normal) maximal subgroup of an almost simple group G.

Lemma 2.2. *Let H be a self-normalising subgroup of a finite group J, let $s \in H$, and let k be the number of J-conjugates of H that contain s. Then the following statements hold.*

(i) *$k \geqslant |N_J(\langle s \rangle) : N_H(\langle s \rangle)|$, with equality if all J-conjugates of $\langle s \rangle$ in H are H-conjugate.*

(ii) *Suppose that $|C_H(f)|$ is constant for all $f \in s^J \cap H$, and let r be the number of H-classes of elements in $s^J \cap H$. Then $k = r|C_J(s) : C_H(s)|$.*

Our next result describes how novelty maximal subgroups of a finite almost simple group G may arise as elements of $\mathcal{M}'_G(s)$, for an element s of the socle S of G. Here, we adapt [6, Lemma 2.4(2)] and its proof, which assume that $|G : S|$ is prime, to the general case.

Lemma 2.3. *Let G be a finite almost simple group with socle S, and $s \in S \setminus \{1\}$. Then each subgroup in $\mathcal{M}'_G(s)$ is the normaliser in G of the intersection of one or more G-conjugate subgroups in $\mathcal{M}_S(s)$. In particular,*

$$\bigcap_{M \in \mathcal{M}_S(s)} M \leqslant \bigcap_{M \in \mathcal{M}_G(s)} M.$$

Proof. Let $M \in \mathcal{M}'_G(s)$. Then $M \cap S \leqslant L$ for some $L \in \mathcal{M}_S(s)$. Since $M \cap S \trianglelefteq M$, we observe that $s^{x^{-1}} \in M \cap S \leqslant L$ for each $x \in M$, and so $s \in L^x$. Thus $X := \bigcap_{x \in M} L^x$ is an intersection of G-conjugate subgroups in $\mathcal{M}_S(s)$. It is clear that $M \leqslant N_G(X) < G$, and hence $M = N_G(X)$. □

Notice that, for a given non-abelian finite simple group S, the final claim in Lemma 2.3 shows that Theorem 3 holds for each finite almost simple group G with socle S if and only if it holds in the special case $G = S$.

Next, observe from the Orbit-Stabiliser Theorem that if L and M are non-conjugate maximal subgroups in S such that $N_G(L)$ and $N_G(M)$ are maximal in G, then these normalisers are not conjugate in G. Combining this with Lemma 2.3 yields the following lemma.

Lemma 2.4. *Let G be a finite almost simple group with socle S, and let s be an element of S such that no two subgroups in $\mathcal{M}_S(s)$ are S-conjugate. If the novelty maximals in $\mathcal{M}'_G(s)$ are pairwise non-conjugate in G, then all subgroups in $\mathcal{M}'_G(s)$ are pairwise non-conjugate in G. In particular, if $G > S$ and $\mathcal{M}_S(s)$ contains at most two G-conjugate subgroups, then Theorem 4(ii) holds for G and s.*

We finish this subsection by proving that Theorems 4 and 2.1 imply Theorem 3. Note that we have included the statements about novelty maximals in the first two of these theorems for general interest; they are not required to prove Theorem 3.

Proof of Theorem 3 (assuming Theorems 4 and 2.1). If $S \cong \mathrm{O}_8^+(q)$ with $q \in \{2, 3, 5\}$, then the result is an immediate consequence of Theorem 2.1(i).

In the remaining cases, let s be the element whose existence is guaranteed by Theorem 4, so that there exists a suitable $x \in N_S(\langle s \rangle) \setminus C_S(s)$. By Theorem

4(ii), no two subgroups in $\mathcal{M}_S(s)$ are S-conjugate. Lemma 2.2(i), with $J = S$ and $H = M \in \mathcal{M}_S(s)$, then shows that $N_S(\langle s \rangle) = N_M(\langle s \rangle)$, and so

$$x \in N_S(\langle s \rangle) \leqslant \bigcap_{M \in \mathcal{M}_S(s)} M.$$

Finally, Lemma 2.3 shows that for each almost simple group G with socle S, the element x lies in $\bigcap_{M \in \mathcal{M}_G(s)} M$. □

The remainder of this section is dedicated to proving Theorems 4 and 2.1. As stated in our proofs, several of our arguments involve computations performed via GAP [24] and Magma [3]. Our proofs also contain details about specific elements s that may be chosen.

2.2. **Alternating, sporadic and exceptional groups.** In this subsection, we prove Theorem 4 when S is an alternating, sporadic or exceptional group.

Proposition 2.5. *Theorem 4 holds when S is an alternating group A_n.*

Proof. Suppose first that $n \in \{5, 6, 7, 9\}$, and let s be any element of S of order 5, 5, 7 or 15, respectively. We deduce from the ATLAS [20] and calculations using the GAP Character Table Library [5] that:

(i) the subgroups in $\mathcal{M}_S(s)$ lie in exactly one, two, two and three S-conjugacy classes of subgroups, respectively; and
(ii) for each $M \in \mathcal{M}_S(s)$, all S-conjugates of $\langle s \rangle$ in M are M-conjugate, and $N_M(\langle s \rangle) = N_S(\langle s \rangle) > C_S(s)$, so Theorem 4(i) holds for s.

Using Lemma 2.2(i), with $J = S$ and $H \in \mathcal{M}_S(s)$, we see from (ii) that $k = 1$, and so no two subgroups in $\mathcal{M}_S(s)$ are conjugate in S. Moreover, if $|\mathcal{M}_S(s)| > 2$, so that $n = 9$, then the three subgroups in $\mathcal{M}_S(s)$ are pairwise non-isomorphic, and hence pairwise non-conjugate in G. Thus Theorem 4(ii) holds for S by Lemma 2.4.

Next, suppose that $n \geqslant 8$ is even. Additionally, let

$$s := (1, \dots, p)(p+1, \dots, n) \in S,$$

where p is the largest prime less than $n - 1$. First observe that s^2 and s^{-1} are both S_n-conjugate to s, and so $|N_{\mathrm{S}_n}(\langle s \rangle) : \langle s \rangle| > 2$. Thus $N_S(\langle s \rangle) > \langle s \rangle = C_S(s)$, and Theorem 4(i) holds for S. Next, Bertrand's Postulate states that there exists a prime strictly between $i := n/2 \geqslant 4$ and $2i - 2$, so $(p, n - p) = 1$. As observed in [31], it follows that $|\mathcal{M}'_G(s)| = 1$. This is because the p-cycle s^{n-p} fixes at least 3 points (since n is even), and so [36] (see also [56, Thm. 13.9]) implies that A_n and S_n are the only primitive subgroups of S_n containing s^{n-p}. It is also clear that an imprimitive group preserving j blocks of size k, with $jk = n$, cannot contain an element of order $p > n/2 \geqslant j, k$. Therefore, $\mathcal{M}'_G(s) = \{(\mathrm{S}_p \times \mathrm{S}_{n-p}) \cap G\}$, and Theorem 4(ii) holds for S.

Suppose now that $n \geqslant 11$ is odd. Here, we let

$$s := (1, \dots, p)(p+1, p+2)(p+3, \dots, n) \in S,$$

where p is the largest prime less than $n - 5$. Applying Bertrand's Postulate to $(n-1)/2 - 1$ yields $p > (n-1)/2 - 1$. Hence $p \geqslant (n-1)/2$, which is greater than each proper divisor of n. In particular, $n - (p + 3)$ is coprime to each of 2, p and $n-(p+2)$, and so $s^{n-(p+3)}$ and s^{-1} are S_n-conjugate to s. Therefore, $N_S(\langle s\rangle) > C_S(s)$. We also observe, similarly to the previous case, that A_n is the only proper transitive subgroup of S_n containing the p-cycle $s^{n-(p+2)}$. Thus $\mathcal{M}'_G(s)$ consists of three intransitive subgroups, of shape $(\mathrm{S}_p \times \mathrm{S}_{n-p}) \cap G$, $(\mathrm{S}_2 \times \mathrm{S}_{n-2}) \cap G$ and $(\mathrm{S}_{p+2} \times \mathrm{S}_{n-(p+2)}) \cap G$, respectively. Since $(n-1)/2 \leqslant p < n-5$, these subgroups are pairwise non-isomorphic, and hence Theorem 4 holds for S. □

We shall treat the Tits group ${}^2\mathrm{F}_4(2)'$ as an exceptional group.

Proposition 2.6. *Theorem 4 holds when S is a sporadic group.*

Proof. For each sporadic group S, [9, Table 1] describes, for at least one element $g \in S$, the corresponding set $\mathcal{M}_S(g)$ (much of this information is also given in [30, Table IV]). Suppose first that $S \notin \{\mathrm{M}_{12}, \mathrm{Suz}\}$, and let s be an element of S described in [9, Table 1], with $|s| = 17$ if $S = \mathrm{He}$, and $|s| = 22$ if $S = \mathrm{Fi}_{22}$. We see in [9, Table 1] that if $\mathcal{M}_S(s)$ contains two isomorphic subgroups, then $|\mathcal{M}_S(s)| = 2$ and $\langle s\rangle$ is a Sylow subgroup of S. Since at least one maximal subgroup in $\mathcal{M}_S(s)$ contains $N_S(\langle s\rangle)$, and $\langle s\rangle$ is a Sylow subgroup, it follows from Lemma 2.2(i) that if $\mathcal{M}_S(s)$ contains two isomorphic subgroups, then they are not S-conjugate.

If instead $S = \mathrm{M}_{12}$, then let s be any element of S of order 11, and if $S = \mathrm{Suz}$, then let s be any element of order 21. Lemma 2.2(i) and character table calculations in GAP show that $\mathcal{M}_S(s)$ contains exactly three subgroups, which are pairwise non-conjugate in S. Furthermore, precisely two of these subgroups are isomorphic when $S = \mathrm{M}_{12}$, and they are pairwise non-isomorphic when $S = \mathrm{Suz}$, so at most two are G-conjugate in each case.

For all S, Lemma 2.4 now yields Theorem 4(ii), and we deduce Theorem 4(i) from the ATLAS. □

Proposition 2.7. *Theorem 4 holds when S is an exceptional group.*

Proof. Suppose first that S is isomorphic to $\mathrm{G}_2(3)$, $\mathrm{G}_2(4)$, $\mathrm{F}_4(2)$ or ${}^2\mathrm{F}_4(2)'$. Then [9, p. 566] describes an element $s \in S$ of order 13, 21, 17 or 16, respectively, that lies in exactly three, one, two or two maximal subgroups of S, respectively. In each of these cases, we deduce from the ATLAS that $N_S(\langle s\rangle) > C_S(s)$, and from Lemma 2.2(i) and character table calculations in GAP that no two maximal subgroups in $\mathcal{M}_S(s)$ are conjugate in S. Additionally, if $S = \mathrm{G}_2(3)$, then we see in the ATLAS that $\mathcal{M}'_G(s)$ contains no novelty maximal. Thus Lemma 2.4 implies that Theorem 4 holds for S.

For each remaining finite exceptional simple S, Propositions 6.1 and 6.2 of [30], building on the work of Weigel [55, §4], give a semisimple $s \in S$ such that $|\mathcal{M}'_G(s)| \leqslant 2$. In fact, if $|\mathcal{M}'_G(s)| = 2$, then S is equal to $\mathrm{G}_2(3^e)$ or $\mathrm{F}_4(2^e)$ with $e \geqslant 2$, $|\mathcal{M}_S(s)| = 2$, and $\mathcal{M}'_G(s)$ contains at most one novelty maximal. Moreover, the two groups in $\mathcal{M}_S(s)$ are not S-conjugate [55, pp. 74–78]. Note that when $S = \mathrm{G}_2(3^e)$, Weigel states only that the groups in $\mathcal{M}_S(s)$ are members of two S-conjugacy classes, with each group having shape $\mathrm{SU}_3(q).2$. We can use Lemma 2.2(i) and [4, Tables 8.5, 8.6 & 8.42] to show that the element s of order q^2-q+1 lies in exactly one member of each of these conjugacy classes. Thus in all cases, Theorem 4(ii) follows from Lemma 2.4.

TABLE I. The order of a Singer cycle $\tilde{s} \in \tilde{S}$, for certain S.

S	$\lvert\tilde{s}\rvert$
$\mathrm{L}_n(q)$	$(q^n-1)/(q-1)$
$\mathrm{U}_n(q)$, n odd	$(q^n+1)/(q+1)$
$\mathrm{S}_n(q)$	$q^{n/2}+1$
$\mathrm{O}_n^-(q)$	$(q^{n/2}+1)/(2,q-1)$

It remains to show that $N_S(\langle s\rangle) > C_S(s)$ in each case. If S is not isomorphic to $\mathrm{E}_7(2)$ or $\mathrm{G}_2(q)$, then this is clear from [27, Table 6]. If instead $S \in \{\mathrm{E}_7(2), \mathrm{G}_2(q)\}$, then $\langle s\rangle$ is a maximal torus of S [19, Tables 3, 7 & 10, p. 46]. As S is the set of fixed points under a Frobenius endomorphism of a simply connected algebraic group, it follows from [22, pp. 2011–2012] that $C_S(s) = \langle s\rangle$. No non-abelian finite simple group contains a self-normalising cyclic subgroup [25], and so $N_S(\langle s\rangle) > C_S(s)$. □

2.3. **Classical groups.** This subsection consists of the proof of Theorem 4 when S is classical, as well as the proof of Theorem 2.1. Let $u := 2$ if S is unitary and $u := 1$ otherwise, and let the natural module for S be $\mathbb{F}_{q^u}^n$. We also let $\tilde{S}$ be a classical quasisimple subgroup of $\mathrm{GL}_n(q^u)$ such that $\tilde{S}/Z(\tilde{S}) \cong S$. For each $h \in S$ and $H \leqslant S$, we will write $\tilde{h}$ to denote a preimage of h in S, and $\tilde{H}$ to denote the preimage of H containing $Z(\tilde{S})$.

If a classical subgroup $\tilde{H}$ of $\mathrm{GL}_n(q^u)$ contains irreducible cyclic subgroups, then a generator $\tilde{y}$ of any such subgroup of maximal order is a *Singer cycle* of H, and the *Singer subgroup* $\langle\tilde{y}\rangle$ is equal to $\tilde{H} \cap \langle\tilde{g}\rangle$ for some Singer cycle $\tilde{g}$ of $\mathrm{GL}_n(q^u)$ (see [2, 34, 35]). We will also say that y is a *Singer cycle* of H.

In order to prove Theorem 4 when S is a classical group, we will often define a suitable s via Singer cycles of subgroups of S. The following lemma details important properties of such a Singer cycle.

Lemma 2.8. *Suppose that S is listed in Table I, and let $\tilde{s}$ be a Singer cycle of $\tilde{S}$. Then $|\tilde{s}|$ is given in the table. Moreover, $N_{\tilde{S}}(\langle\tilde{s}\rangle) > C_{\tilde{S}}(\tilde{s})$ and $N_S(\langle s\rangle) > C_S(s)$.*

Proof. The order of $\tilde{s}$ is given in [2, Table 1], and [49, p. 615] yields $N_{\tilde{S}}(\langle\tilde{s}\rangle) > C_{\tilde{S}}(\tilde{s})$. Hence either $N_S(\langle s\rangle) > C_S(s)$, or $\tilde{s}$ and $\tilde{z}\tilde{s}$ are $\tilde{S}$-conjugate for some non-identity scalar matrix $\tilde{z} \in \tilde{S}$. However, $\tilde{z}\tilde{s}$ and $\tilde{s}$ have different $\mathbb{F}_{q^{un}}$-eigenvalues on $\mathbb{F}_{q^u}^n$, and so $N_S(\langle s\rangle) > C_S(s)$. □

Note that each finite simple classical group that contains a Singer cycle (i.e., that contains an irreducible cyclic subgroup) appears in Table I (see [2, p. 188]).

The arguments later in this subsection do not apply to certain small classical groups. We therefore deal with these groups separately.

Proposition 2.9. *Theorem 4 holds for each classical group S given in Table II.*

Proof. Let s be any element of S such that $|s|$ is as in Table II. We can use Lemma 2.2(i), together with computations in Magma when $S = \mathrm{O}_8^+(4)$, or

TABLE II. The size of $\mathcal{M}_S(s)$, where S is a given classical simple group and s is any element of S of the given order.

