Maximal subgroups of finite groups avoiding the elements of a generating set
MAXIMAL SUBGROUPS OF FINITE GROUPS
AVOIDING THE ELEMENTS OF A GENERATING SET

ANDREA LUCCHINI AND PABLO SPIGA

Abstract. We give an elementary proof of the following remark: if \( G \) is a finite group and \( \{g_1, \ldots, g_d\} \) is a generating set of \( G \) of smallest cardinality, then there exists a maximal subgroup \( M \) of \( G \) such that \( M \cap \{g_1, \ldots, g_d\} = \emptyset \). This result leads us to investigate the freedom that one has in the choice of the maximal subgroup \( M \) of \( G \). We obtain information in this direction in the case when \( G \) is soluble, describing for example the structure of \( G \) when there is a unique choice for \( M \). When \( G \) is a primitive permutation group one can ask whether it is possible to choose in the role of \( M \) a point-stabilizer. We give a positive answer when \( G \) is a 3-generated primitive permutation group but we leave open the following question: does there exist a (soluble) primitive permutation group \( G = \langle g_1, \ldots, g_d \rangle \) with \( d(G) = d > 3 \) and with \( \bigcap_{1 \leq i \leq d} \supp(g_i) = \emptyset \)? We obtain a weaker result in this direction: if \( G = \langle g_1, \ldots, g_d \rangle \) with \( d(G) = d \), then \( \supp(g_i) \cap \supp(g_j) \neq \emptyset \) for all \( i, j \in \{1, \ldots, d\} \).

1. Introduction

We start with a short and elementary proof of the following result:

**Theorem 1.1.** Let \( G \) be a finitely generated group and let \( d = d(G) \) be the smallest cardinality of a generating set of \( G \). If \( G = \langle g_1, \ldots, g_d \rangle \), then there exists a maximal subgroup \( M \) of \( G \) such that \( M \cap \{g_1, \ldots, g_d\} = \emptyset \).

**Proof.** If \( G \) is cyclic, that is, \( d \leq 1 \), the statement is clear. When \( d > 1 \), consider \( H = \langle g_1g_2, g_2g_3, \ldots, g_{d-1}g_d \rangle \). Since \( d(H) \leq d - 1 < d = d(G) \), we have \( H \neq G \). Let \( S \) be the family of the proper subgroups of \( G \) containing \( H \), and observe that \( S \) ordered by “set inclusion” is a non-empty partially ordered set. Let \( C \) be a non-empty chain in \( S \) and set \( K = \bigcup_{C \in C} C \). Clearly, \( K \) is a subgroup of \( G \) containing \( H \). Moreover, as \( G \) is finitely generated, it is easy to see that \( K \neq G \), that is, \( K \in S \). Thus every non-empty chain in \( S \) has a maximal element. By Zorn’s lemma, \( S \) has a maximal element \( M \) and, by construction, \( M \) is a maximal subgroup of \( G \) containing \( H \).

If \( g_i \in M \) and \( i \neq d \), then \( g_{i+1} = g_i^{-1}(g_ig_{i+1}) \in M \). Similarly, if \( g_i \in M \) and \( i \neq 1 \), then \( g_{i-1} = (g_{i-1}g_i)g_i^{-1} \in M \). Thus \( M \cap \{g_1, \ldots, g_d\} \neq \emptyset \) implies \( G = \langle g_1, \ldots, g_d \rangle \leq M \), a contradiction. \( \square \)

Theorem 1.1 does not remain true if we drop the assumption \( d = d(G) \). For example, let \( G = \mathbb{F}_2^d \), the additive group of a vector space of dimension \( d \geq 2 \) over the field \( \mathbb{F}_2 \) with 2 elements and let

\[
g_1 = (1, 0, \ldots, 0), \ g_2 = (0, 1, \ldots, 0), \ldots, g_d = (0, \ldots, 0, 1), \ g_{d+1} = (1, 1, 0, \ldots, 0).
\]

1991 Mathematics Subject Classification. primary 20E28; secondary 20B15, 20F05.

Key words and phrases. group generation; maximal subgroups; permutation groups; primitive groups.

1
Let $M = \{(x_1, \ldots, x_d) \in \mathbb{F}_2^d \mid a_1 x_1 + \cdots + a_d x_d = 0\}$ be a maximal subgroup of $G$. If $i \in \{1, \ldots, d\}$, then $g_i \in M$ only when $a_i = 0$. Therefore

$$\overline{M} = \{(x_1, \ldots, x_d) \in \mathbb{F}_2^d \mid x_1 + \cdots + x_d = 0\}$$

is the unique maximal subgroup of $G$ with $g_i \notin \overline{M}$ for every $i \in \{1, \ldots, d\}$. However $g_{d+1} \in \overline{M}$, hence every maximal subgroup of $G$ contains at least one of the $d + 1$ elements $g_1, \ldots, g_{d+1}$.

One might wonder, if minded so, whether the Frattini subgroup $\text{Frat}(G)$ may play a role in trying to strengthen Theorem 1.1. However, we cannot weaken the assumption “$G = \langle g_1, \ldots, g_d \rangle$" requiring only that “$g_i \notin \text{Frat}(G)$ for every $i \in \{1, \ldots, d\}$"; take for example $g_1 = (1,0,0)$, $g_2 = (0,1,0)$ and $g_3 = (1,1,0)$ in the additive group $G = \mathbb{F}_3^2$.

Moreover, it is not sufficient to assume that $\{g_1, \ldots, g_d\}$ is a minimal generating set of $G$ (i.e. no proper subset of $\{g_1, \ldots, g_d\}$ generates $G$): for example, if $G = \langle x \rangle$ is a cyclic group of order 6, then $\{x^2, x^3\}$ is a minimal generating set of $G$, and $\langle x^2 \rangle$ and $\langle x^3 \rangle$ are the unique maximal subgroups of $G$.

The proof of Theorem 1.1 is extremely easy, but it does not give any insight on the freedom that we have in the choice of the maximal subgroup $M$. One of the purposes of this note is to achieve some information in this direction for finite soluble groups.

**Notation 1.2.** Unless otherwise stated, we assume that $G$ is a finite soluble group with $d = d(G)$ and we assume that $g_1, \ldots, g_d$ satisfy the condition $G = \langle g_1, \ldots, g_d \rangle$.

Let $M$ be a maximal subgroup of $G$ and denote by $Y_M = \bigcap_{g \in G} M^g$ the normal core of $M$ in $G$ and by $X_M/Y_M$ the socle of the primitive permutation group $G/Y_M$ (in its action on the right cosets of $M/Y_M$ in $G/Y_M$); clearly $X_M/Y_M$ is a chief factor of $G$ and $M/Y_M$ is a complement of $X_M/Y_M$ in $G/Y_M$.

Let $\mathcal{M}$ be the set of maximal subgroups of $G$, let $V$ be a set of representatives of the irreducible $G$-modules that are $G$-isomorphic to some chief factor of $G$ having a complement and, for every $V \in \mathcal{V}$, let $\mathcal{M}_V$ be the set of maximal subgroups $M$ of $G$ with $X_M/Y_M \cong_G V$. (Here $V \cong_G W$ means that the $G$-modules $V$ and $W$ are $G$-isomorphic.)

Observe that each element $V$ of $\mathcal{V}$ is $G$-isomorphic to $X_M/Y_M$ for some $M \in \mathcal{M}$, and hence $\mathcal{M}_V \neq \emptyset$. Indeed, if $X/Y$ is a chief factor of $G$ with complement $K/Y$ in $G/Y$, then $K \in \mathcal{M}$ and $X/Y \cong_G X_K/Y_K$.

The question that we want to address is:

For which $V \in \mathcal{V}$, does there exist $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$?