S	$\lvert s\rvert$	$\lvert\mathcal{M}_S(s)\rvert$	S	$\lvert s\rvert$	$\lvert\mathcal{M}_S(s)\rvert$
$\mathrm{L}_3(4)$	7	3	$\mathrm{U}_5(2)$	11	1
$\mathrm{L}_6(2)$	63	2	$\mathrm{U}_6(2)$	11	4
$\mathrm{U}_3(3)$	7	1	$\mathrm{S}_6(2)$	15	2
$\mathrm{U}_3(5)$	10	2	$\mathrm{S}_8(2)$	17	3
$\mathrm{U}_4(2)$	9	2	$\mathrm{O}_7(3)$	14	3
$\mathrm{U}_4(3)$	7	7	$\mathrm{O}_8^+(4)$	65	3

character table calculations in GAP in the remaining cases, to determine the set $\mathcal{M}_S(s)$ (in certain cases, $\mathcal{M}_S(s)$, or its size, is also given in [6, §4], the proof of [30, Prop. 6.3], or the proof of [9, Thm. 6.1]). In particular, $|\mathcal{M}_S(s)|$ has the value given in Table II, and no two subgroups in $\mathcal{M}_S(s)$ are S-conjugate.

To prove Part (ii), we first note that if $S = \mathrm{S}_8(2)$, then no two subgroups in $\mathcal{M}_S(s)$ are isomorphic, and if $S = \mathrm{O}_7(3)$, then the three subgroups in $\mathcal{M}_S(s)$ lie in two isomorphism classes. If instead $S \in \{\mathrm{L}_3(4), \mathrm{O}_8^+(4)\}$, then we can show using Magma that the intersection of any two subgroups in $\mathcal{M}_S(s)$ is equal to the intersection of all three. When $|\mathcal{M}_S(s)| \leqslant 3$, it now follows from Lemma 2.3 that $\mathcal{M}'_G(s)$ contains at most one novelty maximal. In addition, we observe from the ATLAS that if $|\mathcal{M}_S(s)| > 3$ (that is, if $S \in \{\mathrm{U}_4(3), \mathrm{U}_6(2)\}$), then $\mathcal{M}'_G(s)$ contains no novelty maximals. Thus, in each case, Lemma 2.4 implies that no two subgroups in $\mathcal{M}'_G(s)$ are G-conjugate.

For Part (i), we deduce that $N_S(\langle s\rangle) > C_S(s)$, using Lemma 2.8 when s is a Singer cycle of S, using Magma when $S = \mathrm{O}_8^+(4) \cong \Omega_8^+(4)$, and using the ATLAS in the remaining cases. $\square$

In order to prove that Theorem 4 holds in the remaining cases where S contains a Singer cycle, we require the following elementary observation. Throughout the rest of this section, we shall abbreviate *primitive prime divisor* to *ppd*.

Lemma 2.10. *Let p be a prime, f a positive integer, and r a ppd of $p^f - 1$. Then r does not divide f.*

Proof. Suppose, for a contradiction, that $r \mid f$. Then there exists a positive integer $k < f$ such that $p^f = (p^k)^r \equiv p^k \pmod r$. Thus $p^f - 1 \equiv p^k - 1 \pmod r$. As r divides $p^f - 1$, it therefore also divides $p^k - 1$. This contradicts the primitivity of r as a prime divisor of $p^f - 1$. $\square$

Proposition 2.11. *Theorem 4 holds when S is linear, unitary of odd dimension, symplectic, or orthogonal of minus type with $n \geqslant 8$.*

Proof. We may assume that S has not been dealt with in Proposition 2.9, and by Proposition 2.5 that S is not isomorphic to an alternating group. We will also assume that $n \geqslant 4$ in the symplectic case, and that $q \neq 7$ if $n = 2$; we will treat $\mathrm{L}_2(7)$ as $\mathrm{L}_3(2)$.

Let s be a Singer cycle of S. Then $N_S(\langle s\rangle) > C_S(s)$ by Lemma 2.8. Additionally, the main theorem of [2] shows that if $\mathcal{M}_S(s)$ contains a maximal subgroup that is not an extension field type subgroup, then $S = \mathrm{S}_n(q)$ with q even. Moreover, if there is more than one such maximal subgroup, then there are exactly two, they are not conjugate in S, and $n = 4$ [44, Thm. 1.1, p. 94].

If $S = \mathrm{L}_2(q)$, then our exclusions on q imply that $\mathcal{M}_S(s) = \{N_S(\langle s\rangle)\}$. Otherwise, we observe from Lemma 2.8 and Zsigmondy's Theorem (since we exclude the groups in Proposition 2.9) that $|s|$ is divisible by a ppd r of $q^{un}-1$. In addition, by Lemma 2.10, $r \nmid un$. Hence [6, Lemma 2.12] implies that no two extension field subgroups in $\mathcal{M}_S(s)$ are isomorphic. The result now follows from Lemma 2.4. □

Proposition 2.12. *Theorem 4 holds when S is unitary of even dimension or orthogonal of odd dimension.*

Proof. We may assume that S has not been dealt with in Proposition 2.9, and by Proposition 2.11 that $n \geqslant 4$ in the unitary case and $n \geqslant 7$ otherwise.

Let $\tilde{M}$ be the stabiliser in $\tilde{S}$ of a non-degenerate $(n-1)$-dimensional subspace of $\mathbb{F}_{q^u}^n$, of minus type if S is orthogonal. Then $\tilde{M}$ contains a subgroup H isomorphic to $\mathrm{SU}_{n-1}(q)$ or $\Omega^-_{n-1}(q)$. Let $\tilde{s}$ be a Singer cycle of H (with respect to its action on $\mathbb{F}_{q^u}^{n-1}$), and let $\tilde{K} := Z(\tilde{S})H$. Then Lemma 2.8 (or an easy generalisation of this result in the case $Z(\tilde{S}) \not\leqslant H$) yields $N_K(\langle s\rangle) > C_K(s)$, and hence $N_S(\langle s\rangle) > C_S(s)$. Furthermore, $\mathcal{M}_S(s) = \{M\}$ by [44, Thm. 1.1, p. 93], and so the result follows by Lemma 2.4. □

The remainder of this section concerns the case $S = \mathrm{O}^+_{2m}(q)$, where without loss of generality $m \geqslant 4$, so that $\tilde{S} = \Omega^+_{2m}(q)$. The case m odd is straightforward.

Proposition 2.13. *Theorem 4 holds when $S = \mathrm{O}^+_{2m}(q)$, with $m \geqslant 5$ odd.*

Proof. Choose $\tilde{s}$ to be the element of order $(q^{(m-1)/2}+1)(q^{(m+1)/2}+1)/(4, q-1)$ of $\tilde{S}$ described in Proposition 5.13 of [6], so that $\tilde{s}$ is a product of two Singer cycles of orthogonal subgroups of $\tilde{S}$, unless $q \equiv 3 \pmod 4$. Then [6, Proposition 5.13] shows that $\tilde{s}$ lies in a unique maximal subgroup of $\tilde{S}$, namely, the stabiliser of an $(m-1)$-dimensional subspace of $\mathbb{F}_q^{2m}$ of minus type. Hence $|\mathcal{M}_S(s)| = 1$, and Part (ii) follows from Lemma 2.4.

It remains to show that $N_S(\langle s\rangle) > C_S(s)$. The set of $\overline{\mathbb{F}_q}$-eigenvalues of $\tilde{s}$ is a subset of $\mathbb{F}_{q^{(m-1)(m+1)/2}}$ that is closed under conjugation by the field automorphism $\alpha \mapsto \alpha^q$. Thus the distinct elements $\tilde{s}$, $\tilde{s}^q$ and $\tilde{s}^{q^2}$ all have the same eigenvalues. Note also that $\langle\tilde{s}\rangle$ stabilises no one-dimensional subspace of $\mathbb{F}_q^{2m}$; otherwise, $\mathcal{M}_S(s)$ would contain the stabiliser of such a subspace. Thus it follows from [54, pp. 38–39] (see also [6, Prop. 2.11] for an explicit statement) and [21, Thms 6.1.12 & 6.1.15] that $\tilde{s}$ is $\tilde{S}$-conjugate to at least one of $\tilde{s}^q$ and $\tilde{s}^{q^2}$. As $\tilde{s}$ and $-\tilde{s}$ do not have equal eigenvalues when q is odd, we deduce that $N_S(\langle s\rangle) > C_S(s)$. □

The case where m is even is much more involved.

Proof of Theorem 2.1. As specified below, many of the facts about almost simple groups mentioned in this proof were deduced using Magma. In the case $q = 5$, most of our computations were performed in the matrix group $\tilde{S} = \Omega_8^+(5)$, since this group's maximal subgroups can be constructed using the `ClassicalMaximals` function. In general, in order to show that an element $r \in S$ lies in multiple G-conjugates of a given maximal subgroup $M \in \mathcal{M}'_G(r)$, it suffices by Lemma 2.2(i) to verify that $N_G(\langle r\rangle) > N_M(\langle r\rangle)$.

The majority of the proof will be divided into two cases, depending on q. However, we first observe computationally that for the element s specified in each case below, $\bigcap_{M\in\mathcal{M}_S(s)} M$ contains an element of $N_S(\langle s\rangle) \setminus C_S(s)$, and hence by Lemma 2.3, so does $\bigcap_{M\in\mathcal{M}_G(s)} M$. Computations also show that for each $r \in S$, there exist two S-conjugate subgroups in $\mathcal{M}_S(r)$. Therefore it remains to prove Part (ii), and the rest of the final claim of the theorem.

Case (a): $q = 2$. Let s be any element of S of order 15. If $|G : S| \geqslant 3$, then we observe from the ATLAS that, up to G-conjugacy, G has a unique maximal subgroup of order divisible by $|s|$ that does not contain S. In fact, we see using Magma that this maximal subgroup has no element of order $|s|$, and so $\mathcal{M}'_G(s) = \varnothing$.

If instead $|G : S| = 2$, so that $G \cong \mathrm{SO}_8^+(2)$, then no novelty maximal of G has order divisible by $|s|$. Furthermore, computations show that there exist $\alpha, \beta \in \mathrm{Aut}(S)$ such that $\mathcal{M}'_G(s^\alpha) = \varnothing$, while two subgroups in $\mathcal{M}'_G(s^\beta)$ are conjugate in G. We also observe via Magma that for each $h \in S$ that is not G-conjugate to s^α, there exist two G-conjugate subgroups in $\mathcal{M}'_G(h)$. Hence for each $r \in S$, there exists an $\mathrm{Aut}(S)$-conjugate R of G such that $\mathcal{M}'_R(r)$ contains two R-conjugate subgroups.

Case (b): $q \in \{3, 5\}$. Magma computations show that S has precisely three conjugacy classes of cyclic subgroups of order $(q^3 + 1)/2$, and for any element s of this order, the subgroups in $\mathcal{M}_S(s)$ isomorphic to $\Omega_7(q)$ are members of two S-conjugacy classes (with these classes depending on the class of $\langle s\rangle$). Moreover, the maximal subgroups of S isomorphic to $\Omega_7(q)$ fall into six S-conjugacy classes, and only one $\mathrm{Aut}(S)$-conjugacy class [39, Table I]. We therefore deduce that there exist $\theta_1, \theta_2 \in \mathrm{Aut}(S)$ such that $\langle s\rangle$, $\langle s^{\theta_1}\rangle$ and $\langle s^{\theta_2}\rangle$ lie in three distinct S-classes. Additional computations show that for each $t \in \{s, s^{\theta_1}, s^{\theta_2}\}$, the set $\mathcal{M}_S(t)$ contains precisely three subgroups that are not isomorphic to $\Omega_7(q)$: the stabiliser $K_{t,1}$ in S of a 6-dimensional subspace of $\mathbb{F}_q^8$ of minus type, and two of its images $K_{t,2}$ and $K_{t,3}$ under triality automorphisms of S (see [39, Table I]). In particular, these three subgroups are pairwise non-conjugate in S.

Next, we observe using [4, Table 8.50] that if M is a novelty maximal subgroup of G whose order is divisible by $|s|$, then either $M \cap S \cong \mathrm{G}_2(q)$; $M \cap S$ is an extension of a 2-group by A_8 or by $\mathrm{L}_3(2)$; or $M \cap S$ is S-conjugate to $U_t := K_{t,1} \cap K_{t,2} \cap K_{t,3}$. However, we see in the ATLAS that $\mathrm{G}_2(q)$ contains no element of order $|s|$, and no maximal subgroup in $\mathcal{M}_S(t)$ has order divisible by the order of any of these extensions of 2-groups. It therefore follows from Lemma 2.3 that any novelty maximal subgroup in $\mathcal{M}'_G(t)$ is equal to $N_G(U_t)$.

We now conclude from [39, Table I] that, for each $G > S$, there exists $\alpha_G \in \{1, \theta_1, \theta_2\}$ such that, when $t = s^{\alpha_G}$, any subgroup in $\mathcal{M}'_G(t)$ is equal to either

$N_G(U_t)$ or $N_G(K_{t,i})$ for some $i \in \{1,2,3\}$. Moreover, since $K_{t,i}$ and $K_{t,j}$ are not S-conjugate when $i \neq j$, if $N_G(K_{t,i})$ and $N_G(K_{t,j})$ are maximal in G then they are not G-conjugate. Therefore, no two subgroups in $\mathcal{M}'_G(t)$ are G-conjugate.

Finally, let $r \in S$, and suppose that $G \cong \mathrm{PSO}_8^+(q)$ and that no two subgroups in $\mathcal{M}'_G(r)$ are G-conjugate. Using Magma and [39, Table I], we deduce that either there exists $\rho \in \mathrm{Aut}(S)$ such that $\mathcal{M}'_{G^\rho}(r)$ contains two G^ρ-conjugate subgroups; or $q = 5$, and there exists a graph automorphism π of S (of order 2 or 3) such that $\mathcal{M}'_{\langle S,\pi\rangle}(r)$ contains two $\langle S,\pi\rangle$-conjugate subgroups. Therefore, for each $r \in S$, there exists a group R with $S < R \leqslant \mathrm{Aut}(S)$ such that $\mathcal{M}'_R(r)$ contains two R-conjugate subgroups. $\square$

Now, to prove Theorem 4 for m even, we would like to use Proposition 5.14 and Lemma 5.15 of [6]. However, we require a slightly stronger statement than Proposition 5.14. Additionally, the statement of Proposition 5.14 is not quite correct when $4 \mid m$, nor is the proof of Lemma 5.15(b)–(c). We therefore prove the following result, much of whose proof is similar to [6, §5], and which implies that [6, Lemma 5.15(b)] is in fact correct when $q \geqslant 7$. We exclude the groups $\mathrm{O}_8^+(q)$ for $q \leqslant 5$, which we dealt with in Theorem 2.1 and Proposition 2.9.

Theorem 2.14. *Suppose that $S = \mathrm{O}_{2m}^+(q)$, with $m \geqslant 4$ even, and $q \geqslant 7$ if $m = 4$. Then $\tilde{S}$ contains an element $\tilde{s}$ of order $k = k(m,q)$, where*

$$k := \begin{cases} (q^2+1)/(2,q-1), & \text{if } m = 4,\\ (q^{(m-2)/2}+1)(q^{(m+2)/2}+1)/(4,q-1), & \text{if } 4 \nmid m,\\ (q^{(m-2)/2}+1)(q^{(m+2)/2}+1)/(q+1), & \text{if } m = 8 \text{ and } q = 2,\\ (q^{(m-2)/2}+1)(q^{(m+2)/2}+1)/(q+1)^2, & \text{otherwise,} \end{cases}$$

such that the following statements hold.

(i) *There are precisely three subgroups in $\mathcal{M}_{\tilde{S}}(\tilde{s})$, which we will denote by $\tilde{K}_1$, $\tilde{K}_2$ and $\tilde{L}$.*

(ii) *The groups $\tilde{K}_1$ and $\tilde{K}_2$ are extension field subgroups that are not conjugate in $\tilde{S}$. If $4 < m \equiv 0 \pmod 4$, then $\tilde{K}_1$ and $\tilde{K}_2$ are of (Aschbacher) type $\mathrm{GU}_m(q)$. Otherwise, they are of type $\mathrm{GO}_m^+(q^2)$.*

(iii) *Let $V := \mathbb{F}_q^{2m}$. If $m = 4$, then $\tilde{L}$ is imprimitive, stabilising the decomposition $V = U \perp U^\perp$, for some four-dimensional subspace U of V of minus type. Otherwise, $\tilde{L}$ is the stabiliser of an $(m-2)$-dimensional subspace of V of minus type.*

Note that the case $m = 8$ and $q = 2$ is exceptional as here $q^{m-2} - 1 = 2^6 - 1$ has no ppd. We begin by defining the element $\tilde{s}$ that we will use in each case.