To deal with this question it is useful to recall some results by Gaschütz [9]. Given $V \in \mathcal{V}$, let

$$R_G(V) = \bigcap_{M \in \mathcal{M}_V} M.$$

It turns out that $R_G(V)$ is the smallest normal subgroup of $G$ contained in $C_G(V)$ with $C_G(V)/R_G(V)$ being $G$-isomorphic to a direct product of copies of $V$ and having a complement in $G/R_G(V)$. The factor group $C_G(V)/R_G(V)$ is called the $V$-crown of $G$. The non-negative integer $\delta_G(V)$ defined by

$$\frac{C_G(V)}{R_G(V)} \cong_G V^{\delta_G(V)}$$
is called the $V$-rank of $G$ and it equals the number of complemented factors in any chief series of $G$ that are $G$-isomorphic to $V$ (see for example [2, Section 1.3]). Moreover $G/R_G(G) \cong V^{d_{G}(V)} \rtimes H_V$, where $H_V = G/C_G(V)$ acts diagonally on $V^{d_{G}(V)}$, that is, $(v_1, \ldots, v_{\delta_G(V)})^h = (v_1^h, \ldots, v_{\delta_G(V)}^h)$ for every $h \in H_V$ and for every $(v_1, \ldots, v_{\delta_G(V)}) \in V^{\delta_G(V)}$.

**Theorem 1.3.** Let $G = \langle g_1, \ldots, g_d \rangle$ be a finite soluble group with $d = d(G)$ and let $V \in \mathcal{V}$. Set $\theta_G(V) = 1$ if $V$ is a non-trivial $G$-module and $\theta_G(V) = 0$ otherwise, $F_V = \text{End}_{G}(V)$, $q_V = |F_V|$ and $n_V = \dim_{F_V}(V)$. If

$$\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1,$$

then there exists $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

Moreover, if there exists a unique choice for $M$, then one of the following occurs:

1. $V$ is a trivial $G$-module, $q_V = 2$ and $\delta_G(V) = d$;
2. $V$ is a non-trivial $G$-module, $d = 2$, $\delta_G(V) = 1$ and $(q_V, n_V) \in \{(3, 1), (2, 2)\}$.

In Corollary 1.4 and 1.5 we analyse the case that there exists a unique maximal subgroup avoiding a given generating set of minimum cardinality.

**Corollary 1.4.** Let $G$ be a finite soluble group with $d = d(G) \geq 2$. Suppose that there exist $g_1, \ldots, g_d$ generating $G$ with the property that there is a unique maximal subgroup $M$ of $G$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$. Then $|G : M| = 2$ and every normal subgroup $N$ of $G$ with $d(G/N) = d$ is contained in $G^{G/2}$.

Corollary 1.4 can be considerably strengthened when $d(G) = 2$.

**Corollary 1.5.** Let $G$ be a finite group with $d(G) = 2$. Suppose that there exist $g_1, g_2$ generating $G$ with the property that there is a unique maximal subgroup $M$ of $G$ with $M \cap \{g_1, g_2\} = \emptyset$. Then $|G : M| = 2$, $G$ is nilpotent and the Hall $2'$-subgroup of $G$ is cyclic.

**Remark 1.6.** We report some results from [6] related to our work that can shed some light on the condition “$\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$” in Theorem 1.3. Let $\mathcal{N}$ be the set of normal subgroups $N$ of $G$ with $d(G/N) = d$ and $d(G/K) < d$ whenever $N < K \leq G$.

Let $N \in \mathcal{N}$, let $K/N$ be an arbitrary minimal normal subgroup of $G/N$ and let $V = K/N$. As $d(G/K) < d$ and as $V$ is an irreducible $G$-module, it follows easily that $V \in \mathcal{V}$. By [6, Theorem 1.4 and Theorem 2.7], the irreducible $G$-module $V$ satisfies:

(i): $\delta_G(V) \geq (d(G) - 1 - \theta_G(V))n_V + 1$, and

(ii): $d(G/C_G(V)) < d(G)$.

(See Remark 1.8 for a comment concerning (ii).) In other words, for each $N \in \mathcal{N}$, the minimal normal subgroups of $G/N$ give rise to irreducible $G$-modules $V$ satisfying the condition “$\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$”.

Therefore, for soluble groups, Theorem 1.1 follows from Theorem 1.3: the set

$$\mathcal{W} = \{V \in \mathcal{V} \mid \delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1\}$$

is not empty (it contains all the minimal normal subgroups of $G/N$ for each $N \in \mathcal{N}$). Hence, when $G = \langle g_1, \ldots, g_d \rangle$, for every $V \in \mathcal{W}$, there exists $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$. 


Remark 1.7. Assume that $G$ is a soluble primitive permutation group on a finite set $\Omega$ with $d(G) = 2$. (Here and throughout the paper, we denote by $\text{supp}(g)$, or simply $\text{supp}(g)$, the support $\{\omega \in \Omega \mid \omega^g \neq \omega\}$ of the permutation $g$.) Observe that $G = V \rtimes H_V$ (for some $V \in \mathbb{V}$, and $H_V \cong G/\text{C}_G(V)$) and that $\mathcal{M}_V = \{G_\omega \mid \omega \in \Omega\}$, where $G_\omega$ is the stabilizer of the point $\omega \in \Omega$.

Let $g_1, g_2 \in G$. If $\text{supp}(g_1) \cap \text{supp}(g_2) = \varnothing$, then $\text{supp}(g_1)$ and $\text{supp}(g_2)$ are $\langle g_1, g_2 \rangle$-orbits and hence $\langle g_1, g_2 \rangle \neq G$ because $G$ is transitive. (Observe that this holds true regardless of $G$ being soluble.) Therefore, if $G = \langle g_1, g_2 \rangle$, then $\text{supp}(g_1) \cap \text{supp}(g_2) \neq \varnothing$. Moreover,

$$\{M \in \mathcal{M}_V \mid M \cap \{g_1, g_2\} = \varnothing\} = \{G_\omega \mid G_\omega \cap \{g_1, g_2\} = \varnothing\}$$

and hence the number of maximal subgroups $M \in \mathcal{M}_V$ avoiding $\{g_1, g_2\}$ is exactly $|\text{supp}(g_1) \cap \text{supp}(g_2)|$.

When $|\text{supp}(g_1) \cap \text{supp}(g_2)| = 1$, we have a unique choice for $M$ and, from Theorem 1.3, we obtain that $G$ is either the symmetric group $\text{Sym}(3)$ or the symmetric group $\text{Sym}(4)$.

This has a rather remarkable application. Indeed, fix $n \in \mathbb{N}$ and $a \in \{2, \ldots, n - 1\}$, and consider the two cycles $g_1 = (1, \ldots, a)$ and $g_2 = (a + 1, \ldots, n)$ and the group $G = \langle g_1, g_2 \rangle$. It can be easily seen that $G$ is a primitive subgroup of $\text{Sym}(n)$. Since $\text{supp}(g_1) \cap \text{supp}(g_2) = \{a\}$, we deduce that either $n \leq 4$ or $G$ is insoluble. In this way we prove that $\text{Sym}(n)$ is insoluble for $n \geq 5$ using an argument that relies only on linear algebra. (The proof of Theorem 1.3 relies only on linear algebra.)

Remark 1.8. Here we discuss again the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ in Theorem 1.3.

(i): Clearly, this condition is vacuously satisfied when $d = 1$.

(ii): Observe that $d(G/\text{C}_G(V)) \leq d(G) = d$. When $d(G/\text{C}_G(V)) < d$, the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ is necessary and sufficient to ensure that, for every generating $d$-tuple $g_1, \ldots, g_d$, there exists $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \varnothing$.

Indeed, if $\delta_G(V) \leq (d - 1 - \theta_G(V))n_V$ and $d(G/\text{C}_G(V)) < d$, then $d(G/\text{R}_G(V)) \leq d - 1$ (see for example [6, Theorem 2.7]) and hence there exist $x_1, \ldots, x_{d-1} \in G$ with $G = \langle x_1, \ldots, x_{d-1}, \text{R}_G(V) \rangle$. By a result of Gaschütz [8], there exist $r_1, \ldots, r_d \in \text{R}_G(V)$ with $G = \langle x_1r_1, \ldots, x_{d-1}r_{d-1}, r_d \rangle$.