Assumption 2.15. Suppose that $S = \mathrm{O}_{2m}^+(q)$, with $m \geqslant 4$ even, and $q \geqslant 7$ if $m = 4$. Additionally, let $k = k(m,q)$ be as in Theorem 2.14. If $4 \nmid m$, then let $\tilde{s} \in \tilde{S}$ be as described in [6, Prop. 5.14], so that $\langle \tilde{s} \rangle$ has order k and stabilises exactly two proper non-zero subspaces of $V := \mathbb{F}_q^{2m}$, namely, an $(m-2)$-dimensional subspace of V of minus type and its orthogonal complement.

From now on, suppose that $4 \mid m$. Let $\tilde{X}$ be the stabiliser in $\tilde{S}$ of a subspace U of V of minus type, of dimension four if $m = 4$ or dimension $m - 2$ if $m > 4$.

Then $U^\perp$ is also of minus type. Additionally, $\tilde{X}$ contains the subgroup $R_1 \times R_2$, where $R_1 \cong \Omega(U)$ and $R_2 \cong \Omega(U^\perp)$.

We define $\tilde{r}_1$ and $\tilde{r}_2$ to be elements of Singer subgroups of R_1 and R_2, respectively (corresponding to their actions on U and $U^\perp$), as follows; in each case, an element of the specified order exists by Lemma 2.8. If $m = 4$, then let $\tilde{r}_1$ and $\tilde{r}_2$ both have order k. Then $\tilde{r}_1$ has eigenvalues α, α^q, α^{q^2} and α^{q^3} on U, while $\tilde{r}_2$ has eigenvalues β, β^q, β^{q^2} and β^{q^3} on $U^\perp$, where α and β are elements of $\mathbb{F}_{q^4}$ of order k. Similarly to the proof of [6, Lemma 5.15], we choose $\tilde{r}_2$ in this case so that these eight eigenvalues are all distinct (we will place further restrictions on $\tilde{r}_2$ in the case $m = 4$ in the proof of Proposition 2.21). If instead $m > 4$, then let $\tilde{r}_1$ and $\tilde{r}_2$ have order $(q^{(m-2)/2}+1)/t$ and $(q^{(m+2)/2}+1)/(q+1)$, respectively, where $t := 1$ if $m = 8$ and $q = 2$, and $t := q + 1$ in all remaining cases. For all m (with $4 \mid m$), let $\tilde{s} := (\tilde{r}_1, \tilde{r}_2) \in \tilde{X}$. We deduce that $|\tilde{s}| = k$.

Next, we show that when $4 \mid m$, the group $\tilde{L}$ from Theorem 2.14 is the unique subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ that is not isomorphic to the specified extension field group $\tilde{K}_1$. We first state two preliminary results.

Lemma 2.16. *Let $\tilde{S}$, U and $\tilde{s}$ be as in Assumption 2.15, with $4 \mid m$. Then U and $U^\perp$ are the only proper non-zero subspaces of $\mathbb{F}_q^n$ stabilised by $\langle \tilde{s} \rangle$.*

Proof. If $m = 8$ and $q = 2$, then the element $\tilde{r}_1$ from Assumption 2.15 is a Singer cycle of $\Omega_6^-(2)$ by Lemma 2.8, and hence $\langle \tilde{r}_1 \rangle$ acts irreducibly on U. In the remaining cases, $|\tilde{r}_1|$ is divisible by each ppd of $q^{\dim(U)} - 1$, and in all cases, $|\tilde{r}_2|$ is divisible by each ppd of $q^{\dim(U^\perp)} - 1$. We therefore deduce from [33, Thm. 3.5] that $\tilde{s} = (\tilde{r}_1, \tilde{r}_2)$ acts irreducibly on each of U and $U^\perp$.

Now, if $m = 4$, then the eigenvalues of $\tilde{s}$ on U are distinct from its eigenvalues on $U^\perp$, and otherwise, $\dim(U) \neq \dim(U^\perp)$. Thus U and $U^\perp$ are non-isomorphic irreducible $\mathbb{F}_q[\langle \tilde{s} \rangle]$-modules, and the result follows. □

Lemma 2.17. *Let $m \geqslant 8$ be a multiple of 4, and suppose that $m + 3$ is a ppd of $q^{m+2} - 1$. Then the symmetric group S_{2m+2} contains no element of order $k = k(m, q)$, as defined in Theorem 2.14.*

Proof. If $q = 2$ and $m = 8$, then $\mathrm{S}_{2m+2} = \mathrm{S}_{18}$ contains no element of order $k = 99$. Assume therefore that $q > 2$ or $m > 8$, and suppose for a contradiction that y is an element of S_{2m+2} of order k. Observe that k is divisible by each ppd of $q^{m+2} - 1$, and hence by $m + 3$. Similarly, k is divisible by each ppd of $q^{m-2} - 1$, and such a prime is no smaller than $m - 1$ (see [29, Remark 1.1]). As $(m - 1) + (m + 3)$ is the degree of S_{2m+2}, we deduce that k is the product $(m-1)(m+3)$ of two primes. Now, $(q^{(m-2)/2}+1, q^{(m+2)/2}+1) = q+1$, and it follows that $m-1 = (q^{(m-2)/2}+1)/(q+1)$ and $m+3 = (q^{(m+2)/2}+1)/(q+1)$. Substituting these equalities into $(m - 1) + 4 = m + 3$, we deduce that $4 = q^{(m-2)/2}(q - 1)$, a contradiction for all q and m. □

Proposition 2.18. *Let $\tilde{S}$, U and $\tilde{s}$ be as in Assumption 2.15, with $m \geqslant 8$ and $4 \mid m$. Then the stabiliser of U in $\tilde{S}$ is the unique subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ that is not an extension field subgroup of type $\mathrm{GU}_m(q)$.*

Proof. Notice that $|\tilde{s}|$ is divisible by each ppd of $q^{m+2}-1$. The main theorem of [29] yields all possibilities for maximal subgroups of $\tilde{S}$ whose orders are divisible by such a prime. We deduce, with the aid of [38, Table 3.5.E] and [4, Table 2.5], that if $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains a subgroup $\tilde{M}$ that is not reducible or an extension field subgroup, then $m+3$ is the unique ppd of $q^{m+2}-1$, and $\tilde{M}$ is an extension of a (possibly trivial) 2-group by an alternating or symmetric group of degree at most $2m+2$. As $|\tilde{s}|$ is odd, S_{2m+2} must then contain an element of order $|\tilde{s}|$. However, Lemma 2.17 shows that this is not the case. Therefore, each subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ is reducible or an extension field subgroup.

It is clear from Lemma 2.16 that the stabiliser of U in $\tilde{S}$ is the unique reducible subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$. Thus it remains to show that $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains no extension field subgroup $\tilde{Y}$ that is not of type $\mathrm{GU}_m(q)$. By [29], any such $\tilde{Y}$ whose order is divisible by a ppd of $q^{m+2}-1$ is defined over q^2, and so $\tilde{Y}$ is an extension of $\Omega_m^+(q^2)$ by a group of order 4 [4, Table 2.6]. The p'-part of the order of $\Omega_m^+(q^2)$ divides $(q^m-1)\prod_{i=1}^{m/2-1}(q^{4i}-1)$, and for each positive integer $f \in \{m+3,\ldots,2m-4\}$, no ppd of $q^{m+2}-1$ divides q^f-1.We conclude that $|\tilde{Y}|$ is not divisible by any ppd of $q^{m+2}-1$, and therefore $\tilde{Y} \notin \mathcal{M}_{\tilde{S}}(\tilde{s})$. □

In order to prove a similar proposition when $m=4$, we consider maximal tori of $\tilde{S}$ (or $\mathrm{SO}_{2m}^+(q)$ if q is odd) that contain $\tilde{s}$, via a brief discussion of related algebraic groups. We in fact allow m to be any even integer at least 4, as the results here will also be useful when considering extension field subgroups in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ in each case.

Let $\underline{S}$ be the algebraic group $\mathrm{SO}_{2m}(\overline{\mathbb{F}_q})$ for some $m \geqslant 4$. There exists a Frobenius endomorphism σ of $\underline{S}$ such that the subgroup $\hat{S} := \underline{S}_\sigma$ of fixed points of $\underline{S}$ under σ is equal to $\mathrm{SO}_{2m}^+(q)$ if q is odd, or $\Omega_{2m}^+(q)$ if q is even (see [45, pp. 193–194], where $\Omega_{2m}^+(q)$ is written as $\mathrm{SO}_{2m}^+(q)$ when q is even). By definition, each maximal torus $\hat{T}$ of $\hat{S}$ is equal to $\underline{T} \cap \hat{S}$ for a corresponding maximal torus $\underline{T}$ of $\underline{S}$. An element $\tilde{r}$ of $\hat{T}$ is called *regular* if the dimension of $C_{\underline{S}}(\tilde{r})$ is no larger than the dimension of $C_{\underline{S}}(\tilde{x})$ for any $\tilde{x} \in \underline{S}$, or equivalently, if $\underline{T}$ is equal to $C_{\underline{S}}(\tilde{r})^\circ$, the connected component of $C_{\underline{S}}(\tilde{r})$ containing the identity [45, Defn. 14.8, Cor. 14.10]. We will continue to use this notation in the following two results and their proofs.

Lemma 2.19. *Let $\tilde{r}$ be a regular element of a maximal torus $\hat{T}$ of $\hat{S}$. If $|\tilde{r}|$ is odd, then $C_{\hat{S}}(\tilde{r}) = \hat{T}$.*

Proof. As $\tilde{r}$ is regular, $\underline{T} = C_{\underline{S}}(\tilde{r})^\circ$. In addition, it follows from [45, pp. 70–72, Prop. 14.20] that the order of $C_{\underline{S}}(\tilde{r})/C_{\underline{S}}(\tilde{r})^\circ$ divides $(2, q-1)$, and its exponent divides $|\tilde{r}|$. Hence if $|\tilde{r}|$ is odd, then $C_{\underline{S}}(\tilde{r}) = \underline{T}$, and so $C_{\hat{S}}(\tilde{r}) = \underline{T} \cap \hat{S} = \hat{T}$. □

Lemma 2.20. *Let $\tilde{S}$ and $\tilde{s}$ be as in Assumption 2.15. Then the centraliser $C_{\hat{S}}(\tilde{s}) = C_{\mathrm{GO}_{2m}^+(q)}(\tilde{s})$ is a maximal torus of $\hat{S}$ of shape $(q^a+1)\times(q^b+1)$, where $a+b=m$, with $a := 2$ if $m=4$ and $a := (m-2)/2$ otherwise.*

Proof. As $\tilde{s}$ is semisimple, it lies in a maximal torus $\hat{T}$ of $\hat{S}$. By considering the maximal tori of $\hat{S}$ (see [11, §4–5], [53, §9] and [51, Lemma 2]), we deduce that if $\hat{T}$ does not have shape $(q^a+1)\times(q^b+1)$, then $m=4$ and $\hat{T}$ is a cyclic group of order q^4-1 that stabilises a totally singular four-dimensional subspace of $\mathbb{F}_q^8$. Lemma 2.16 shows that this second case cannot occur.

Recall that when $m=4$, the elements $\tilde{r}_1$ and $\tilde{r}_2$ from Assumption 2.15 have distinct eigenvalues on $\mathbb{F}_q^8$. Additionally, even though $q^{2a}-1$ has no ppd when $m=8$ and $q=2$, the element $\tilde{r}_1$ in this case has order 9, and no element of this order lies in a proper subfield of $\mathbb{F}_{q^{2a}}=\mathbb{F}_{2^6}$. We therefore deduce from [53, §9] in each case that $\tilde{s}^2$ is a regular element of $\hat{T}$ (as is $\tilde{s}$). Since $C_{\hat{S}}(\tilde{s})\leqslant C_{\hat{S}}(\tilde{s}^2)$ and $|\tilde{s}^2|$ is odd, we obtain $C_{\hat{S}}(\tilde{s})=\hat{T}$ from Lemma 2.19.

Finally, it follows from Lemma 2.16 if $4\mid m$, or from the definition of $\tilde{s}$ in Assumption 2.15 if $4\nmid m$, that $\langle\tilde{s}\rangle$ stabilises no one-dimensional subspace of $\mathbb{F}_q^n$. Hence $\tilde{s}$ has no linear elementary divisor, and so [21, p. 85–86] yields $C_{\hat{S}}(\tilde{s})=C_{\mathrm{GO}_{2m}^+(q)}(\tilde{s})$. □

We can now prove a version of Proposition 2.18 with $m=4$.

Proposition 2.21. *Let $\tilde{S}$ and U be as in Assumption 2.15, with $m=4$ and $q\geqslant 7$. Then the element $\tilde{s}$ from Assumption 2.15 can be chosen so that the stabiliser of the decomposition $\mathbb{F}_q^{2m}=U\perp U^\perp$ in $\tilde{S}$ is the unique subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ that is not an extension field subgroup of type $\mathrm{GO}_m^+(q^2)$.*

Proof. We shall initially consider an arbitrary choice for $\tilde{s}$, and work through the families of maximal subgroups of $\tilde{S}$, given in [4, Table 8.50] (see also [39, Table I]). Let $\tilde{L}$ be the stabiliser in $\tilde{S}$ of the decomposition of $V:=\mathbb{F}_q^8$ as $U\perp U^\perp$. Then $\tilde{L}$ contains the stabiliser in $\tilde{S}$ of U. Lemma 2.16 shows that U and $U^\perp$ are the only proper non-zero subspaces of V stabilised by $\langle\tilde{s}\rangle$. Therefore, $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains no reducible subgroups. Moreover, if $\langle\tilde{s}\rangle$ stabilises a decomposition $V=W_1\oplus W_2$, where $\dim(W_1)=\dim(W_2)=4$, then $\langle\tilde{s}^2\rangle=\langle\tilde{s}\rangle$ stabilises each of W_1 and W_2, and hence $\{W_1,W_2\}=\{U,U^\perp\}$. Thus $\tilde{L}$ is the unique stabiliser of such an imprimitive decomposition that contains $\tilde{s}$.

Next, let $\tilde{E}$ be an extension field subgroup of $\tilde{S}$ of type $\mathrm{GU}_4(q)$, and recall that $\hat{S}=\mathrm{SO}_{2m}^+(q)$ if q is odd, and $\hat{S}=\tilde{S}$ if q is even. We see from [7, Construction 2.5.14, Lemma 5.3.6] that $\hat{E}:=N_{\hat{S}}(\tilde{E})$ has shape $\mathrm{GU}_4(q).2$. Thus by [11, Cor. 2] (see also [51, Lemma 2]), each (semisimple) element of $\hat{E}$ of order $k:=|\tilde{s}|$ lies in a cyclic maximal torus of $\mathrm{GU}_4(q)$ of order q^4-1. However, Lemma 2.20 shows that $C_{\hat{S}}(\tilde{s})$ is not cyclic. We therefore deduce that $\tilde{s}\notin\tilde{E}$.

For a similar argument, let X be a maximal subgroup of S that is isomorphic to $\Omega_7(q)$ if q is odd, or to $\mathrm{Sp}_6(q)$ if q is even. Then each element of X of order $|s|=k$ lies in a maximal torus of shape $k\times(q+1)$ or $k\times(q-1)$ [11, Thms. 3–4]. Additionally, $C_S(s)$ is abelian of order k^2 [11, Thms. 5 & 7]. As k^2 is divisible by neither $q+1$ nor $q-1$ (since $q\neq 2$), we see that $s\notin X$ and $\tilde{s}\notin\tilde{X}$.

Suppose now that q is odd, and let H be a maximal subgroup of S of shape $(\mathrm{L}_2(q)\times\mathrm{S}_4(q)).2$. Since $|\mathrm{L}_2(q)|$ and $|s|$ are coprime, any element of H of order k has a centraliser that contains the non-abelian group $\mathrm{L}_2(q)$. Thus $\tilde{s}\notin\tilde{H}$.