When $V$ is a trivial $G$-module, we have $G = \text{C}_G(V)$, $d(G/\text{C}_G(V)) < d$ and hence the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ is necessary and sufficient.

(iv): When $d = 2$ and $V$ is a non-trivial $G$-module, the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ simplifies to $\delta_G(V) \geq 1$, which clearly holds true.

(v): The condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ in general is not necessary when $d(G/\text{C}_G(V)) = d$. Let $\tilde{G}$ be the soluble primitive permutation group $V \rtimes G/\text{C}_G(V)$ (with its natural affine action) and let $\tilde{G} : G \to \tilde{G}$ be the natural projection. We have $\delta(\tilde{G}) = d$ and, arguing as in Remark 1.7, a sufficient condition for the existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \varnothing$ is that $\cap_{1 \leq i \leq d} \text{supp}(g_i) \neq \varnothing$ whenever $G = \langle g_1, \ldots, g_d \rangle$. This always holds.
true (for example) when \( d = 3 \), as it can be deduced from the following, more general, result:

**Theorem 1.9.** If \( G = \langle g_1, g_2, g_3 \rangle \) is a primitive group with \( d(G) = 3 \), then \( \text{supp}(g_1) \cap \text{supp}(g_2) \cap \text{supp}(g_3) \neq \emptyset \).

(See also Remark 1.7 to see how this result fits within our investigation.)

**Remark 1.8.** (continued)

(v): In particular, when \( d(G) = d(G/C_G(V)) = 3 \), there always exists \( M \in \mathcal{M}_V \) with \( M \cap \{g_1, g_2, g_3\} = \emptyset \), regardless of whether the condition \( \delta_G(V) \geq (d - 1 - \theta_G(V))m_V + 1 \) holds or not.

(vi): We do not have any example of a finite soluble group \( G = \langle g_1, \ldots, g_d \rangle \) with \( d = d(G) = d(G/C_G(V)) \) and of a non-trivial \( G \)-module \( V \in \mathcal{V} \) where there is no \( M \in \mathcal{M}_V \) with \( M \cap \{g_1, \ldots, g_d\} = \emptyset \).

It is not clear whether Theorem 1.9 admits some generalisations. In particular:

**Question 1.10.** Does there exist a (soluble) primitive group \( G = \langle g_1, \ldots, g_d \rangle \) with \( d(G) = d > 3 \) and \( \bigcap_{1 \leq i \leq d} \text{supp}(g_i) = \emptyset \)?

An answer to Question 1.10 may shed some light on Remark 1.8 (vi). Indeed, an affirmative answer to Question 1.10 yields a primitive group \( G = \langle g_1, \ldots, g_d \rangle \) on \( \Omega \) with \( d(G) = d \) and \( \bigcap_{1 \leq i \leq d} \text{supp}(g_i) = \emptyset \). As \( G \) is soluble, we get \( G = V \times H \) where \( V \) is the socle of \( G \) and \( H \leq \text{GL}(V) \) is irreducible. Now, \( d(G) = d(G/C_G(V)) \) by [6]; moreover \( \mathcal{M}_V = \{G_{\omega} \mid \omega \in \Omega\} \) and hence there is no \( M \in \mathcal{M}_V \) with \( M \cap \{g_1, \ldots, g_d\} = \emptyset \).

A weaker result in this direction is the following:

**Theorem 1.11.** If \( G = \langle g_1, \ldots, g_d \rangle \) is a primitive permutation group with \( d(G) = d \geq 1 \), then \( \text{supp}(g_i) \cap \text{supp}(g_j) \neq \emptyset \) for all \( i, j \in \{1, \ldots, d\} \).

Theorem 1.11 does not remain true if we replace “primitive” with “transitive”. For example take \( g_1 = (1, 2, 3, 4), g_2 = (5, 7), g_3 = (1, 5)(2, 6)(3, 7)(4, 8) \). We have that \( G = \langle g_1, g_2, g_3 \rangle \) is a Sylow 2-subgroup of \( \text{Sym}(8) \): in particular \( d(G) = 3 \) but \( \text{supp}(g_1) \cap \text{supp}(g_2) = \emptyset \).

2. **Proof of Theorem 1.3**

Before proving Theorem 1.3 we need a preliminary lemma.

**Lemma 2.1.** Let \( V_1, \ldots, V_d \) be vector spaces of the same dimension, say \( n \), over a finite field \( \mathbb{F} \) of cardinality \( q \). Assume \( d \geq 2 \) and, when \( q = 2 \), assume also \( n \geq 2 \). Let \( W \) be a subspace of the direct product \( V_1 \times \cdots \times V_d \) and let \( U \) be a subspace of \( W \) with \( \dim_{\mathbb{F}}(U) = n \). If \( \dim_{\mathbb{F}}(W) > n(d - 1) \), then there exists \( (v_1, \ldots, v_d) \in W \setminus U \) such that \( v_i \neq 0 \) for every \( i \in \{1, \ldots, d\} \). Moreover, when \( (q, n, d) \notin \{(3, 1, 2), (2, 2, 2)\} \), there are at least two \( \mathbb{F} \)-linearly independent elements satisfying this property.

**Proof.** For the time being, let \( W \) be any subspace of \( V_1 \times \cdots \times V_d \) with \( m = \dim_{\mathbb{F}}(W) \), let \( \pi_i \) be the projection from \( V_i \times \cdots \times V_d \) to the direct factor \( V_i \) and let

\[
a_d = \dim_{\mathbb{F}} \pi_d(W),
\]

\[
a_i = \dim_{\mathbb{F}}(\ker \pi_d \cap \ker \pi_{d-1} \cap \cdots \cap \ker \pi_{i+1}),
\]

for each \( i \in \{1, \ldots, d - 1\} \),

\[
\Lambda = \{(v_1, \ldots, v_d) \in W \mid v_i \neq 0, \text{ for every } i \in \{1, \ldots, d\}\}.
\]
We claim that
\[ |A| \geq \prod_{i=1}^{d} (q^{a_i} - 1). \]

We argue by induction on \( d \). When \( d = 1 \), we have \( W = \pi_1(W) \leq V_1, a_d = m \) and \( W \) has \( q^m - 1 \) non-zero vectors. Assume now that \( d > 1 \). Let \( \rho: V_1 \times V_2 \times \cdots \times V_d \to V_2 \times \cdots \times V_d \) be the natural projection. Replacing \( V_1 \times \cdots \times V_d \) by \( V_2 \times \cdots \times V_d \), \( W \) by \( \rho(W) \) and \( \Lambda \) by \( \rho(\Lambda) \), the inductive hypothesis gives \( \rho(\Lambda) \geq \prod_{i=2}^{d} (q^{a_i} - 1) \).

For each \( x = (v_2, \ldots, v_d) \in \rho(\Lambda) \), choose \( v_{1x} \in V_1 \) with \((v_{1x}, v_2, \ldots, v_d) \in W \). Observe now that \( \ker \rho = \ker \pi_d \cap \cdots \cap \ker \pi_2 \) has dimension \( a_1 \) and hence \( W \) contains \( q^{a_1} \) vectors of the form \((v_{11}, 0, \ldots, 0)\). In particular, for each \( x = (v_2, \ldots, v_d) \in \rho(\Lambda) \), there are at least \( q^{a_1} - 1 \) elements \((v_1, 0, \ldots, 0)\) in \( W \) with \((v_{1x}, v_2, \ldots, v_d) + (v_1, 0, \ldots, 0) = (v_{1x} + v_1, v_2, v_3, \ldots, v_d) \in \Lambda \).

Therefore \( |A| \geq (q^{a_1} - 1)|\rho(\Lambda)| \geq \prod_{i=1}^{d} (q^{a_i} - 1) \) and the claim is proved.

Assume now that \( d \geq 2, m \geq n(d - 1) + 1 \), and \( n \geq 2 \) when \( q = 2 \). We need to show that \( \Lambda \setminus U \neq \emptyset \) and, for the stronger statement, that \( \Lambda \setminus U \) has at least two \( F \)-linearly independent vectors when \((q, n, d) \notin \{(3, 1, 2), (2, 2, 2)\} \). Since \( \dim_F(U) = n \), \( U \) contains at most \( q^n - 1 \) elements of \( \Lambda \); hence it suffices to prove that
\[ |A| \geq q^n \]
and, for the stronger statement, that
\[ |A| \geq q^n + (q - 1) \]
when \((q, n, d) \notin \{(3, 1, 2), (2, 2, 2)\} \).

Since \( a_i \leq \dim_F(V_i) = n \) for every \( i \in \{1, \ldots, d\} \) and \( a_1 + \cdots + a_d = \dim_F(W) = m \geq n(d - 1) + 1 \), we have \( 1 \leq a_i \leq n \) for every \( i \in \{1, \ldots, d\} \).

CASE 1: \( n = 1 \).

As \( n = 1 \), we have \( q \neq 2 \) and hence
\[ |A| \geq \prod_{i=1}^{d} (q^{a_i} - 1) \geq (q - 1)^d \geq (q - 1)^2 \geq q; \]
moreover \((q - 1)^d \geq q + (q - 1) \) when \((q, n, d) \neq (3, 1, 2) \).

Suppose \( n \geq 2 \). As \( \sum_{i=1}^{d} a_i = m \geq 2(d - 1) + 1 > d \), we get \( a_j > 1 \) for some \( j \in \{1, \ldots, d\} \). Therefore
\[ |A| \geq \prod_{i=1}^{d} (q^{a_i} - 1) = (q^{a_j} - 1) \prod_{i=1; i \neq j}^{d} (q^{a_i} - 1) \geq (q^{a_j} - 1) \prod_{i=1; i \neq j}^{d} (q - 1)^{q^{a_i} - 1} \]
\[ \geq ((q - 1)^{q^{a_j} - 1}) \prod_{i=1; i \neq j}^{d} (q - 1)^{q^{a_i} - 1} + 1 = (q - 1)^d q^{m-d} + 1 \]
\[ \geq (q - 1)^d q^{(d-1)(n-1)} + 1. \]

CASE 2: \( n \geq 2 \) and \( d \geq 3 \).

Here,
\[ |A| \geq (q - 1)^d q^{(d-1)(n-1)} + 1 \geq (q - 1)^2 q^{2(n-1)} + 1 \geq (q - 1)^2 + q^{2(n-1)} \geq q - 1 + q^n. \]
(In the third inequality we have used $ab + 1 \geq a + b$, which is valid for all $a, b \in \mathbb{N} \setminus \{0\}$.)

**Case 3:** $d = 2, n \geq 2$ and $(m, q) \not\in \{(n + 1, 2), (n + 1, 3)\}$. We have

$$|\Lambda| \geq (q^{a_1} - 1)(q^{a_2} - 1) = q^n - q^{a_1} - q^{a_2} + 1 \geq q^n - 2q^n + 1 \geq q^n + (q - 1).$$

(In the last inequality we used $(m, q) \not\in \{(n + 1, 2), (n + 1, 3)\}$.)

**Case 4:** $d = 2, n \geq 2$ and $(m, q) = (n + 1, 3)$. Here $n + 1 = m = a_1 + a_2$ and $|\Lambda| \geq (3^{a_1} - 1)(3^{a_2} - 1) = 3^n + 3^{n+1} - 3^{a_1} - 3^{a_2} + 1 \geq 3^n + (3 - 1) = 2^n + 3$ because $a_1$ and $a_2$ cannot be both $n$.

**Case 5:** $d = 2, n \geq 2$ and $(m, q) = (n + 1, 2)$. We have $|\Lambda| \geq 2^n + 2^{a_1} - 2^{a_2} + 1 \geq 2^n + (2 - 1) = 2^n$ except when $(a_1, a_2) \in \{(1, n), (n, 1)\}$.

Assume $(a_1, a_2) = (1, n)$ and fix $(f, 0)$ a non-zero vector of ker $\pi_2$. For every non-zero vector $v \in V_2$, there exists $w \in V_1$ such that $(w, v) \in W$. Since also $(w + f, v) \in W$, a moment’s thought gives that either $|\Lambda| \geq 2^n$, or $|\Lambda| = 2^n - 1$ and $\pi_1(W)$ is the 1-dimensional subspace of $V_1$ spanned by $f$. In the former case, the lemma is proved. In the latter case, $W = \langle f \rangle \times V_2$, $\Lambda = \{(f, v) \mid v \in V_2 \setminus \{0\}\}$ and $|\Lambda| = 2^n - 1$. With this concrete description of $W$ and $\Lambda$, we see that an $n$-dimensional subspace $U$ of $W$ can contain at most $2^{n-1}$ elements of $\Lambda$: so there are at least $2^n - 1 - 2^{n-1} = 2^{n-1} - 1$ elements in $\Lambda \setminus U$. Clearly, $\Lambda \setminus U$ contains at least two $\mathbb{F}$-linearly independent vectors as long as $2^{n-1} - 1 \geq 2$, that is, $n \neq 2$.

A similar argument works when $(a_1, a_2) = (n, 1)$. \hfill \Box

**Proof of Theorem 1.3.** We write $\bar{G} = G/R_G(V)$ and, for every $g \in G$, we denote by $\bar{g}$ the element $gR_G(V)$ of $\bar{G}$. We distinguish two cases.

**Case 1:** $V$ is a trivial $G$-module.

In this case $G = C_G(V)$ and $\bar{G}$ is elementary abelian and hence it can be viewed as the vector space $\mathbb{F}_p^d$ of dimension $\delta = \delta_G(V)$ over the finite field $\mathbb{F}_p$ of prime cardinality $p = |V|$. Therefore $q_V = p$, $n_V = 1$, $\theta_G(V) = 0$ and the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ simplifies to $\delta \geq d$. As $d(\bar{G}) = \delta$ and $d(G) = d$, we have $\delta \leq d$ and hence $\delta = d$. Moreover, the elements in $\mathcal{M}_V$ are in one-to-one correspondence with the maximal subgroups of $\bar{G}$, that is, with hyperplanes of $\mathbb{F}_p^d$.

For every $i \in \{1, \ldots, d\}$, we identify $\bar{g}_i$ with the vector $(x_{i1}, \ldots, x_{id})$ of $\mathbb{F}_p^d$. A maximal subgroup $M$ of $\bar{G}$ is determined by a linear equation $a_1x_1 + \cdots + a_dx_d = 0$ for suitable $a_1, \ldots, a_d \in \mathbb{F}_p$, and $\bar{g}_i \in M$ if and only if $\sum_{j=1}^d a_jx_{ij} = 0$.

Consider the linear map $\phi : \mathbb{F}_p^d \to \mathbb{F}_p^d$ defined by setting

$$\phi(a_1, \ldots, a_d) = \left( \sum_{j=1}^d a_jx_{1j}, \ldots, \sum_{j=1}^d a_jx_{dj} \right)$$

and observe that $\phi$ is injective and hence bijective because $\delta = d$. Let $\Lambda = \{(b_1, \ldots, b_d) \in \mathbb{F}_p^d \mid b_i \neq 0, \text{ for every } i \in \{1, \ldots, d\}\}$. The existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ is equivalent to $\phi(\mathbb{F}_p^d) \cap \Lambda \neq \emptyset$, which is clearly satisfied as $\phi(\mathbb{F}_p^d) \cap \Lambda = \Lambda$. Moreover, there are $|\Lambda|/(p - 1) = (p - 1)^{d-1}$ maximal subgroups $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$. Thus the choice of $M$ is unique only when $q_V = p = 2$. 