It now follows from [39, Table I] and [4, Table 8.50] that if $\tilde{Y}$ is any other maximal subgroup of $\tilde{S}$ whose order is divisible by k, such that $\tilde{Y}$ is not an extension field subgroup of type $\mathrm{GO}_m^+(q^2)$, then q is a square and $Y\cong\Omega_8^-(\sqrt{q})$.

For a subspace W of V and an element $g \in \tilde{S}$, let g_W denote the set of $\mathbb{F}_{q^8}$-eigenvalues of g on W. Recall from Assumption 2.15 that $\tilde{s}_U = \mathcal{A} := \{\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}\}$ and $\tilde{s}_{U^\perp} = \mathcal{B} := \{\beta, \beta^q, \beta^{q^2}, \beta^{q^3}\}$, where α and β are elements of $\mathbb{F}_{q^4}$ of order k and $\mathcal{A} \cap \mathcal{B} = \varnothing$. Let $\mathcal{Y}$ be the set of maximal subgroups $\tilde{Y}$ of $\tilde{S}$ such that $Y \cong \Omega_8^-(\sqrt{q})$, and for $\tilde{Y} \in \mathcal{Y}$, let $\mathcal{J}(\tilde{Y})$ be the set of elements $y \in \tilde{Y}$ of order k, such that the proper non-zero subspaces of V stabilised by y are precisely U and $U^\perp$; the set y_V contains $\mathcal{A}$; and $y_V \setminus \mathcal{A} = \{\gamma, \gamma^q, \gamma^{q^2}, \gamma^{q^3}\}$ for some $\gamma \in \mathbb{F}_{q^4}$ of order k. Additionally, let

$$\mathcal{E} := \left\{ y_V \setminus \mathcal{A} \mid y \in \mathcal{J}(\tilde{Y}), \tilde{Y} \in \mathcal{Y} \right\}.$$

We will determine an upper bound for $|\mathcal{E}|$. Using this bound, we will show that the element $\tilde{r}_2$ in Assumption 2.15 (equivalently, the set $\mathcal{B}$) can be chosen so that, for all $\tilde{Y} \in \mathcal{Y}$, the set $\mathcal{J}(\tilde{Y})$ does not contains $\tilde{s}$, and so $\tilde{s} \notin \tilde{Y}$.

Fix $\tilde{Y} \in \mathcal{Y}$ and $y \in \mathcal{J}(\tilde{Y})$. Notice that $\{\mathcal{A}, y_V \setminus \mathcal{A}\} = \{y_U, y_{U^\perp}\}$, and that a given $c \in \langle y \rangle \cap \mathcal{J}(\tilde{Y})$ satisfies $c_U = y_U$ if and only if $c_{U^\perp} = y_{U^\perp}$ (additionally, at least one of c_U and $c_{U^\perp}$ is equal to $\mathcal{A}$). We also deduce from [11, §4–5] (and the fact that $Y \cong \mathrm{PSO}_8^-(\sqrt{q})$ if q is odd) that any two cyclic subgroups of $\tilde{Y}$ of order k are conjugate in $\tilde{S}$. Thus the fixed $\tilde{Y} \in \mathcal{Y}$ contributes two (not necessarily distinct) sets to $\mathcal{E}$: the set $y_{U^\perp}$ for elements $y \in \mathcal{J}(\tilde{Y})$ such that $y_U = \mathcal{A}$, and the set y_U for elements $y \in \mathcal{J}(\tilde{Y})$ such that $y_{U^\perp} = \mathcal{A}$.

We observe from Rows 64–69 and Columns V and XII of [39, Table I] that the subgroups in $\mathcal{Y}$ form exactly two $N_{\mathrm{GL}_8(q)}(\tilde{S})$-conjugacy classes. Thus there exist $\tilde{Y}_1, \tilde{Y}_2 \in \mathcal{Y}$ such that

$$\mathcal{E} = \left\{ y_V \setminus \mathcal{A} \mid y \in \mathcal{J}(\tilde{Y}_1) \cup \mathcal{J}(\tilde{Y}_2) \right\}.$$

By the previous paragraph, each of $\tilde{Y}_1$ and $\tilde{Y}_2$ contributes at most two sets to $\mathcal{E}$, and thus $|\mathcal{E}| \leqslant 4$.

To ensure that $\tilde{s}$ does not lie in $\mathcal{J}(\tilde{Y})$ for any $\tilde{Y} \in \mathcal{Y}$ (and hence that $\tilde{s} \notin \tilde{Y}$), it suffices to choose $\tilde{r}_2$ in Assumption 2.15 so that the corresponding set $\mathcal{B}$ intersects trivially with each of the sets in $\mathcal{E}$, and with $\mathcal{A}$ (as required to satisfy Assumption 2.15). Since each of these sets of eigenvalues has size four, this is possible as long as $\varphi(k)/4 \geqslant 6$, where φ is Euler's totient function. It is well known (see, e.g., [47, Prop. 2]) that $\varphi(i) \geqslant \sqrt{i/2}$ for each i. Hence an appropriate $\tilde{r}_2$ exists if $k \geqslant 1152$. If instead $k < 1152$, then the square $q \geqslant 9$ is at most 25, and again $\varphi(k)/4 \geqslant 6$. $\square$

We observe from [6, Prop. 5.14] that, when $4 \nmid m$, the subgroup $\tilde{L}$ described in Theorem 2.14 is the unique subgroup in $\mathcal{M}_{\tilde{S}}(\tilde{s})$ that is not an extension field subgroup. Thus to prove Theorem 2.14, it remains to show, for all even $m \geqslant 4$, that $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains exactly two extension field subgroups of the specified type, and that they are not conjugate in $\tilde{S}$.

Proposition 2.22. *Let $\tilde{S}$ and $\tilde{s}$ be as in Assumption 2.15. Then $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains exactly two extension field subgroups of type J, where $J \cong \mathrm{GU}_m(q)$ if*

$4 < m \equiv 0 \pmod 4)$, *and* $J \cong \mathrm{GO}_m^+(q^2)$ *otherwise. Additionally, the two subgroups are not conjugate in* $\tilde{S}$.

Proof. Let a, b, and $\hat{S}$ be as in Lemma 2.20, so that $C_{\hat{S}}(\tilde{s}) = C_{\mathrm{GO}_{2m}^+(q)}(\tilde{s})$ is a maximal torus $\hat{T}$ of $\hat{S}$ of shape $(q^a+1) \times (q^b+1)$. Additionally, let $\tilde{K}$ be a subgroup of $\tilde{S}$ of type J. Then [7, Constructions 2.5.13–2.5.14, Lemmas 5.3.4 & Lemma 5.3.6] and [38, Tables 3.5.E & 3.5.G] imply that

$$\hat{K} := N_{\hat{S}}(\tilde{K}) \cong J.\langle \phi \rangle,$$

where ϕ is the involutory field automorphism of the subgroup $\mathrm{SU}_m(q)$ or $\Omega_m^+(q^2)$ of J. As all maximal tori of $\hat{S}$ isomorphic to $\hat{T}$ are conjugate in $\hat{S}$ [53, p. 394], and as J contains such a maximal torus (see [11, Cor. 2], [53, §9] and [51, Lemma 2]), some $\hat{S}$-conjugate of $\hat{K}$ contains $\hat{T}$, and hence contains $\tilde{s}$. Now, by [4, Tables 8.50 & Table 8.82] and [38, Tables 3.5.E & 3.5.G], $\tilde{S}$ has exactly two conjugacy classes of maximal subgroups that are extension field subgroups of type J, and these extend to two conjugacy classes of maximal subgroups of $\hat{S}$. We have shown that each of these two conjugacy classes has at least one subgroup containing $\tilde{s}$.

To complete the proof, we will show that $\mathcal{M}_{\tilde{S}}(\tilde{s})$ contains exactly two extension field subgroups of type J. If $4 \nmid m$, then this is the case by [6, Prop. 5.14]. If instead $4 \mid m$, then $|s|$ is odd. Thus [54, p. 34, pp. 38–39] (see also [6, Prop. 2.11]) implies that any two similar elements of $\mathrm{GO}_{2m}^+(q)$ are conjugate, as are any two similar elements of J. Additionally, conjugating $\tilde{K}$ by an element of $\hat{S}$ if necessary, we may assume that $\hat{T} \leqslant \hat{K}$. Therefore, arguing as in the proof of [6, Lemma 5.9], we deduce that the elements of $\tilde{s}^{\mathrm{GO}_{2m}^+(q)} \cap \hat{K}$ form exactly two $\hat{K}$-conjugacy classes.

Now, any two extension field subgroups of $\tilde{S}$ of type J extend to conjugate subgroups of $\mathrm{GO}_{2m}^+(q)$ [38, Tables 3.5.E & Table 3.5.G], and so $\hat{K}$ is self-normalising in $\mathrm{GO}_{2m}^+(q)$. Moreover, by considering the maximal tori of J (again, see [11, Cor. 2], [53, §9] and [51, Lemma 2]), we deduce that $C_{\mathrm{GO}_{2m}^+(q)}(\tilde{f}) \leqslant \hat{K}$ for each $\tilde{f} \in \tilde{s}^{\mathrm{GO}_{2m}^+(q)} \cap \hat{K}$. Therefore, Lemma 2.2(ii) implies that $\tilde{s}$ lies in exactly two $\mathrm{GO}_{2m}^+(q)$-conjugates of $\hat{K}$, and hence in exactly two $\mathrm{GO}_{2m}^+(q)$-conjugates of $\tilde{K}$. □

Theorem 2.14 now follows from [6, Prop. 5.14] (with $4 \nmid m$) and Propositions 2.18, 2.21 and 2.22. We are also now able to prove the final case of Theorem 4, and hence complete the proof of Theorem 3.

Proposition 2.23. *Theorem 4 holds when* $S = \mathrm{O}_{2m}^+(q)$, *with* $m \geqslant 4$ *even.*

Proof. By [23, Lemma 10], s is S-conjugate to its inverse, and so $N_S(\langle s \rangle) > C_S(s)$. Additionally, Theorem 2.14 shows that $\mathcal{M}_S(s)$ consists of three subgroups, K_1, K_2 and L, no two of which are conjugate in S. If $m = 4$, then the intersection of any two of these subgroups is equal to the intersection of all three [6, Lemma 5.15(e)], and hence Lemma 2.3 shows that $\mathcal{M}'_G(s)$ contains at most one novelty maximal. If instead $m > 4$, then L is isomorphic to neither

K_1 nor K_2 (see Table 3.5.E and the corresponding results in Chapter 4 of [38]). In each case, Lemma 2.4 yields the result. □

3. Finite groups satisfying the independence property are supersoluble

The aim of this section is to prove that each finite group G satisfying the independence property is supersoluble. We will reduce the proof of this statement to the case where G is almost simple, and finally, in the almost simple case, we will reach our conclusion by applying Theorem 3. Two elements x and y of a group G are *dependent* if no minimal generating set for G contains $\{x, y\}$.

We shall assume throughout this section that G is a finite group satisfying the independence property. Our first result reduces the study of such groups to the case where their Frattini subgroup is trivial.

Proposition 3.1. *The Frattini subgroup $\Phi(G) \neq 1$ if and only if G is either a cyclic p-group or the quaternion group of order 8.*

Proof. Suppose that $\Phi(G) \neq 1$, and let x be an element of $\Phi(G)$ of prime order. Since x is a non-generator of G, x and y are dependent for each $y \in G \setminus \{x\}$. In particular, since $|x|$ is prime, $\langle x\rangle \subseteq \langle y\rangle$ for every $y \in G \setminus \{1\}$. Thus $\langle x\rangle$ is the unique minimal subgroup of G and therefore either G is a cyclic p-group or $G = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, a^b = a^{-1}\rangle$ (with $n \geqslant 3$) is a generalized quaternion group (see [50, Thm. 9.7.3]). In the second case, $a^2 \in \Phi(G)$ and therefore b and ba^2 are dependent. Since G satisfies the independence property, $\langle b, ba^2\rangle$ is cyclic, and hence $[b, a^2] = 1$. This implies that $n = 3$, as required. The converse is clear. □

We now present a sequence of results characterising the minimal normal subgroups of our group G.

Lemma 3.2. *Suppose that $\Phi(G) = 1$, and that G has an abelian minimal normal subgroup N. Then N is cyclic of prime order.*

Proof. Let n_1 and n_2 be distinct non-trivial elements of N. We claim that they are dependent. Indeed, assume for a contradiction that $X := \{n_1, n_2, g_1, \dots, g_t\}$ is a minimal generating set for G and let $H := \langle g_1, \dots, g_t\rangle$. Since

$$G = \langle n_1, n_2, g_1, \dots, g_t\rangle \leqslant HN,$$

$G = HN$ and N is H-irreducible. But then $G = \langle n_1, g_1, \dots, g_t\rangle$, contradicting the minimality of X.

Since n_1 and n_2 are dependent, one of them is a power of the other. Since N is elementary abelian, it follows that $\langle n_1\rangle = \langle n_2\rangle$. Therefore, $N \cong C_p$. □

Lemma 3.3. *Suppose that $\Phi(G) = 1$, and that G has a non-abelian minimal normal subgroup N. If $\mathrm{O}_8^+(2)$ is not a composition factor of N, then N is simple.*

Proof. Here, $N = S_1 \times \cdots \times S_t$ with $S_i \cong S$ a non-abelian finite simple group. Assume for a contradiction that $S \neq \mathrm{O}_8^+(2)$ and $t \geqslant 2$. By [28, Cor. 7.2], there exist x and y in S such that $S = \langle x^\alpha, y^\beta\rangle$ for every $\alpha, \beta \in \mathrm{Aut}(S)$. Notice that in particular $y \neq x^\gamma$ for all $\gamma \in \mathrm{Aut}(S)$.

Let $n := (x, y, 1, \dots, 1) \in N$ and choose $g_1, \dots, g_d \in G$ such that $G = \langle g_1, \dots, g_d \rangle N$. Set $H := \langle n, g_1, \dots, g_d \rangle$ and denote by $\pi_i : N \to S_i$ the projection to the i-th factor of N. The factors $S_1, \dots, S_t$ are permuted transitively by H, so in particular there exists $h \in H$ such that $S_2^h = S_1$. Thus $\pi_1(n^h) = y^\beta$ for some $\beta \in \mathrm{Aut}(S)$.

It follows that $S_1 = \langle x, y^\beta \rangle \leqslant \langle \pi_1(n), \pi_1(n^h) \rangle \leqslant \pi_1(H \cap N)$, and since H is transitive on $\{S_1, \dots, S_t\}$, the image $\pi_i(H \cap N) = S_i$ for all $i \in \{1, \dots, t\}$. Therefore, there exists a partition of $\{1, \dots, t\}$ into u blocks of size $v := t/u$, say $J_i := \{j_{i1}, \dots, j_{iv}\}$ for $1 \leqslant i \leqslant u$, corresponding elements $\alpha_{ik} \in \mathrm{Aut}(S)$, and diagonal subgroups $\Delta_i := \{(s^{\alpha_{i1}}, \dots, s^{\alpha_{iv}}) \mid s \in S\}$ of $S_{j_{i1}} \times \cdots \times S_{j_{iv}}$, such that $H \cap N = \Delta_1 \times \cdots \times \Delta_u$. We may assume that $1 = j_{11} \in J_1$.

Since $n \in H \cap N$, it follows that $J_1 \subseteq \{1, 2\}$. If $J_1 = \{1, 2\}$, then

$$\Delta_1 = \{(s, s^\gamma) \mid s \in S\} \leqslant S_1 \times S_2,$$

with $\gamma = \alpha_{11}^{-1}\alpha_{12}$, and $n \in \Delta_1$. This implies that $y = x^\gamma$, a contradiction. Hence $J_1 = \{1\}$, so $|J_i| = 1$ for all i and $H \cap N = S_1 \times \cdots \times S_t = N$. We conclude that $G = H = \langle n, g_1, \dots, g_d \rangle$.