---

**MAXIMAL SUBGROUPS AVOIDING GENERATING SETS**

7
CASE 2: $V$ is a non-trivial $G$-module.

Let $\delta = \delta_G(V), H = G/C_G(V), \mathbb{F} = \text{End}_G(V), q = |\mathbb{F}|, n = uV$. We know that $G = G/R_G(V) \cong V^d \rtimes H$. For every $i \in \{1, \ldots, d\}$, we may write $g_i = h_iw_i$ with $h_i \in H$ and $w_i = (v_{i1}, \ldots, v_{id}) \in V^d$.

Let $\Omega = V \times \mathbb{F} \cong \mathbb{F}^{n+\delta}$ and let $\Omega^* = \{(w, \lambda_1, \ldots, \lambda_\delta) \in \Omega \mid (\lambda_1, \ldots, \lambda_\delta) = (0, \ldots, 0)\}$. For every $\omega = (w, \lambda_1, \ldots, \lambda_\delta) \in \Omega \setminus \Omega^*$, we associate the following subgroup $M_\omega$ of $G$:

$$M_\omega = \left\{ h(v_1, \ldots, v_\delta) \in G \mid w - w^h + \sum_{j=1}^\delta \lambda_j v_j = 0 \right\}.$$  

(It is an exercise to prove that $M_\omega$ is indeed a subgroup of $G$.) Observe that if $\omega \in \Omega \setminus \Omega^*$ and $\lambda \in \mathbb{F} \setminus \{0\}$, then $M_\omega = M_{\lambda\omega}$.

Since $(\lambda_1, \ldots, \lambda_\delta) \neq (0, \ldots, 0)$, for every $h \in H$, there exists $(v_1, \ldots, v_\delta) \in V^d$ with $w^h - w = \sum_{j=1}^\delta \lambda_j v_j$, that is, $h(v_1, \ldots, v_\delta) \in M_\omega$. Therefore $M_\omega V^d = H V^d = G$. Moreover $M_\omega \cap V^d$ is a maximal $H$-submodule of $V^d$, so $M_\omega$ is a maximal subgroup of $G$.

By [3, Proposition 2.1], the linear map $\phi : V \times \mathbb{F} \rightarrow V^d$ defined by setting

$$\phi(w, \lambda_1, \ldots, \lambda_\delta) = \left(\left(w - wh_1, \sum_{j=1}^\delta \lambda_j v_j \right), \ldots, \left(w - wh_\delta, \sum_{j=1}^\delta \lambda_j v_j \right)\right)$$

is injective. Moreover, $\{M \mid M \in \mathcal{M}_V\} = \{M_\omega \mid \omega \in \Omega \setminus \Omega^*\}$. Therefore we have a one-to-one correspondence between the elements of $\mathcal{M}_V$ and the $1$-dimensional subspaces of $\Omega$ contained in $\Omega \setminus \Omega^*$. Under this mapping the elements $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ correspond to the elements $\omega \in \Omega \setminus \Omega^*$ with $\phi(\omega) = (v_1, \ldots, v_\delta)$ having all non-zero coordinates, that is, $v_i \neq 0$ for every $i \in \{1, \ldots, d\}$.

Let $\Lambda = \{(v_1, \ldots, v_\delta) \in V^d \mid v_i \neq 0, \text{ for every } i \in \{1, \ldots, d\}\}, \text{ let } W = \phi(\Omega) \text{ and let } U = \phi(\Omega^*). \text{ Observe that dim}_\mathbb{F}(W) = n + \delta, \text{ dim}_\mathbb{F}(U) = n \text{ and } U \subseteq W \leq V^d.$ Summing up, there exists a maximal subgroup $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ if and only if there exists a vector of $W$ in $\Lambda \setminus U$.

The condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n + 1$ simplifies to $\delta \geq (d - 2)n + 1$, that is, $\text{dim}_\mathbb{F}(W) = n + \delta \geq n(d - 1) + 1 = \text{dim}_\mathbb{F}(U)(d - 1) + 1$. Now, the existence of a vector of $W$ in $\Lambda \setminus U$ is guaranteed by Lemma 2.1. Moreover, the choice of $M$ is unique if and only if there are no two $\mathbb{F}$-linearly independent vectors of $W$ in $\Lambda \setminus U$, that is, when $(q, n, d) \in \{(3, 1, 2), (2, 2, 2)\}$ in view of Lemma 2.1. 

3. PROOFS OF COROLLARY 1.4 AND COROLLARY 1.5

Proof of Corollaries 1.4 and 1.5. Recall Remark 1.6 and the notation therein. The uniqueness of $M$ implies that the set $W$ contains a unique $G$-module, say $V$. Moreover $\mathcal{M}_V$ contains a unique maximal subgroup $M$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

Suppose $d \geq 3$. Now, Theorem 1.3 yields $|V| = 2$, $C_G(V) = G$ and $R_G(V) = G'G^2$. Moreover, from Remark 1.6, we deduce that $N \leq R_G(V) = G'G^2$ for each $N \in N$. Since every normal subgroup $N$ of $G$ with $d(G/N) = d(G)$ is contained in some member of $N$, it follows that $N \leq G'G^2$. This proves Corollary 1.4 when $d \geq 3$. Observe that Corollary 1.5 implies Corollary 1.4 when $d = 2$. In particular, it remains to prove Corollary 1.5.
Assume then $d(G) = 2$. Suppose that $G$ is not soluble. Let $Y_1/Y_2$ be a non-abelian chief factor of $G$ and let $X = C_G(Y_1/Y_2)$. The factor group $G/X$ is monolithic (that is, it has a unique minimal normal subgroup) and its socle $N/X$ is isomorphic to $Y_1/Y_2$. We use the “bar” notation to denote the images under the projection $\pi : G \to G/X = G$. Let $P$ be a Sylow $p$-subgroup of $N$. From the Frattini argument we have $G = N_P(P)$, and hence there exists a maximal subgroup $M$ of $G$ with $N_G(P) \leq M$. The action of $\bar{G} = \langle g_1, g_2 \rangle$ on the set $\Omega$ of the right cosets of $M$ in $G$ is faithful and primitive. If $M^* \cap \{g_1, g_2\} \neq \emptyset$ for each $x \in G$, then every point of $\Omega$ is fixed by either $g_1$ or $g_2$, that is, $\Omega = (\Omega \setminus \text{supp}_1(g_1)) \cup (\Omega \setminus \text{supp}_2(g_2))$ and $\text{supp}_1(g_1) \cap \text{supp}_2(g_2) = \emptyset$, but this forces the group $\bar{G} = \langle g_1, g_2 \rangle$ to be intransitive. Therefore there exists $x \in G$ with $M^* \cap \{g_1, g_2\} = \emptyset$.

Since $N \leq M$, there exists a prime $q$ with $q \neq p$, $q \mid |N|$ and with $\bar{M}$ not containing any Sylow $q$-subgroup of $N$. Applying the Frattini argument as above with the prime $p$ replaced by the prime $q$, we find a maximal subgroup $\bar{K}$ of $\bar{G}$ containing the normalizer of a Sylow $q$-subgroup of $\bar{N}$ and an element $y \in G$ with $K^y \cap \{g_1, g_2\} = \emptyset$. Therefore we have two distinct maximal subgroups $M^*$ and $K^y$, both avoiding the two generators $g_1$ and $g_2$, against our assumption. Thus $G$ is soluble.

Observe that the condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ is always satisfied when $d = 2$ and $V$ is a non-trivial $G$-module (see Remark 1.8 (iv)). Therefore, by Theorem 1.3, for every non-trivial $G$-module $V \in \mathcal{V}$, there exists at least a maximal subgroup $M \in \mathcal{V}$ with $M \cap \{g_1, g_2\} = \emptyset$. Since we are assuming that there is a unique maximal subgroup with $M \cap \{g_1, g_2\} = \emptyset$, we deduce that $\mathcal{V}$ contains at most a unique non-trivial irreducible $G$-module.