We have shown that $\langle n, g_1, \dots, g_d \rangle = G$ for all $g_1, \dots, g_d \in G$ such that $\langle g_1, \dots, g_d \rangle N = G$. Thus no minimal generating set for G contains both n and $m := (y, 1, \dots, 1) \in N$. Consequently, one of n and m is a power of the other. This implies in particular that $\langle x, y \rangle$ is cyclic, contradicting $\langle x, y \rangle = S$. □

The restriction in the previous lemma concerning $\mathrm{O}_8^+(2)$ can be removed by a different argument. For this purpose we need the following lemma. In the next few results, we shall denote elements $h \in X \wr \mathrm{S}_t$ by $(\rho_1(h), \dots, \rho_t(h))\sigma(h)$, where ρ_i is the projection from the base group to the i-th copy of X and $\sigma(h) \in \mathrm{S}_t$.

Lemma 3.4. *Let X be a finite group, let a be an element of X, let $t \geqslant 2$, and let $\alpha := (a, a^2, 1, \dots, 1)$ and $\beta := (a, 1, \dots, 1)$ be elements of $X \wr \mathrm{S}_t$. Let Y be a subgroup of $X \wr \mathrm{S}_t$ and set $R := \langle \alpha, Y \rangle$ and $K := \langle \alpha, \beta, Y \rangle$. For any given $k \in K$ and $i \in \{1, \dots, t\}$, there exists $r \in R$ such that $\rho_i(r) = \rho_i(k)$ and $\sigma(r) = \sigma(k)$.*

Proof. Let $A := \langle \alpha \rangle$ and $B := \langle \beta \rangle$. Any element $k \in K$ can be written in the form $k = z_1 \cdots z_\ell$ with $z_i \in A \cup B \cup Y$. We prove the statement by induction on ℓ. First assume $\ell = 1$. If $k = z_1 \in Y \cup A$, we set $r = k$. If $k = z_1 = \beta^m \in B$, we set $r = \alpha^m$ if $i = 1$, and $r = 1$ otherwise.

Now assume $\ell > 1$ and set $k^* = z_2 \cdots z_\ell$. We have $\sigma(k) = \sigma(z_1)\sigma(k^*)$ and $\rho_i(k) = \rho_i(z_1)\rho_{i\sigma(z_1)}(k^*)$. By induction, for each i there exist $r_1, r_2 \in R$ such that $\sigma(r_1) = \sigma(z_1)$, $\sigma(r_2) = \sigma(k^*)$, $\rho_i(r_1) = \rho_i(z_1)$, and $\rho_{i\sigma(z_1)}(r_2) = \rho_{i\sigma(z_1)}(k^*)$. The element $r = r_1 r_2$ satisfies the required properties. □

Lemma 3.5. *Suppose that $\Phi(G) = 1$, and that G has a non-abelian minimal normal subgroup N. Then N is simple.*

Proof. We have $N = S_1 \times \cdots \times S_t$, with $S_i \cong S$ a non-abelian finite simple group. By Lemma 3.3, we may assume that $S = \mathrm{O}_8^+(2)$. In particular, S contains an element a of order four.

Assume for a contradiction that $t \geqslant 2$, and let $\alpha := (a, a^2, 1, \dots, 1)$ and $\beta := (a, 1, \dots, 1)$. Suppose that $G = \langle \alpha, \beta, g_1, \dots, g_d \rangle$ for some $g_1, \dots, g_d \in G$, and let $Y := \langle g_1, \dots, g_d \rangle$ and $R := \langle \alpha, g_1, \dots, g_d \rangle$. We apply Lemma 3.4 to

$RC_G(N)/C_G(N)$ and $G/C_G(N) \leqslant \mathrm{Aut}(N) = \mathrm{Aut}(S) \wr \mathrm{S}_t$, with the element $(s, s, \dots, s)C_G(N) \in G/C_G(N)$, for an arbitrary $s \in S$, with $i = 1$. We deduce that there exist $\gamma_2, \dots, \gamma_t \in \mathrm{Aut}(S)$ such that $(s, \gamma_2, \dots, \gamma_t)C_G(N) \in RC_G(N)$.

Let π_1 be the projection from N to S_1. Since S is non-abelian simple and $\alpha \in R \cap N \trianglelefteq R$, we deduce that $\pi_1(R \cap N) = S$. Since $RN = G$, the action of R on $S_1, \dots, S_t$ is transitive and consequently, arguing as in the proof of Lemma 3.3, we see that $R \cap N = \Delta_1 \times \cdots \times \Delta_u$, where $\Delta_i := \{(s^{\alpha_{i1}}, \dots, s^{\alpha_{iv}}) \mid s \in S\}$ is a diagonal subgroup of $S_{j_{i_1}} \times \cdots \times S_{j_{i_v}}$ and each $\alpha_{ik} \in \mathrm{Aut}(S)$. On the other hand, $\alpha \in R \cap N$, so the order of a implies that $v = 1$, hence $R \cap N = N$ and $R = RN = G$. This implies that α and β are dependent, a contradiction since neither of α and β is a power of the other. □

Lemma 3.6. *Let N_1 and N_2 be two distinct minimal normal subgroups of a finite group X, and let $a \in N_1$ and $b \in N_2$. If ab and b are independent in X, then there exists an isomorphism $\phi : N_1 \to N_2$ such that $\phi(a) = b$, and such that ϕ is an X-isomorphism if N_1 is abelian.*

Proof. Assume that ab and b are independent, and let $\{ab, b, x_1, \dots, x_d\}$ be a minimal generating set for X. Additionally, let $H := \langle ab, x_1, \dots, x_d\rangle$, so $H \neq X$. We have $b = a^{-1}(ab) \in N_2 \cap HN_1$ and therefore $X = \langle H, b\rangle = HN_1 = HN_2$. Moreover $H \cap N_1$ is normalized by H and centralized by N_2, so $H \cap N_1$ is normal in $X = HN_2$ and therefore $H \cap N_1 = 1$. Similarly $H \cap N_2 = 1$, so H is a common complement of N_1 and N_2 in X. In particular, for any n in N_1 there exists a unique n^* in N_2 such that $nn^* \in H$, and since $[N_1, N_2] = 1$, the map $\phi : N_1 \to N_2$ sending n to n^* is an isomorphism. Now $ab \in H$, so $\phi(a) = b$.

Suppose now that N_1 is abelian, and let $n \in N_1$ and $x \in X$. Then $x = n'h$ for some $n' \in N_1$ and $h \in H$. As $[N_1, N_1] = 1 = [N_1, N_2]$, we see that $(nn^*)^x = (nn^*)^h \in H$. Thus $\phi(n^x) = (n^*)^x = \phi(n)^x$, and so ϕ is an X-isomorphism. □

Lemma 3.7. *The group G contains at most one non-abelian minimal normal subgroup.*

Proof. If $\Phi(G) \neq 1$ then the result is immediate from Proposition 3.1, so assume $\Phi(G) = 1$. Assume further, for a contradiction, that N_1 and N_2 are distinct non-abelian minimal normal subgroups of G. By Lemma 3.5, N_1 and N_2 are simple. Therefore, there exist $a \in N_1$ and $b \in N_2$ such that $|a| = |b| \neq 1$.

Since neither of ab and b is a power of the other, they are independent and therefore, by Lemma 3.6, there exist a non-abelian simple group S with $N_1 \cong N_2 \cong S$, and an element $\phi \in \mathrm{Aut}(S)$ such that $b = \phi(a)$. So S is a non-abelian simple group such that all elements of the same order are conjugate in its automorphism group. By [61, Thm. 3.1], $S \in \{\mathrm{L}_2(5), \mathrm{L}_2(7), \mathrm{L}_2(8), \mathrm{L}_2(9), \mathrm{L}_3(4)\}$.

Assume that S contains an element a of order p^2, for some prime p, and consider (a, a^p) and $(1, a^p)$ in $N_1 \times N_2$. Neither of these elements is a power of the other, so they are independent, contradicting Lemma 3.6. So S contains no elements of order p^2, and therefore $S \cong \mathrm{L}_2(5) \cong \mathrm{A}_5$.

Here, we consider an element u of order 5 in S and an involution t in $\mathrm{N}_S(\langle u\rangle)$. Then $M := \langle t, u\rangle$ is isomorphic to the dihedral group of order 10, and is the unique maximal subgroup of S containing u. Let $x := (t, u), y := (1, t) \in N_1 \times N_2 \cong S^2$. Neither of x and y is a power of the other, so they are independent.

Let $\{x, y, g_1, \ldots, g_d\}$ be a minimal generating set for G, and define $H := \langle x, g_1, \ldots, g_d\rangle$. We have $HN_2 = G$, since $y \in N_2$. Let $X := HN_1 \cap N_1N_2$. Now $(t, u) \in H$ and $(t^{-1}, 1) \in N_1$, so $(1, u) \in HN_1 \cap N_1N_2 = X$. Furthermore, $\langle(1, t), (1, u)\rangle N_1$ is the unique maximal subgroup of N_1N_2 that contains $\langle(1, u), N_1\rangle$, so if $X \neq N_1N_2$, then $X \leqslant \langle(1, t), (1, u)\rangle N_1$. But then y normalizes X and consequently $X \trianglelefteq G$, contradicting the minimality of N_2.

Thus $X = N_1N_2 \leqslant HN_1$ and using Dedekind's modular law and $HN_2 = G$ we see that

$$(H \cap N_1N_2)N_1 = N_1N_2 = (H \cap N_1N_2)N_2.$$

In particular $H \cap N_1N_2$ is a subdirect product of $N_1N_2 \cong \mathrm{A}_5^2$. If $N_1N_2 \leqslant H$, then $G = N_1N_2\langle g_1, \ldots, g_d\rangle \leqslant H$, a contradiction. Hence $H \cap N_1N_2 = \{(s, s^\phi) \mid s \in S\}$ for some $\phi \in \mathrm{Aut}(S)$, but this contradicts $(t, u) \in H \cap N_1N_2$. □

In the following, we write $F(G)$ for the Fitting subgroup of G (the largest normal nilpotent subgroup of G), $E(G)$ for the subgroup of G generated by all quasisimple subnormal subgroups of G, and $F^*(G)$ for the generalized Fitting subgroup of G (the subgroup generated by $F(G)$ and $E(G)$).

Corollary 3.8. *If G is insoluble, then:*

(i) *$E(G)$ is a non-abelian simple group; and*
(ii) *$G/E(G)$ is soluble.*

Proof. The Frattini subgroup of G is trivial, otherwise, by Proposition 3.1, G would be nilpotent. This implies that all quasisimple subnormal subgroups of G are simple, and so $\mathrm{soc}(G) = F^*(G) = E(G) \times F(G)$. Moreover $C_G(\mathrm{soc}(G)) = F(G)$, and we may write $F(G) = N_1 \times \cdots \times N_t$ as a product of abelian minimal normal subgroups of G.

By Lemma 3.2, for $1 \leqslant i \leqslant t$, $N_i \cong C_{p_i}$ for a suitable prime p_i and therefore

$$G/C_G(F(G)) \cong G/\bigcap_{1\leqslant i\leqslant t} C_G(N_i) \leqslant \prod_{1\leqslant i\leqslant t} G/C_G(N_i) \leqslant \prod_{1\leqslant i\leqslant t} \mathrm{Aut}(C_{p_i})$$

is abelian. If $E(G) = 1$, then $\mathrm{soc}(G) = F(G)$, so $C_G(F(G)) = F(G)$ and G is metabelian, a contradiction. Hence G contains a non-abelian minimal normal subgroup and so by Lemmas 3.5 and 3.7, $E(G)$ is a non-abelian simple group S. Therefore,

$$G/F(G) = G/C_G(\mathrm{soc}(G)) = G/(C_G(S) \cap C_G(F(G)) \leqslant G/C_G(S) \times G/C_G(F(G)).$$

Since $G/C_G(S)$ is almost simple with socle isomorphic to S, and $G/C_G(F(G))$ is abelian, we conclude that $S = E(G)$ is the unique non-abelian composition factor of G and therefore $G/E(G)$ is soluble. □

We now show that in an insoluble group with the independence property, certain elements are dependent, and so in particular must commute.

Lemma 3.9. *Suppose that G is insoluble and let $S = E(G)$ be the unique non-abelian minimal normal subgroup of G. Suppose in addition that there exist $x, s \in S$ such that $xC_G(S)$ and $sC_G(S)$ are dependent in $G/C_G(S)$. Then x and s are dependent, and in particular they commute.*

Proof. Let $\overline{G} := G/C_G(S)$, and, for all $g \in G$, let $\overline{g} := gC_G(S)$. Assume for a contradiction that $\{x, s, g_1, \ldots, g_t\}$ is a minimal generating set for G. We may order the indices so that, for some r, the subset $\{g_1, \ldots, g_r\}$ of $\{g_1, \ldots, g_t\}$ is minimal, subject to $\overline{G} = \langle \overline{x}, \overline{s}, \overline{g}_1, \ldots, \overline{g}_r \rangle$. It follows that there exists $z \in \{x, s\}$ such that $\overline{G} = \langle \overline{z}, \overline{g}_1, \ldots, \overline{g}_r \rangle$.

Let $R := \langle z, g_1, \ldots, g_t \rangle$. Clearly $G = S\langle z, g_1, \ldots, g_t \rangle = RS$. If $R \cap S = 1$, then $R \cong G/S$ is soluble by Corollary 3.8, contradicting $RC_G(S)/C_G(S) = \overline{G}$. Thus $R \cap S$ is a non-trivial and normalized by $RC_G(S) = G$, and consequently $S = R \cap S$ and $G = R$, contradicting the fact that $\{x, s, g_1, \ldots, g_t\}$ is a minimal generating set for G. Hence x and s are dependent, so $\langle x, s \rangle$ is cyclic. $\square$

Recall that for a group X and an element $x \in X$, we write $\mathcal{M}_X(x)$ for the set of maximal subgroups of X containing s.

Lemma 3.10. *Let X be a finite group and let $x, y \in X$ be such that $y \in \cap_{M \in \mathcal{M}_X(x)} M$. Then no minimal generating set for X contains $\{x, y\}$.*

Proof. Suppose, for a contradiction, that there exist $g_1, \ldots, g_d \in X$ such that $\{x, y, g_1, \ldots, g_d\}$ is a minimal generating set for X. Then $\langle x, g_1, \ldots, g_d \rangle \neq X$, so there exists $M \in \mathcal{M}_X(x)$ such that $\langle x, g_1, \ldots, g_d \rangle \leqslant M$. By assumption, $y \in M$, so $X = \langle x, y, g_1, \ldots, g_d \rangle \leqslant M$, a contradiction. $\square$

Finally, we reach the main result of this section. Recall that G is assumed to be a finite group that satisfies the independence property.

Theorem 3.11. *The group G is supersoluble.*

Proof. First assume that G is insoluble, so that $S := E(G)$ is non-abelian simple by Corollary 3.8. Let $H \cong G/C_G(S)$. By Theorem 3, $\mathrm{soc}(H) \cong S$ contains two non-commuting elements $xC_G(S)$ and $sC_G(S)$ with the property that every maximal subgroup of H containing $sC_G(S)$ also contains $xC_G(S)$. Furthermore, since $S \cap C_G(S) = 1$, we can choose the corresponding x, s to lie in $E(G)$. By Lemma 3.10, no minimal generating set for H contains $\{xC_G(S), C_G(S)\}$, that is, $xC_G(S)$ and $yC_G(S)$ are dependent in H. But then, by Lemma 3.9, s and x must commute, a contradiction. So G is soluble.

If $\Phi(G) \neq 1$ then G is nilpotent, by Proposition 3.1, so assume otherwise. By Lemma 3.2, $F(G) = N_1 \times \cdots \times N_u$ is a direct product of minimal normal subgroups of prime order, and $G/F(G) \leqslant \prod_{1 \leqslant i \leqslant u} \mathrm{Aut}(N_i)$ is abelian, hence G is supersoluble. $\square$

4. Supersoluble groups with the independence property

In this section we shall determine the structure of the finite supersoluble groups G satisfying the independence property. By Proposition 3.1, we may restrict our attention to the case $\Phi(G) = 1$. This implies that the Fitting subgroup $\mathrm{Fit}(G)$ of G is a direct product of minimal normal subgroups of G, and is complemented in G. Let K be a complement of $\mathrm{Fit}(G)$ in G. Since G is supersoluble, $G' \leqslant \mathrm{Fit}(G)$, and consequently K is abelian. Let W be a complement of $Z(G)$ in $\mathrm{Fit}(G)$. Then $G = W \rtimes H$, with $H = \langle K, Z(G) \rangle$.