By [7, Ch. A, Theorem 13.8], the Fitting subgroup $\text{Fit}(G)$ is the intersection of the centralisers of the chief factors of $G$ which are complemented. Therefore, from the previous paragraph, either $G$ is nilpotent (that is, $G$ has no non-trivial chief factors) or $\text{Fit}(G) = C_G(V)$, where $V$ is the unique non-trivial $G$-module in $\mathcal{V}$. Assume that $G$ is not nilpotent, and let $V$ be the unique non-trivial irreducible $G$-module in $\mathcal{V}$. Again by Theorem 1.3, either $|V| = 4$ and $G/C_G(V) \cong \text{GL}_2(2) \cong \text{Sym}(3)$, or $|V| = 3$ and $G/C_G(V) \cong \text{GL}_3(2) \cong C_2$. In both cases, there exists a group epimorphism $\phi : G \to \text{Sym}(3)$ (in the first case, by taking the projection of $G$ to $G/C_G(V)$, and in the second case, by taking the affine action of $G$ on $V$). Let $x_1 = \phi(g_1), x_2 = \phi(g_2)$. As $G$ contains a unique maximal subgroup avoiding $g_1$ and $g_2$, we deduce that $\text{Sym}(3)$ contains a unique maximal subgroup $K$ with $K \cap \{x_1, x_2\} = \emptyset$. But this is false: either one of the two elements $x_1, x_2$ has order 3 and in this case there are two subgroups of order 2 of $\text{Sym}(3)$ with trivial intersection with $\{x_1, x_2\}$, or both $x_1$ and $x_2$ have order 2, in which case there is one subgroup of order 2 and one of order 3 avoiding $x_1$ and $x_2$. Therefore $\mathcal{V}$ has no non-trivial irreducible $G$-modules, and $G$ is nilpotent.

The condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ reduces to $\delta_G(V) \geq 2$ for each $V \in \mathcal{V}$ because $d(G) = 2$. In particular, if $\delta_G(V) \geq 2$ for some irreducible $G$-module $V \in \mathcal{V}$ of odd order $p$ (that is, $G$ has an epimorphic image isomorphic to $C_p \times C_p$), then the second part of Theorem 1.3 guarantees the existence of two distinct maximal subgroups avoiding $g_1, g_2$, contrary to our assumption. Therefore $\delta_G(V) = 1$ for each irreducible $G$-module $V \in \mathcal{V}$ of odd order, that is, the Hall 2'-subgroup of $G$ is cyclic. Let $M$ be the unique maximal subgroup avoiding $g_1$ and $g_2$. As $d(G) = 2$, $G$ is not cyclic and hence $G$ has an irreducible $G$-module
We have $G$ Case a: use the classification of Guralnick and Magaard and we distinguish two possibilities:

Moreover $Y$ is the subgroup of $\text{Sym}(T)$ induced by the conjugacy action of $\{Y_1, \ldots, Y_\ell\}$. Let $V_m = V_{m,1} \oplus \cdots \oplus V_{m,\ell_m}$, where $V_{m,i}$ is an irreducible $N$-module for every $i \in \{1, \ldots, \ell_m\}$. Since $N$ is generated by transvections and since $N$ acts faithfully on $V$, there exists a transvection $h \in N$ with $h$ not centralizing $V_m$, that is, $h$ acts as a transvection on $V_m$. Therefore, $h$ acts as a transvection on $V_{m,i}$ for some $i \in \{1, \ldots, \ell_m\}$, and $h$ centralizes $V_{m,j}$ for every $j \in \{1, \ldots, \ell_m\} \setminus \{i\}$. If $\ell_m > 1$, then this contradicts the fact that $V_{m,1}, \ldots, V_{m,\ell_m}$ are pair-wise isomorphic $N$-modules. Thus $\ell_m = 1$ and $V_m$ is an irreducible $N$-module.

Let $Y_m$ and $X_m$ be the linear groups induced, respectively, by the actions of $N$ and $N_H(V_m)$ on $V_k$. We also write $X = X_1$ and $Y = Y_1$. Then $N$ is a subdirect product of $Y_1 \times \cdots \times Y_\ell$ and $H$ acts transitively by conjugation on $\{Y_1, \ldots, Y_\ell\}$. Moreover $Y_1 \cong \cdots \cong Y_\ell \cong Y$, $X_1 \cong \cdots \cong X_\ell \cong X$, $Y \leq X \leq \text{SL}_m(2)$, with $m = k/\ell$, and $H$ can be identified with a subgroup of the imprimitive linear group $X/T$, where $T$ is the subgroup of $\text{Sym}(\ell)$ induced by the conjugacy action of $H$ on $\{Y_1, \ldots, Y_\ell\}$.
Notice that $T$ is an epimorphic image of $G/N$, which is generated by the elements $g_k N$ with $k \in \{1, \ldots, d\} \setminus \{i, j\}$, so
\begin{equation}
 d(T) \leq d - 2.
\end{equation}

As $N$ is generated by transvections, we deduce that also $Y$ is generated by transvections. Then the structure of $Y$ can be deduced from [17, Theorem]: $Y$ is one of the following groups:

1. $\text{SL}_m(2)$ for $m \geq 2$,
2. $\text{Sp}_m(2)$ for $m \geq 4$,
3. $\text{O}^+_m(2)$ for $m \geq 6$,
4. $\text{O}^-_m(2)$, for $m \geq 4$,
5. $\text{Sym}(m+2)$ or $\text{Sym}(m+1)$ for $m \geq 4$.

From [13, Section 3 and Table 3.5A], we see that $\text{Sp}_m(2)$ is maximal in $\text{SL}_m(2)$ and, from [13, Section 3 and Table 3.5C], we see that $\text{O}^+_m(2)$ and $\text{O}^-_m(2)$ are both maximal in $\text{Sp}_m(2)$. It follows that $\text{SL}_m(2)$, $\text{Sp}_m(2)$, $\text{O}^+_m(2)$ and $\text{O}^-_m(2)$ are self-normalizing in $\text{SL}_m(2)$. As $\text{Aut}(\text{Sym}(\kappa)) = \text{Sym}(\kappa)$ except when $\kappa = 6$, it follows from Schur’s lemma that also $\text{Sym}(m+2)$ and $\text{Sym}(m+1)$ are self-normalizing in $\text{SL}_m(2)$, except possibly when $m \in \{4, 5\}$. Finally, a direct computation yields that $\text{Sym}(6)$ is self-normalizing in $\text{SL}_4(2)$ and in $\text{SL}_5(2)$. Therefore, in all these cases, $Y$ is self-normalizing in $\text{SL}_m(2)$.

Since $Y \leq X$, we conclude $Y = X$. Moreover $\text{soc}(Y)$ is a simple group (not necessarily non-abelian) and $|Y/\text{soc}(Y)| \leq 2$. Let $\Delta = Y \setminus \{1\}$ if $Y = \text{soc}(Y)$, and let $\Delta = Y \setminus \text{soc}(Y)$ otherwise.

Since $N$ is a subdirect product of $Y^\ell$ and it is generated by transvections, there exists a transvection $n = (y_1, \ldots, y_\ell) \in N$ with $y_j \in \Delta$ for some $j \in \{1, \ldots, \ell\}$. Now, to be a transvection $n$ must be equal to $(1, \ldots, 1, y_j, 1 \ldots 1)$. Let $\pi_j$ be the projection from $N$ to $Y_j$. Since $\pi_j(N) = Y_j$, we have that $[N, n]$ contains all the elements of the form $(1, \ldots, s, \ldots, 1)$ with $s \in [Y, y_j]$. As $\langle y_j, [Y, y_j] \rangle = Y$, we obtain that $N$ contains $(1, \ldots, y_j, 1 \ldots 1)$ for every $y \in Y$. This implies $N = Y^\ell$ and $H = Y \wr T$.