Moreover, by Lemma 3.2, each minimal normal subgroup of G is cyclic (of prime order). As a consequence, we assume through this section that

$$G = (V_1^{\delta_1} \times \cdots \times V_r^{\delta_r}) \rtimes H,$$

where H is abelian, $\delta_1, \ldots, \delta_r$ are positive integers, and $V_1, \ldots, V_r$ are irreducible H-modules of prime order that are pairwise non-H-isomorphic, such that H acts non-trivially on each. (So if G is abelian then $r = 0$ and $G = H$.) For each $i \in \{1, \ldots, r\}$, we set

$$p_i := |V_i|, \quad W_i := V_i^{\delta_i}, \quad \text{and} \quad W := V_1^{\delta_1} \times \cdots \times V_r^{\delta_r} = W_1 \times \cdots \times W_r.$$

Observe now that, for each h in H, there exists an $\alpha_i(h) \in \mathbb{F}_{p_i}^{\times}$ such that $w^h = \alpha_i(h)w$ for all $w \in W_i$.

Notation 4.1. Let $g_1 := h_1(w_{1,1}, \ldots, w_{1,r}), \ldots, g_t := h_t(w_{t,1}, \ldots, w_{t,r})$ be elements of G, with $h_i \in H$ and $w_{i,j} := (x_{i,j,1}, \ldots, x_{i,j,\delta_j}) \in W_j$. For each $j \in \{1, \ldots, r\}$, we define a matrix $A^{(j)} = A^{(j)}(g_1, \ldots, g_t)$ whose columns are $a_1^{(j)}, \ldots, a_t^{(j)}$, where for each $i \in \{1, \ldots, t\}$ the transpose of $a_i^{(j)}$ is

$$(1 - \alpha_j(h_i), x_{i,j,1}, x_{i,j,2}, \ldots, x_{i,j,\delta_j}) \in \mathbb{F}_{p_j}^{\delta_j+1}.$$

Lemma 4.2. *Let $g_1, \ldots, g_t$ be as in Notation 4.1. Then $G = \langle g_1, \ldots, g_t \rangle$ if and only if $\langle h_1, \ldots, h_t \rangle = H$ and $\operatorname{rank}(A^{(j)}) = \delta_j + 1$ for all $j \in \{1, \ldots, r\}$.*

Proof. See Propositions 2.1 and 2.2 in [43]. □

Lemma 4.3. *Suppose that G satisfies the independence property. Then the following statements hold.*

(i) *If $\delta_i = 1$, then $|H/C_H(V_i)|$ is prime.*
(ii) *If $|V_i| = |V_j|$, then $i = j$.*
(iii) $(|H|, |W|) = 1$.

Proof. For (i), notice first that by assumption, $|H/C_H(V_i)| > 1$. Assume for a contradiction that $\delta_i = 1$ but $|H/C_H(V_i)|$ is not prime, and choose $h \in H$ such that $|hC_H(V_i)|$ is prime. Take $0 \neq x \in V_i = W_i$, and let $g_1 := h = h(0, 0, \ldots, 0)$ and $g_2 := hx = h(0, \ldots, 0, x, 0, \ldots, 0)$ (with x in position i). Since $h \notin C_H(V_i)$, the elements g_1 and g_2 do not commute, so neither is a power of the other. Furthermore, $\langle g_1, g_2 \rangle \neq G$. Since G satisfies the independence property, g_1 and g_2 are therefore independent, so there exist $g_3, \ldots g_t \in G$ such that $\{g_1, g_2, g_3, \ldots, g_t\}$ is a minimal generating set for G. Using Notation 4.1, since $\langle h_1, h_2, h_3, \ldots, h_t \rangle = \langle h, h_3, \ldots, h_t \rangle$ and $\langle h, C_H(V_i) \rangle \neq H$, there exists $k \geqslant 3$ such that $h_k \notin C_H(V_i)$. Since $\delta_i = 1$, the matrix $A^{(i)} = A^{(i)}(g_1, \ldots, g_t)$ has two rows. From $h_k \notin C_H(V_i)$ we deduce that $1 - \alpha_i(h_k) \neq 0$, so there exists an $\ell \in \{1, 2\}$ such that the columns $a_\ell^{(i)}$ and $a_k^{(i)}$ of $A^{(i)}$ are linearly independent. Moreover, if $j \neq i$ then $a_1^{(j)} = a_2^{(j)}$. It follows from Lemma 4.2 that $\langle g_\ell, g_3, \ldots, g_m \rangle = G$, a contradiction. This proves (i).

For (ii), assume for a contradiction that $|V_i| = |V_j|$ for distinct i and j, and let $a \in V_i \setminus \{0\}$ and $b \in V_j \setminus \{0\}$, so that $|a| = |b|$. Then ab and b are independent in G, and hence Lemma 3.6 shows that there is a G-isomorphism, and hence an H-isomorphism, between V_i and V_j, a contradiction.

For (iii), assume, for a contradiction, that p_i divides $|H|$ for some $i \in \{1, \dots, r\}$. Fix $v \in V_i$ and $h \in H$ with $|h| = |v| = p_i$. Neither of $g_1 := h$ and $g_2 := hv$ is a power of the other, so there exist $g_3, \dots, g_t \in G$ such that $\{g_1, g_2, g_3, \dots, g_t\}$ is a minimal generating set for G. The condition $|h| = |v| = p_i$ implies that $h \in C_H(V_i)$. With the notation of Notation 4.1, we notice that $\langle h_1, h_2, h_3, \dots, h_t\rangle = \langle h, h_3, \dots, h_t\rangle$, and if $j \neq i$ then $a_1^{(j)} = a_2^{(j)}$, and $a_1^{(i)}$ is zero. But then $\langle g_2, \dots, g_t\rangle = G$, a contradiction. □

The following example shows that three necessary conditions in Lemma 4.3 are not sufficient to ensure that G satisfies the independence property.

Example 4.4. Consider the group

$$G := (V_1 \times V_2^2) \rtimes (\langle x\rangle \times \langle y\rangle) \cong \mathrm{AGL}_1(3) \times (\mathbb{F}_5^2 \rtimes \langle 2I_2\rangle) \leqslant \mathrm{AGL}_1(3) \times \mathrm{AGL}_2(5),$$

so that $|V_1| = 3, |V_2| = 5, |x| = 4, |y| = 2$, $x \in C_G(V_1)$, $y \in C_G(V_2)$, $w^x = 2w$ for all $w \in V_2^2$ and $v^y = 2v$ for all $v \in V_1$. Observe that G satisfies Conditions (i)–(iii) of Lemma 4.3.

We claim that x^2y and y are dependent in G. To see this, suppose for a contradiction that $\{g_1, \dots, g_r, x^2y, y\}$ is a minimal generating set for G, and let $R := \langle g_1, \dots, g_r, x^2y\rangle$. It is not restrictive to assume that $g_1, \dots, g_r \in (V_1 \times V_2^2)\langle x\rangle$. Notice that $RV_1\langle y\rangle = G$, and therefore R contains xy^kv for some $k \in \mathbb{Z}$ and $v \in V_1$. However, $(xy^kv)^2 = x^2$, so $y \in R$, a contradiction. As x^2y and y generate distinct subgroups of order 2, the group G does not satisfy the independence property.

In the remainder of the section, we will determine some additional conditions. For this purpose we need some definitions. Let g_1 and g_2 be as in Notation 4.1. Then we say that g_1 and g_2 are *j-independent* for some $j \in \{1, \dots, r\}$ if either $\mathrm{rank}(A^{(j)}(g_1, g_2)) = 2$ or, for some ordering λ, μ of 1 and 2, the column $a_\lambda^{(j)} \neq 0$, $a_\mu^{(j)} = 0$, and $\langle h_\lambda\rangle\,\Phi(H) \neq \langle h_1, h_2\rangle\,\Phi(H)$.

Similarly, g_1 and g_2 are *$\{i, j\}$-independent* for distinct $i, j \in \{1, \dots, r\}$ if $\langle h_1\rangle\,\Phi(H) = \langle h_2\rangle\,\Phi(H)$ and for some ordering λ, μ of 1 and 2, the columns $a_\lambda^{(i)}$ and $a_\mu^{(j)}$ are non-zero, and $a_\lambda^{(j)} = a_\mu^{(i)} = 0$.

Lemma 4.5. *Assume that G satisfies the three conditions of Lemma 4.3. Two elements $g_1 = h_1(w_{1,1}, \dots, w_{1,r})$ and $g_2 = h_2(w_{2,1}, \dots, w_{2,r})$ are independent in G if and only if one of the following statements holds:*

(i) *h_1 and h_2 are independent in H;*
(ii) *there exists $j \in \{1, \dots, r\}$ such that g_1 and g_2 are j-independent; or*
(iii) *there exist distinct $i, j \in \{1, \dots, r\}$ such that g_1 and g_2 are $\{i, j\}$-independent.*

Proof. If G is abelian, i.e., if $G = H$, then (ii) and (iii) cannot hold, and (i) is equivalent to g_1 and g_2 being independent. Thus we will assume that G is non-abelian. We first show the sufficiency of each of the three conditions in turn, and then the necessity that at least one of them holds. While proving the sufficiency of each condition, we may assume that G is not equal to $\langle g_1, g_2\rangle$, as otherwise g_1 and g_2 are independent.

If h_1 and h_2 are independent in H, then for some $a \geqslant 2$ there exist $h_3, \ldots, h_a$ in H such that $\{h_1, h_2, h_3, \ldots, h_a\}$ is a minimal generating set for H. Then we take $v_1, \ldots, v_b \in W$ such that $\{v_1, \ldots, v_b\}$ is minimal, subject to

$$\{g_1, g_2, h_3, \ldots, h_a, v_1, \ldots, v_b\}$$

being a generating set for G. In this way we obtain a minimal generating set for G containing g_1 and g_2.

Next suppose that g_1 and g_2 are j-independent for a fixed j. First, let $A := A^{(j)}(g_1, g_2)$, and assume that $\mathrm{rank}(A) = 2$. Let $\{h_3, \ldots, h_m\}$ be a subset of H of minimal cardinality, subject to $m \geqslant \delta_j + 1$ and $H = \langle h_1, h_2, h_3, \ldots, h_m \rangle$. Since H acts as scalars on V_j, the group $H/C_H(V_j)$ is cyclic, so we may choose $h_3, \ldots, h_m$ so that $\langle h_1, h_2, h_3, C_H(V_j) \rangle = H$ and $h_i \in C_H(V_j)$ if $i \geqslant 4$. If $\langle h_1, h_2, C_H(V_j) \rangle = H$ and $m \geqslant 3$, we can additionally require $h_3 \in C_H(V_j)$. Notice in particular that if $\delta_j = 1$, then $H/C_H(V_j)$ is assumed to be of prime order, so $\langle h_1, h_2, C_H(V_j) \rangle = H$ and either $m = 2$ or $h_3 \in C_H(V_j)$. If $m > 2$, then choose $z_{i,k} \in \mathbb{F}_{p_j}$ for $i \in \{3, \ldots, \delta_j + 1\}$ and $k \in \{1, \ldots, \delta_j\}$ such that

$$\mathrm{rank} \begin{pmatrix} 1 - \alpha_j(h_1) & 1 - \alpha_j(h_2) & 1 - \alpha_j(h_3) & 0 & \ldots & 0 \\ x_{1,j,1} & x_{2,j,1} & z_{3,1} & z_{4,1} & \cdots & z_{\delta_{j+1},1} \\ \vdots & \vdots & \vdots & \vdots & \ldots & \vdots \\ x_{1,j,\delta_j} & x_{2,j,\delta_j} & z_{3,\delta_j} & z_{4,\delta_j} & \cdots & z_{\delta_{j+1},\delta_j} \end{pmatrix} = \delta_j + 1,$$

which is possible since $\mathrm{rank}(A) = 2$. Set $g_i := h_i(z_{i,1}, \ldots, z_{i,\delta_j})$ for each $i \in \{3, \ldots, \delta_j + 1\}$, and $g_i := h_i$ for each $i \in \{\delta_j + 2, \ldots, m\}$. Additionally, let

$$Z_j := \prod_{i \in \{1,\ldots,r\} \setminus \{j\}} W_i.$$

Then, by Lemma 4.2, $\{g_1 Z_j, g_2 Z_j, g_3 Z_j, \ldots, g_m Z_j\}$ is a minimal generating set for G/Z_j and therefore there exist elements $g_{m+1}, \ldots, g_{m+\ell}$ of Z_j, for some ℓ, such that $\{g_1, g_2, g_3, \ldots, g_{m+\ell}\}$ is a minimal generating set for G.

Hence without loss of generality we may assume that $a_1^{(j)} \neq 0$, $a_2^{(j)} = 0$ and $\langle h_1 \rangle \Phi(H) \neq \langle h_1, h_2 \rangle \Phi(H)$. There exists a (possibly empty) subset $\{h_3, \ldots, h_\ell\}$ of H such that $\{h_2, h_3, \ldots, h_\ell\}$ is minimal subject to $\langle h_1, h_2, h_3, \ldots, h_\ell \rangle = H$. Since $H/C_H(V_j)$ is cyclic, we may choose $h_4, \ldots, h_\ell$ to lie in $C_H(V_j)$. Let $m := \max\{\ell, \delta_j + 2\}$ and set $h_i = 1$ for each $i \in \{\ell + 1, \ldots, m\}$. If $\alpha_j(h_1) = 1$ then $\alpha_j(h_3) \neq 1$, since H does not centralise V_j. Thus we may choose $z_{i,k} \in \mathbb{F}_{p_j}$ for $i \in \{3, \ldots, \delta_j + 2\}$ and $k \in \{1, \ldots, \delta_j\}$ such that

$$\mathrm{rank} \begin{pmatrix} 1 - \alpha_j(h_1) & 1 - \alpha_j(h_3) & 0 & \ldots & 0 \\ x_{1,j,1} & z_{3,1} & z_{4,1} & \cdots & z_{\delta_{j+2},1} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ x_{1,j,\delta_j} & z_{3,\delta_j} & z_{4,\delta_j} & \cdots & z_{\delta_{j+2},\delta_j} \end{pmatrix} = \delta_j + 1.$$

Set $g_i := h_i(z_{i,1}, \ldots, z_{i,\delta_j})$ for each $i \in \{3, \ldots, \delta_j + 2\}$, and $g_i := h_i$ for each $i \in \{\delta_j + 3, \ldots, m\}$. Then $\{g_1 Z_j, g_2 Z_j, g_3 Z_j, \ldots, g_m Z_j\}$ is a minimal generating set for G/Z_j and as in the previous case, there exist elements of Z_j that extend $\{g_1, g_2, g_3, \ldots, g_m\}$ to a minimal generating set for G.

Finally, for this direction of the proof, assume that g_1 and g_2 are $\{i,j\}$-independent for distinct i and j, so that $\langle h_1\rangle \Phi(H) = \langle h_2\rangle \Phi(H)$. Without loss of generality, $a_1^{(j)}$ and $a_2^{(i)}$ are non-zero, whilst $a_2^{(j)} = a_1^{(i)} = 0$. Let $B := \{h_3,\dots,h_m\}$ be a subset of H of minimal cardinality subject to $m \geqslant \max\{\delta_i,\delta_j\}+2$ and $H = \langle h_1, B\rangle = \langle h_2, B\rangle$. Without loss of generality, suppose that $\delta_i \leqslant \delta_j$. Let $C := C_G(V_i) \cap C_G(V_j)$. We shall split into two cases to place various assumptions on B and define associated matrices over $\mathbb{F}_{p_i}$ and $\mathbb{F}_{p_j}$, before concluding both cases of the proof.