Let $K = (\text{soc}(Y))^\ell$ : an easy case-by-case analysis shows that $K$ is the unique minimal normal subgroup of $H$, so by [16, Theorem 1.1] $d(H) = \max\{2, d(H/K)\}$. On the other hand either $\text{soc}(Y) = Y$ and $H/K \cong T$ or $[Y : \text{soc}(Y)] = 2$ and $H/K \cong C_2 \wr T$. In both cases, $d(H/K) \leq d(T) + 1$. Now, Eqs. (4.1) and (4.2) yield $2 < d = d(G) = d(H) \leq \max\{2, d - 1\}$, a contradiction.

Case b: $G \leq H \wr \text{Sym}(t)$, where $H$ is a primitive group on $\Delta$ and the wreath product $H \wr \text{Sym}(t)$ has its product action on $\Omega = \Delta^t$. Moreover $H$ is almost simple with $\text{soc}(H) \in \{\text{Alt}(k), \Omega_{2k+1}(2), \Omega_{2k}^+(2), \Omega_{2k}(2)\}$ and $|H/\text{soc}(H)| \leq 2$.

The argument here is similar to the previous case. Write the element $g \in G$ as $(x_1, \ldots, x_t)\pi_s$ where $(x_1, \ldots, x_t)$ lies in the base subgroup $H^t$ and $\pi_s \in \text{Sym}(t)$. Setting $g_i = (a_1, \ldots, a_t)\pi_i$ and $g_j = (b_1, \ldots, b_t)\pi_j$ with $\pi_i, \pi_j \in \text{Sym}(t)$ and $(a_1, \ldots, a_t), (b_1, \ldots, b_t) \in H^t$, it can be easily seen that the assumption $\text{supp}(g_i) \cap \text{supp}(g_j) = \emptyset$ implies $\pi_i = \pi_j = 1$ and that there exists $s \in \{1, \ldots, t\}$ with $a_r = b_r = 1$ whenever $r \in \{1, \ldots, t\} \setminus \{s\}$.

If $a_s$ and $b_s$ are both in $\text{soc}(H)$, then $g_i, g_j \in \text{soc}(G) = \text{soc}(H)^t$ and this implies $d(G/\text{soc}(G)) \leq d - 2$. As usual, from [16, Theorem 1.1], we deduce $d(G) = \max\{2, d(G/\text{soc}(G))\} \leq \max\{2, d - 2\}$, a contradiction. Thus, we may assume $a_s \notin \text{soc}(H)$. Then $|H : \text{soc}(H)| = 2$. 
Arguing exactly as in Case A, we get $G = H \wr T$ with $T$ a transitive subgroup of $\text{Sym}(t)$ and $G/\text{soc}(G) \cong C_2 \wr T$. Since $g_1, g_2 \in H^t$, we must have $d(T) \leq d - 2$ and therefore $d(G) = \max\{2, d(G/\text{soc}(G))\} \leq \max\{2, d(T) + 1\} \leq \max\{2, d - 1\}$, again a contradiction.

**Proof of Theorem 1.9.** Let $G = \langle g_1, g_2, g_3 \rangle$ be a primitive subgroup of $\text{Sym}(\Omega)$ with $d(G) = 3$. We argue by contradiction and we suppose that $\text{supp}(g_1) \cap \text{supp}(g_2) \cap \text{supp}(g_3) = \emptyset$. Then $\text{fix}(g_1) \cup \text{fix}(g_2) \cup \text{fix}(g_3) = \Omega$ and

$$
|\text{fix}(g_1)| + |\text{fix}(g_2)| + |\text{fix}(g_3)| \geq |\Omega|.
\tag{4.3}
$$

We use the O’Nan-Scott theorem, as stated in [14]. According to this, we have five cases to consider. Let $N$ be the socle of $G$.

**Case A:** $G$ is an affine group.

Here, $N$ is an elementary abelian $p$-group for some prime $p$, $G = N \rtimes H$ where $H$ is an irreducible subgroup of $\text{GL}(N)$ and the action of $G$ on $\Omega$ is permutation equivalent to the affine action of $N \rtimes H$ on $N$.

Let $F = \text{End}_H(N)$, $q = |F|$, $\kappa = \text{dim}_F(N)$. We write $g_1 = h_1v_1$, $g_2 = h_2v_2$, $g_3 = h_3v_3$, with $h_1, h_2, h_3 \in H$ and $v_1, v_2, v_3 \in N$. In particular, given $n \in N$, we have $n^{h_i}v_i = n^{h_i} + v_i$ and hence $\text{supp}(g_i) = \{n \in N \mid n^{h_i} + v_i \neq n\}$. For simplicity, we define $\text{supp}(g_i) = N_i = \{n \in N \mid n - n^{h_i} = v_i\}$. As $\text{supp}(g_1) \cap \text{supp}(g_2) \cap \text{supp}(g_3) = \emptyset$, there exists no $w \in N$ with $w - w^{h_i} \neq v_i$ for every $i \in \{1, 2, 3\}$.

The mapping $\phi : N \times F \to N^3$ defined by setting

$$
\phi(w, \lambda) = (w - w^{h_1} + \lambda v_1, w - w^{h_2} + \lambda v_2, w - w^{h_3} + \lambda v_3)
$$

is clearly linear and (by [3, Proposition 2.1]) injective. We have $d(H) = d(G) = 3$ from [1, Corollary 1], and hence $h_i \neq 1$ for every $i \in \{1, 2, 3\}$. This means that $\kappa_i = \text{dim}_F(N^{1-h_i}) \geq 1$; in particular the set $N_i = \{n \in N \mid n - n^{h_i} = v_i\}$ has cardinality at most $q^{\kappa_i - 1} \leq q^{\kappa_i - 1}$. If $\sum_{1 \leq i \leq 3} q^{\kappa_i} < q^\kappa$, then $N \neq N_1 \cup N_2 \cup N_3$ and we are done: in particular, since $\sum_{1 \leq i \leq 3} q^{\kappa_i} \leq 3q^{\kappa_i - 1}$, we may assume $q \leq 3$.

If $q = 3$, then $N \neq N_1 \cup N_2 \cup N_3$ except (possibly) when $\kappa_i = 1$ for every $i \in \{1, 2, 3\}$. In this case, the fact that $\phi$ is injective implies that $3 = \kappa_1 + \kappa_2 + \kappa_3 \geq \kappa$. On the other hand, if $\kappa \leq 2$, then $d(H) \leq 2$ by [12, Theorem 1.2], against our assumption; so $\kappa = 3$ and $(N \times \{0\})^\phi = N^{1-h_1} \times N^{1-h_2} \times N^{1-h_3}$ and we can easily conclude that there is $(u_1, u_2, u_3) \in N^{1-h_1} \times N^{1-h_2} \times N^{1-h_3}$ with $u_i \neq v_i$ for every $i \in \{1, 2, 3\}$.

Finally suppose $q = 2$. Relabelling the indexed set $\{1, 2, 3\}$ if necessary, we may assume that $\kappa_1 \leq \kappa_2 \leq \kappa_3$. As above, if $N \neq N_1 \cup N_2 \cup N_3$, then we are done. Since $|N_1 \cup N_2 \cup N_3| \leq 2^{\kappa_1 - \kappa_3} + 2^{\kappa_2 - \kappa_3} < 2^{\kappa_1 - \kappa_3} + 2^{\kappa_2 - \kappa_3}$, we may restrict our attention to the case $2^{\kappa_1 - \kappa_3} + 2^{\kappa_2 - \kappa_3} \geq 2^\kappa$. This implies that either $(\kappa_1, \kappa_2, \kappa_3) = (1, 2, 2)$, or $(\kappa_1, \kappa_2) = (1, 1)$. In the first case $\kappa \leq \kappa_1 + \kappa_2 + \kappa_3 \leq 5$, but then $d(H) \leq 2$ by [12, Theorem 1.2], against our assumption. It remains to consider the case $(\kappa_1, \kappa_2) = (1, 1)$. This means that $h_1, h_2$ both act as transvections on the irreducible $H$-module $N$.