Case (a): $\delta_j \geqslant 2$, or $\delta_i = \delta_j = 1$ and either G/C is cyclic or $\langle h_1,h_2\rangle \nleqslant C$. Since $H/C_H(V_j)$ and $H/C_H(V_i)$ are cyclic, if $\delta_j \geqslant 2$ then we may assume that $h_4,\dots,h_m$ lie in $C_H(V_i)$, and satisfy $h_k \in C\cap H$ if $k > 4$. Similarly, if $\delta_i = \delta_j = 1$, then $H/(C\cap H) \cong G/C$ is either cyclic or isomorphic to C_q^2 for some prime q (this is because $\langle h_1,h_2\rangle \nleqslant C$ is equivalent to $h_1,h_2 \notin C$), so we may assume in this case that $h_4,\dots,h_m \in C\cap H$. In all three cases, we may choose elements $z_{\ell,s,k} \in \mathbb{F}_{p_s}$ for $\ell \in \{3,\dots,m\}$, $s \in \{i,j\}$ and $k \in \{1,\dots,\delta_s\}$ such that

$$\operatorname{rank}\begin{pmatrix} 1-\alpha_s(h_{f(s)}) & 1-\alpha_s(h_3) & \dots & 1-\alpha_s(h_{\delta_s+2}) \\ x_{f(s),s,1} & z_{3,s,1} & \cdots & z_{\delta_s+2,s,1} \\ \vdots & \vdots & \cdots & \vdots \\ x_{f(s),s,\delta_s} & z_{3,s,\delta_s} & \cdots & z_{\delta_s+2,s,\delta_s} \end{pmatrix} = \delta_s + 1$$

for each s, where $f(j) := 1$ and $f(i) := 2$, and $z_{\ell,s,k} = 0$ $\ell > \delta_s + 2$.

Case (b): $\delta_i = \delta_j = 1$, G/C is not cyclic, and $\langle h_1,h_2\rangle \leqslant C$. Here, our assumptions on G imply that $H/(C\cap H) \cong C_q^2$ for some prime q. Hence we may assume that $h_3 \in C_H(V_i) \setminus C_H(V_j)$, $h_4 \in C_H(V_j) \setminus C_H(V_i)$, and $h_5,\dots,h_m \in C\cap H$. Since $h_1,h_2 \in C$, and $a_1^{(j)}$ and $a_2^{(i)}$ are non-zero by assumption, we observe that

$$\operatorname{rank}\begin{pmatrix} 1-\alpha_j(h_1) & 1-\alpha_j(h_3) \\ x_{1,j,1} & 0 \end{pmatrix} = \operatorname{rank}\begin{pmatrix} 1-\alpha_i(h_2) & 1-\alpha_i(h_4) \\ x_{2,i,1} & 0 \end{pmatrix} = 2.$$

We set $z_{k,s,1} := 0$ for all $k \in \{3,\dots,m\}$ and $s \in \{i,j\}$.

To conclude Cases (a) and (b), we set

$$g_k := h_k(z_{k,j,1},\dots,z_{k,j,\delta_j})(z_{k,i,1},\dots,z_{k,i,\delta_i})$$

for each $k \in \{3,\dots,m\}$, and let $Z_{i,j} := \prod_{k\neq i,j} W_k$. Then $G/Z_{i,j}$ has minimal generating set $\{g_1Z_{i,j}, g_2Z_{i,j}, g_3Z_{i,j},\dots,g_mZ_{i,j}\}$, and therefore there exist elements of $Z_{i,j}$ that extend $\{g_1,\dots,g_m\}$ to a minimal generating set for G, as required.

For the converse direction, suppose that h_1, and h_2 are dependent in H, and that there is no $j \in \{1,\dots,r\}$ such that g_1 and g_2 are j-independent and no 2-set $\{i,j\}$ such that g_1 and g_2 are $\{i,j\}$-independent. Assume, for a contradiction, that $\{g_1,g_2,g_3,\dots,g_d\}$ is a minimal generating set for G, with $d \geqslant 2$. We may assume that $h_2 = h_1^t f$ with $t \in \mathbb{Z}$ and $f \in \Phi(H)$, so in particular $H = \langle h_1,h_3,\dots,h_d\rangle$.

For each j, let $A^{(j)} := A^{(j)}(g_1,\dots,g_d)$ and let $B^{(j)}$ be the matrix obtained from $A^{(j)}$ by deleting its second column. Since g_1 and g_2 are j-dependent, columns $a_1^{(j)}$ and $a_2^{(j)}$ are linearly dependent. If $a_2^{(j)} = 0$ whenever $a_1^{(j)} =$

0, then $\mathrm{rank}(A^{(j)}) = \mathrm{rank}(B^{(j)})$ for all j, and therefore $G = \langle g_1, g_3, \dots, g_d\rangle$ by Lemma 4.2, a contradiction. So there exists a k such that $a_1^{(k)} = 0$ and $a_2^{(k)} \neq 0$. Since g_1 and g_2 are k-dependent, $\langle h_2\rangle\,\Phi(H) = \langle h_1, h_2\rangle\,\Phi(H) = \langle h_1, h_1^t f\rangle\,\Phi(H) = \langle h_1\rangle\,\Phi(H)$. In particular $H = \langle h_2, h_3, \dots, h_d\rangle$ and as before we can conclude that there exists an ℓ such that $a_2^{(\ell)} = 0$ and $a_1^{(\ell)} \neq 0$. But then g_1 and g_2 are $\{k, \ell\}$-independent, a contradiction. $\square$

In what follows, we let $I_h := \{i \in \{1, \dots, r\} \mid h \in C_H(V_i)\}$ for $h \in H$, and set $F := \Phi(H)$.

Corollary 4.6. *Assume that G satisfies the three conditions of Lemma 4.3, and let $x, y \in H$ be such that $y \in \langle x\rangle F$ and $I_x \subseteq I_y$. Then x and y are dependent in G. If, in addition, G satisfies the independence property and $I_x \neq \varnothing$, then $y \in \langle x\rangle$.*

Proof. If $G = H$, then the result is clear, so assume that $r \geqslant 1$. For each $j \in \{1, \dots, r\}$, let $A^{(j)} := A^{(j)}(x, y)$. Clearly $\mathrm{rank}(A^{(j)}) \leqslant 1$ for every j. Notice that $a_1^{(j)} = 0$ if and only if $x \in C_H(V_j)$, and $a_2^{(j)} = 0$ if and only if $y \in C_H(V_j)$. In particular, since $I_x \subseteq I_y$, if $a_1^{(j)} = 0$ then $a_2^{(j)} = 0$. This, together with $\langle x, y\rangle F = \langle x\rangle F$, implies that x and y are j-dependent for all j, and $\{j_1, j_2\}$-dependent for all 2-subsets $\{j_1, j_2\}$. The result now follows from Lemma 4.5.

Assume now in addition that G satisfies the independence property and that $I_x \neq \varnothing$. Let $k \in I_x \cap I_y$, $0 \neq v \in V_k$, and for $j \in \{1, \dots, r\}$ let $\tilde{A}^{(j)} := A^{(j)}(xv, y)$, with columns $\tilde{a}_1^{(j)}$ and $\tilde{a}_2^{(j)}$. Then $\tilde{a}_1^{(k)} \neq 0$, $\tilde{a}_2^{(k)} = 0$, and $\tilde{A}^{(j)} = A^{(j)}$ if $j \neq k$. Thus, arguing as before, we conclude that xv and y are dependent, and consequently one of xv and y is a power of the other. As $H \cap V_k$ is trivial, we deduce that $y \in \langle xv\rangle$, and in fact $y \in \langle x\rangle$. $\square$

Thus if G satisfies the independence property, then Conditions (a)–(d) of Theorem 5(iii) hold. The following result completes the proof of Theorem 5.

Proposition 4.7. *Assume that G satisfies Conditions (a)–(d) of Theorem 5(iii). Then G satisfies the independence property.*

Proof. Let $g_1 := h_1 w_1$ and $g_2 := h_2 w_2$ be elements, as in Notation 4.1, that are dependent in G. We shall prove that one of g_1 and g_2 is a power of the other.

By Lemma 4.5, the fact that g_1 and g_2 are dependent in G implies that h_1 and h_2 are dependent in H. We may therefore assume throughout the proof that $h_2 = h_1^u f$ for some $u \in \mathbb{Z}$ and $f \in F$. If $r = 0$ then $G = H$, and so $F = 1$ and $g_2 = g_1^u$, as required. Hence we may assume that $r \geqslant 1$.

For $1 \leqslant j \leqslant r$, consider the matrix $A^{(j)} := A^{(j)}(g_1, g_2)$. We shall repeatedly use the fact that

$$\mathrm{rank}(A^{(j)}) < 2 \text{ for all } j \in \{1, \dots, r\},$$

since otherwise g_1 and g_2 are j-independent, and hence by Lemma 4.5 are independent, a contradiction. Note that that lemma's proof uses Condition (a).

By conjugating g_1 and g_2 by a common element of W, if necessary, we may assume that $w_{1,j} = 0$ whenever $j \notin I_{h_1}$. Hence if $j \notin I_{h_1}$ then $w_{2,j} = 0$, and otherwise $\mathrm{rank}(A^{(j)}) = 2$. Thus if $I_{h_1} = \varnothing$, then $g_1 = h_1$ and $g_2 = h_2$, and the result follows from Condition (d). If $I_{h_2} = \varnothing$, then we reach the same conclusion by a similar argument, corresponding to conjugation by a different element of W. Therefore, we shall assume for the remainder of the proof that $I_{h_1}, I_{h_2} \neq \varnothing$, and that $w_{1,j} = w_{2,j} = 0$ whenever $j \notin I_{h_1}$. We distinguish between two possibilities.

Case (a): $\langle h_2 \rangle F \neq \langle h_1, h_2 \rangle F$. Since g_1 and g_2 are j-dependent for all $j \in \{1, \ldots, r\}$, if $a_1^{(j)} = 0$ then $a_2^{(j)} = 0$. Fix $k \in I_{h_1}$, so that $a_1^{(k)} = (0, w_{1,k})^T$. If $w_{1,k} = 0$, then $a_1^{(k)} = 0$ and consequently $a_2^{(k)} = 0$, yielding $k \in I_{h_2}$. If $w_{1,k} \neq 0$ and $k \notin I_{h_2}$, then $\operatorname{rank}(A^{(k)}) = 2$, a contradiction. So $I_{h_1} \subseteq I_{h_2}$.

Letting $\mathcal{C}_1 := \{j \in I_{h_1} \mid w_{1,j} \neq 0\}$ and $\mathcal{C}_2 := \{j \in I_{h_1} \mid w_{2,j} \neq 0\}$, we see that $\mathcal{C}_2 \subseteq \mathcal{C}_1$, $w_1 = \prod_{j \in \mathcal{C}_1} w_{1,j}$, and $w_2 = \prod_{j \in \mathcal{C}_2} w_{2,j}$. Since $|V_1|, \ldots, |V_t|$ are pairwise coprime by Condition (b), and since $\operatorname{rank}(A^{(j)}) < 2$ for each j, it follows that $w_2 = w_1^\ell$ for some $\ell \in \mathbb{Z}$. We also deduce from Condition (d) that $h_2 = h_1^t$ for some $t \in \mathbb{Z}$. Since $(|W|, |H|) = 1$ by Condition (c), there exists $s \in \mathbb{Z}$ such that $s \equiv t \mod |H|$ and $s \equiv \ell \mod |W|$, and so $g_2 = w_2 h_2 = w_1^\ell h_1^t = w_1^s h_1^s = g_1^s$.

Case (b): $\langle h_1 \rangle F = \langle h_2 \rangle F$, so that $h_1 \in \langle h_2 \rangle F$ and $h_2 \in \langle h_1 \rangle F$. Assume first that there exist $j \in I_{h_1} \setminus I_{h_2}$ and $k \in I_{h_2} \setminus I_{h_1}$. If $a_1^{(j)} \neq 0$ then $\operatorname{rank}(A^{(j)}) = 2$, a contradiction. So $a_1^{(j)} = 0$, and similarly, $a_2^{(k)} = 0$. But then g_1, g_2 are $\{j, k\}$-independent, and therefore, by Lemma 4.5, independent in G, a contradiction.

We may therefore assume (by swapping g_1 and g_2 throughout the proof if necessary) that $\varnothing \neq I_{h_1} \subseteq I_{h_2}$, so that by Condition (d), $h_2 = h_1^t$ for some $t \in \mathbb{Z}$. Assume that $\Omega := I_{h_2} \setminus I_{h_1} \neq \varnothing$. For each $\omega \in \Omega$, we see that $a_1^{(\omega)} \neq 0$ and $a_2^{(\omega)} = 0$. Therefore if $k \in I_{h_1}$ and $w_{2,k} \neq 0$, then $w_{1,k} \neq 0$ (otherwise $a_2^{(k)}$ is non-zero, $a_1^{(k)} = 0$, and g_1 and g_2 are $\{\omega, k\}$-independent, a contradiction). We deduce that $w_2 = w_1^\ell$ for some $\ell \in \mathbb{Z}$, and as in Case (a), that $g_2 \in \langle g_1 \rangle$.

So we may assume that $I_{h_1} = I_{h_2} \neq \varnothing$. It follows from two applications of Condition (d) that $\langle h_1 \rangle = \langle h_2 \rangle$, $g_1 = h_1(\prod_{j \in I_{h_1}} w_{1,j})$, and $g_2 = h_2(\prod_{j \in I_{h_1}} w_{2,j})$. Let $\mathcal{C}_1 := \{j \in I_{h_1} \mid w_{1,j} \neq 0\}$ and $\mathcal{C}_2 := \{j \in I_{h_1} \mid w_{2,j} \neq 0\}$. If neither $\mathcal{C}_1 \subseteq \mathcal{C}_2$ nor $\mathcal{C}_2 \subseteq \mathcal{C}_1$, then g_1 and g_2 are $\{i, k\}$-independent for all $i \in \mathcal{C}_1 \setminus \mathcal{C}_2$ and $k \in \mathcal{C}_2 \setminus \mathcal{C}_1$, a contradiction. So without loss of generality $\mathcal{C}_2 \subseteq \mathcal{C}_1$, and we conclude again that g_2 is a power of g_1. $\square$

5. Groups satisfying the rank-independence property

The aim of this section is to classify the finite groups that satisfy the rank-independence property, so assume throughout this section that G is a finite group. Note that the proof of the following result uses the classification of finite simple groups.

Theorem 5.1 ([40])**.** *If N is a minimal normal subgroup of G with $N \neq G$, then $d(G) \leqslant d(G/N) + 1$.*

We can easily reduce to the supersoluble case. In the next proof, $\operatorname{Fit}(G)$ denotes the Fitting subgroup of G.

Proposition 5.2. *Assume that G satisfies the rank-independence property. Then G is supersoluble.*

Proof. If G is cyclic then the result is immediate, so assume otherwise. First we claim that $G/\Phi(G)$ is not simple, so assume otherwise for a contradiction. Since G is not cyclic, $G/\Phi(G)$ is a non-abelian simple group and therefore it contains two distinct involutions $x\,\Phi(G)$ and $y\,\Phi(G)$. But then $\langle x, y\rangle$ is not cyclic, so x and y are rank-independent. However, $\langle x, y\rangle\,\Phi(G)/\Phi(G)$ is dihedral, so in particular $\langle x, y\rangle$ is a proper subgroup of G, contradicting the fact that $d(G) = d(G/\Phi(G)) = 2$. Therefore $G/\Phi(G)$ is not simple.

Now let $N/\Phi(G)$ be a minimal normal subgroup of $G/\Phi(G)$. By Theorem 5.1, $d(G) = d(G/\Phi(G)) \leqslant d(G/N) + 1$. In particular, no two distinct elements of N are rank-independent, so every pair of such elements generates a cyclic group. It follows that no generating set for N of minimal size contains more than one element, i.e., N is cyclic. So $\mathrm{Fit}(G)/\Phi(G)$ is a direct product of cyclic minimal normal subgroups of $G/\Phi(G)$ and this implies that $G/\Phi(G)$ is supersoluble, and hence G is supersoluble. □

Lemma 5.3. *Assume that G satisfies the rank-independence property, and has a non-cyclic normal p-subgroup P. Then P is either elementary abelian or generalized quaternion.*

Proof. If $\Phi(P) = 1$, then P is elementary abelian, and the result is immediate, so let x be an element of $\Phi(P)$ of order p. Since $\Phi(P) \leqslant \Phi(G)$, the element x does not lie in any minimal generating set for G, and so $\langle x, y\rangle$ is cyclic for all $y \in G$. This implies in particular that $\langle x\rangle$ is the unique minimal subgroup of P. Since we are assuming that P is not cyclic, it follows from [50, Thm. 9.7.3] that P is a generalized quaternion group. □

Proposition 5.4. *Assume that G is a non-cyclic nilpotent group. Then G satisfies the rank-independence property if and only if one of the following holds:*

(i) $G \cong C_p \times C_p$;
(ii) $G \cong Q_8$;
(iii) $G \cong P \times C$, *with P an elementary abelian Sylow subgroup of G such that $d(P) \geqslant 3$, and C cyclic (this includes the case $|C| = 1$).*

Proof. It is easy to check that if G satisfies (i), (ii) or (iii), then G satisfies the rank-independence property. Conversely, suppose that G has the rank-independence property and let $d := d(G)$. There exists a prime p dividing $|G|$ such that the Sylow p-subgroup P of G satisfies $d(P) = d$. Let C be a p-complement in G. Distinct elements of C cannot belong to a generating set for G of cardinality d, so C is cyclic. If $d \geqslant 3$, then P is an elementary abelian p-group by Lemma 5.3. If $d = 2$, then each proper subgroup of G is cyclic, hence $G = P$ is isomorphic either to $C_p \times C_p$ or to Q_8. □

Proposition 5.5. *Assume that G is not nilpotent, and that $d(G) \geqslant 3$. Then G satisfies the rank-independence property if and only if $G = P \rtimes C$, where P is an elementary abelian Sylow p-subgroup of G and C is a cyclic group, acting on P as scalar multiplication.*

Proof. Assume that G satisfies the rank-independence property and set $F := \Phi(G)$. Since G is supersoluble,

$$G/F \cong (V_1^{\delta_1} \times \cdots \times V_r^{\delta_r}) \rtimes H$$

where H is abelian, $\delta_1, \dots, \delta_r$ are positive integers, and $V_1, \dots, V_r$ are pairwise non-H-isomorphic, irreducible H-modules on each of which H acts non-trivially. Moreover, $r > 0$ since G is not nilpotent, and for $i \in \{1, \dots, V_i\}$ the group V_i has prime order p_i. By Lemma 4.2,

$$d := d(G) = \max\{d(H), \delta_i + 1 \mid 1 \leqslant i \leqslant r\}. \tag{5.1}$$

Since $r \neq 0$, there exists a non-central minimal normal subgroup N/F of G/F. Since N is non-central, there exist $x \in N$ and $y \in G$ such that $[x, y] \neq 1$. Now $\langle x, y\rangle$ is not abelian, so there exist $z_3, \dots, z_d \in G$ such that $G = \langle x, y, z_3, \dots, z_d\rangle$. In particular, $G = N\langle y, z_3, \dots, z_d\rangle$ and hence $d(H) \leqslant d(G/N) \leqslant d-1$. It follows from (5.1) that $d = \delta_i + 1$ for some $i \in \{1, \dots, r\}$. We may assume that $i = 1$.

Set $V := V_1$, $p := p_1$, and $\delta := \delta_1 = d - 1$. We identify each element w of V^δ with an element $(x_1, \dots, x_\delta) \in \mathbb{F}_p^\delta$. Let $L = C/F$ be a complement of V^δ in G/F. For each ℓ in L, there exists an $\alpha(\ell) \in \mathbb{F}_p^\times$ such that $w^\ell = \alpha(\ell)w$ for all $w \in V^\delta$. Given $g_1, \dots, g_d \in G$, we shall write $g_iF = \ell_i(x_{i,1}, \dots, x_{i,\delta})$, with $x_{i,j} \in \mathbb{F}_p$. Consider the matrix

$$A = A(g_1, \dots, g_d) := \begin{pmatrix} 1-\alpha(\ell_1) & \cdots & 1-\alpha(\ell_d) \\ x_{1,1} & \cdots & x_{d,1} \\ \vdots & \cdots & \vdots \\ x_{1,\delta} & \cdots & x_{d,\delta} \end{pmatrix},$$

similar to Notation 4.1. It follows from Lemma 4.2 that $\langle g_1, \dots, g_d\rangle = G$ if and only if $\langle \ell_1, \dots, \ell_d\rangle = L$, and $\mathrm{rank}(A) = d$.

We now show that C is cyclic. Assume for a contradiction that there exist $g_1, g_2 \in C$ such that $\langle g_1, g_2\rangle$ is not cyclic. Since G satisfies the rank-independence property, there exist $g_3, \dots, g_d \in G$ such that $\langle g_1, \dots, g_d\rangle = G$. However the first two columns of the matrix $A = A(g_1, \dots, g_d)$ are linearly dependent, contradicting $\mathrm{rank}(A) = d$. Since C is cyclic, L is also cyclic and consequently $r = 1$, and so

$$G/F \cong V^\delta \rtimes H.$$

We show next that p does not divide $|H|$. Assume, for a contradiction, that there exists $y_1 \in G$ such that y_1F is an element of H of order p, and choose $y_2 \in G$ so that y_2F is a non-trivial element of V^δ. Then $K = \langle y_1, y_2\rangle F \cong (C_p \times C_p)F$ is a non-cyclic normal subgroup of G. As G has the rank-independence property, there exist $y_3, \dots, y_d \in G$ such that $G = \langle y_1, y_2, y_3, \dots, y_d\rangle$. However, this is not possible, since $d(G/K) = d(V^{\delta-1} \rtimes H/\langle y_1\rangle) > d - 2$. Hence $(p, |H|) = 1$.

Let P be a Sylow p-subgroup of G. From $(p, |H|) = 1$ we deduce that $P \cap C \leqslant F$. Moreover, P is a normal subgroup of G and $d(P) \geqslant \delta = d-1 \geqslant 2$, so, by Lemma 5.3, P is either elementary abelian or generalized quaternion. But in the second case, $|V| = 2$, contradicting the assumption that H acts non-trivially on V. Thus P is elementary abelian, and consequently $P \cap C \leqslant P \cap F = 1$. In particular $P \cong V^\delta$ and $G \cong V^\delta \rtimes C$, so p does not divide C.

Conversely, assume $G = P \rtimes C$, with $P \cong C_p^\delta$, $\delta \geqslant 2$, $(|C|, p) = 1$ and C acting on P as scalar multiplication. Since G is not nilpotent, C acts non-trivially on P. Additionally, $d := d(G) = \delta + 1$. We again apply Lemma 4.2. We identify each element of P with a vector $(y_1, \ldots, y_\delta) \in \mathbb{F}_p^\delta$. For each $c \in C$, there exists an $\alpha(c) \in \mathbb{F}_p^\times$ such that $y^c = \alpha(c)y$ for all $y \in P$. Let $g_1 := c_1(y_{1,1}, \ldots, y_{1,\delta}), g_2 := c_2(y_{2,1}, \ldots, y_{2,\delta}) \in G$, and suppose $\langle x \rangle = C$. If $\langle g_1, g_2 \rangle$ is not cyclic, then we may choose $y_3, y_4, \ldots, y_d \in \mathbb{F}_p^\delta$ in such a way that $\mathrm{rank}(A(g_1, g_2, xy_3, y_4, \ldots, y_d))$ is equal to d. Then by Lemma 4.2, $\langle g_1, g_2, xy_3, \ldots, y_d \rangle = G$, as required. □

Propositions 5.4 and 5.5 combine to prove Theorem 2. The following result completes the proof of Theorem 1.

Proposition 5.6. *Assume that G is not nilpotent, and that $d(G) = 2$. Then G satisfies the rank-independence property if and only if G is as described in Theorem 1(iii).*

Proof. The group G has the rank-independence property if and only if all proper subgroups of G are cyclic. The conclusion follows from the description of minimal non-abelian groups by Miller and Moreno in [46]. □

Acknowledgements. We are grateful to Peter Cameron for helpful discussions, and in particular for suggesting the problem of classifying the groups satisfying the rank-independence property; and to anonymous referees for helpful comments. The first author was supported by a St Leonard's International Doctoral Fees Scholarship and a School of Mathematics & Statistics PhD Funding Scholarship at the University of St Andrews. The fourth author would like to thank the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality during the programme "Groups, Representations and Applications: New perspectives", where work on this paper was undertaken. This work was supported by EPSRC grant no EP/R014604/1, and also partially supported by a grant from the Simons Foundation.

References

1. C. Acciarri and A. Lucchini. Graphs encoding the generating properties of a finite group. *Math. Nachr.*, 293(9):1644–1674, 2020.
2. Á. Bereczky. Maximal overgroups of Singer elements in classical groups. *J. Algebra*, 234(1):187–206, 2000.
3. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.
4. J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Math. Soc. Lecture Note Ser.* CUP, Cambridge, 2013.
5. T. Breuer. *The GAP Character Table Library, Version 1.3.1*, 2020.
6. T. Breuer, R. M. Guralnick, and W. M. Kantor. Probabilistic generation of finite simple groups. II. *J. Algebra*, 320(2):443–494, 2008.
7. T. C. Burness and M. Giudici. *Classical groups, derangements and primes*, volume 25 of *Aust. Math. Soc. Lecture Ser.* CUP, Cambridge, 2016.
8. T. C. Burness, R. M. Guralnick, and S. Harper. The spread of a finite group. *Ann. of Math. (2)*, 193(2):619–687, 2021.
9. T. C. Burness and S. Harper. On the uniform domination number of a finite simple group. *Trans. Amer. Math. Soc.*, 372(1):545–583, 2019.

10. S. Burris and H. P. Sankappanavar. *A course in universal algebra*. Grad. Texts in Math., vol. 78, Springer-Verlag, New York-Berlin, 1981.
11. A. A. Buturlakin and M. A. Grechkoseeva. The cyclic structure of maximal tori in finite classical groups. *Algebra Logika*, 46(2):129–156, 2007.
12. P. J. Cameron and P. Cara. Independent generating sets and geometries for symmetric groups. *J. Algebra*, 258(2):641–650, 2002.
13. P. J. Cameron and S. Ghosh. The power graph of a finite group. *Discrete Math.*, 311(13):1220–1222, 2011.
14. P. J. Cameron. The power graph of a finite group, II. *J. Group Theory*, 13(6):779–783, 2010.
15. P. J. Cameron, H. Guerra, and Š. Jurina. The power graph of a torsion-free group. *J. Algebraic Combinatorics*, 49(1):83–98, 2019.
16. P. J. Cameron and S. H. Jafari, On the connectivity and independence number of power graphs of groups. *Graphs Combin.*, 36(3):895–904, 2020.
17. P. J. Cameron and B. Kuzma. Between the enhanced power graph and the commuting graph. Preprint, 2020, arXiv:2012.03789.
18. P. J. Cameron, P. Manna, and R. Mehatari. On finite groups whose power graph is a cograph. *J. Algebra*, 591:59–74, 2022.
19. R. W. Carter. Conjugacy classes in the Weyl group. *Compositio Math.*, 25:1–59, 1972.
20. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. OUP, Eynsham, 1985.
21. G. De Franceschi. *Centralizers and conjugacy classes in finite classical groups*. PhD thesis, University of Auckland, 2018.
22. D. I. Deriziotis. Centralizers of semisimple elements in a Chevalley group. *Comm. Algebra*, 9(19):1997–2014, 1981.
23. A. A. Gal't. Strongly real elements in finite simple orthogonal groups. *Sibirsk. Mat. Zh.*, 51(2):241–248, 2010.
24. The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.
25. Z. Guangxiang. On self-normalizing cyclic subgroups. In *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, volume 47 of *Proc. Sympos. Pure Math.*, pp419–422. Amer. Math. Soc., Providence, RI, 1987.
26. R. Guralnick. On the number of generators of a finite group. *Arch. Math. (Basel)*, 53(6):521–523, 1989.
27. R. Guralnick and G. Malle. Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.*, 25(1):77–121, 2012.
28. R. Guralnick and G. Malle. Simple groups admit Beauville structures. *J. Lond. Math. Soc. (2)*, 85(3):694–721, 2012.
29. R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl. Linear groups with orders having certain large prime divisors. *Proc. London Math. Soc. (3)*, 78(1):167–214, 1999.
30. R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000.
31. R. M. Guralnick and G. Tracey. On elements of finite groups contained in a unique maximal subgroup. In preparation.
32. S. Harper. Flexibility in generating sets of finite groups. *Arch. Math. (Basel)*, 118(3):231–237, 2022.
33. C. Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order. *Geometriae Dedicata*, 2:425–460, 1974.
34. M. D. Hestenes. Singer groups. *Canadian J. Math.*, 22:492–513, 1970.
35. B. Huppert. Singer-Zyklen in klassischen Gruppen. *Math. Z.*, 117:141–150, 1970.
36. C. Jordan. Sur la limite de transitivité des groupes non alternés. *Bull. Soc. Math. France*, 1:40–71, 1872/73.
37. A. V. Kelarev and S. J. Quinn. A combinatorial property and power graphs of groups. In *Contributions to general algebra, 12 (Vienna, 1999)*, pages 229–235. Heyn, Klagenfurt, 2000.

38. P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Math. Soc. Lecture Note Ser.* CUP, Cambridge, 1990.
39. P. B. Kleidman. The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra*, 110(1):173–242, 1987.
40. A. Lucchini. Generators and minimal normal subgroups. *Arch. Math. (Basel)*, 64(4):273–276, 1995.
41. A. Lucchini. The independence graph of a finite group. *Monatsh. Math.*, 193(4):845–856, 2020.
42. A. Lucchini. Some questions on the number of generators of a finite group. *Rend. Sem. Mat. Univ. Padova*, 83:201–222, 1990.
43. A. Lucchini and A. Maróti. On the clique number of the generating graph of a finite group. *Proc. Amer. Math. Soc.*, 137(10):3207–3217, 2009.
44. G. Malle, J. Saxl, and T. Weigel. Generation of classical groups. *Geom. Dedicata*, 49(1):85–116, 1994.
45. G. Malle and D. Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics.* CUP, Cambridge, 2011.
46. G. A. Miller and H. C. Moreno. Non-abelian groups in which every subgroup is abelian. *Trans. Amer. Math. Soc.*, 4(4):398–404, 1903.
47. F. Nicolas. A simple, polynomial-time algorithm for the matrix torsion problem. Preprint, 2009, arXiv:0806.2068.
48. R. P. Panda, S. Dalal, and J. Kumar. On the enhanced power graph of a finite group. *Comm. Algebra*, 49(4):1697–1716, 2021.
49. C. E. Praeger. Primitive prime divisor elements in finite classical groups. In *Groups St. Andrews 1997 in Bath, II*, volume 261 of *London Math. Soc. Lecture Note Ser.*, pp605–623. CUP, Cambridge, 1999.
50. W. R. Scott. *Group theory.* Dover Publications, Inc., New York, second edition, 1987.
51. G. M. Seitz. On the subgroup structure of classical groups. *Comm. Algebra*, 10(8):875–885, 1982.
52. G. M. Tracey. Minimal generation of transitive permutation groups. *J. Algebra*, 509:40–100, 2018.
53. F. D. Veldkamp. Regular elements in anisotropic tori. In *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, pp389–424. Academic Press, New York, 1977.
54. G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Austral. Math. Soc.*, 3:1–62, 1963.
55. T. S. Weigel. Generation of exceptional groups of Lie type. *Geom. Dedicata*, 41(1):63–87, 1992.
56. H. Wielandt. *Finite permutation groups.* Academic Press, New York-London, 1964.
57. J. Whiston. Maximal independent generating sets of the symmetric group. *J. Algebra*, 232(1):255–268, 2000.
58. J. Whiston and J. Saxl. On the maximal size of independent generating sets of $PSL_2(q)$. *J. Algebra*, 258(2):651–657, 2002.
59. S. Zahirović. The power graph of a torsion-free group determines the directed power graph. *Discrete Appl. Math.*, 305:109–118, 2021.
60. S. Zahirović, I. Bošnjak, and R. Madarśz. A study of enhanced power graphs of finite groups. *J. Algebra Appl.*, 19(4):2050062, 2020.
61. J. P. Zhang. On finite groups all of whose elements of the same order are conjugate in their automorphism groups. *J. Algebra*, 153(1):22-–36, 1992.

Saul D. Freedman, School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, UK, email: sdf8@st-andrews.ac.uk

Andrea Lucchini, Università di Padova, Dipartimento di Matematica "Tullio Levi-Civita", Via Trieste 63, 35121 Padova, Italy, email: lucchini@math.unipd.it

Daniele Nemmi, Università di Padova, Dipartimento di Matematica "Tullio Levi-Civita", Via Trieste 63, 35121 Padova, Italy, email: dnemmi@math.unipd.it

Colva M. Roney-Dougal, School of Mathematics and Statistics, University of St Andrews, St Andrews, KY16 9SS, UK, email: colva.roney-dougal@st-andrews.ac.uk