Using as a crib the argument in Case A in the proof of Theorem 1.11, we deduce $d(G) \leq 2$, a contradiction.

**Case B:** $G$ is of simple diagonal type.

Here $N = S^\kappa$, for some non-abelian simple group $S$ and for some positive integer $\kappa$ with $\kappa \geq 2$. Moreover, $|\Omega| = |S|^\kappa - 1$. Let $g$ be a non-identity element of $G$. An upper bound for $|\text{fix}(g)|$ is given in [15, p. 310] (see also [10, Section 5]). We have
When \( \kappa \geq 3 \), we deduce \( |\text{fix}(g)| \leq |\Omega|/60 \), contradicting (4.3). Suppose then \( \kappa = 2 \). From [18, Theorem 3.1], we have \( |\{s \in S \mid s^\alpha = s^{-1}\}| \leq 4|S|/15 \), for each automorphism \( \alpha \) of \( S \). Therefore, \( |\text{fix}(g)| \leq 4|\Omega|/15 < |\Omega|/3 \), contradicting again (4.3).

**Case c:** \( G \) is of twisted wreath type.

Here \( N \) is a normal regular subgroup of \( G \) and the action of a point-stabilizer on \( \Omega \) is permutation equivalent to its action on \( N \) by conjugation. Consequently, if \( g \) is a non-identity element of a point-stabilizer, then \( |\text{fix}(g)| \leq |C_N(g)| \leq |N|/5 = |\Omega|/5 \), again contradicting (4.3).

**Case d:** \( G \) is almost simple.

From [5], the condition \( d(G) = 3 \) implies that either \( N = \text{PSL}_n(q) \) with \( n \geq 4 \) or \( N = \text{PQ}_n^+(q) \) with \( n \geq 8 \), moreover (in both cases) \( q \) is an even power of an odd prime. In particular, \( q \geq 9 \). By [15, Theorem 1], for each non-identity element \( g \in G \), we have

\[
|\text{fix}(g)| \leq \frac{4|\Omega|}{3q} \leq \frac{4|\Omega|}{27} < \frac{|\Omega|}{3},
\]

again contradicting (4.3).

**Case e:** \( G \) is of wreath product type.

In particular \( G \leq H \wr \text{Sym}(t) \), where \( H \) is a primitive group on \( \Delta \) and the wreath product has its product action on \( \Omega = \Delta^t \). Moreover \( H \) is either of almost simple type or of simple diagonal type and \( \text{soc}(G) = (\text{soc}(H))^\prime \). Let \( g_1 = (a_1, \ldots, a_t)\pi_1 \), \( g_2 = (b_1, \ldots, b_t)\pi_2 \) and \( g_3 = (c_1, \ldots, c_t)\pi_3 \), where \( (a_1, \ldots, a_t) \), \( (b_1, \ldots, b_t) \) and \( (c_1, \ldots, c_t) \) are in the base group \( H^t \) and \( \pi_1, \pi_2, \pi_3 \in \text{Sym}(t) \).

Let \( g \in G \) and write \( g \) as \((x_1, \ldots, x_t)\pi_g \) where \((x_1, \ldots, x_t)\) lies in the base group \( H^t \) and \( \pi_g \in \text{Sym}(t) \).

We claim that, if \( \pi_g \neq 1 \), then

\[(4.4) \quad |\text{fix}(g)| \leq |\Delta^{t-1}|\]

and the bound is met if and only if \( g \) is \((H \wr \text{Sym}(t))-\)conjugate to 

\[(x, x^{-1}, 1, \ldots, 1)(1 \, 2),\]

for some \( x \in H \). Indeed, choose \( i, j \in \{1, \ldots, t\} \) with \( i\pi_g = j \) and \( i \neq j \). Observe that if \((\delta_1, \ldots, \delta_t) \in \text{fix}(g)\), then \( \delta_j = \delta_{\pi_g}^i \). Consequently, for the elements in \( \text{fix}(g) \) the \( j^{\text{th}}\)-coordinate is uniquely determined by the \( i^{\text{th}}\)-coordinate and (4.4) is proved. Moreover, if the bound in Eq. (4.4) is met then, \( \pi_g \) is a transposition, say \( \pi_g = (i \, j) \), and moreover \( x_k = 1 \) for every \( k \in \{1, \ldots, t\} \setminus \{i, j\} \). Now, a direct computation with this explicit description of \( g \) yields that the bound in Eq. (4.4) is met if and only if \( x_i x_j = 1 \).

We observe that, if \( \pi_g = 1 \) and \( g \neq 1 \), then

\[(4.5) \quad |\text{fix}(g)| \leq (|\Delta| - 2)|\Delta|^{t-1}\]

and the bound is met if and only if \( g \) is \((H \wr \text{Sym}(t))-\)conjugate to 

\[(x, 1, \ldots, 1),\]
where \( x \) is a transposition in \( H \). See for example [10, Section 3].

We now use Eqs. (4.4) and (4.5) and their characterisation of equalities to the elements \( g_1, g_2, g_3 \). Suppose that \( \pi_1, \pi_2, \pi_3 \neq 1 \). Using Eqs. (4.4), we get \( |\Omega| \leq \sum_{i=1}^{t} |\text{fix}(g_i)| \leq 3|\Delta|^t - 1 < |\Delta|^t = |\Omega| \), a contradiction. Suppose next that \( \pi_1 = 1 \) and \( \pi_2, \pi_3 \neq 1 \). Using Eqs. (4.4) and (4.5), we get \( |\Omega| \leq \sum_{i=1}^{t} |\text{fix}(g_i)| \leq (|\Delta| - 2)|\Delta|^{t-1} + 2|\Delta|^{t-1} = |\Delta|^t = |\Omega| \). In particular, \( |\text{fix}(g_1)| = (|\Delta| - 2)|\Delta|^{t-1} \) and \( |\text{fix}(g_2)| = |\text{fix}(g_3)| = |\Delta|^{t-1} \). Using the characterisations above it is easy to conclude that \( G = \text{Sym}(\Delta) \wr \text{Sym}(2) \) or \( G = \text{Sym}(\Delta) \wr \text{Sym}(3) \). In both cases, \( d(G) = 2 \), a contradiction.

Relabelling the indexed set \( \{1, 2, 3\} \) if necessary, we may assume \( \pi_1 = \pi_2 = 1 \). In particular, \( \pi_3 \) is a \( t \)-cycle and, relabelling the indexed set \( \{1, \ldots, t\} \) if necessary, we may assume \( \pi_3 = (1 2 \ldots t) \).

There exists \( j_1, j_2 \in \{1, \ldots, t\} \) with \( a_{j_1} \neq b_{j_2} \neq 1 \). If \( \text{supp}(a_{j_1}) > |\Delta|/2 \) and \( \text{supp}(b_{j_2}) > |\Delta|/2 \), then there exist \( i \in \{1, \ldots, t\} \) and \( \omega = (\delta_1, \ldots, \delta_t) \in \Delta^t = \Omega \) such that \( \delta_j a_{j_1} \neq \delta_j, \delta_j b_{j_2} \neq \delta_j, \) and \( \delta_i \neq \delta_{i+2} \). In this case \( \omega \in \text{supp}(g_1) \cap \text{supp}(g_2) \cap \text{supp}(g_3) \) and we are done. Therefore, we may assume that there exists \( h \in H \) with \( |\text{supp}(h)| \leq |\Delta|/2 \). The primitive groups with these properties have been classified by Guralnick and Magaard [11, Theorem 1]: \( H \) is an almost simple group and in all cases \( |H/\text{soc}(H)| \leq 2 \). (Here we follow closely the ideas in the proof of Theorem 1.11 Case B.) Then \( G/\text{soc}(G) \leq C_2 \wr C_n \). To conclude the proof we need the following claim.

**Claim** Let \( X \) be a subgroup of \( C_2 \wr \langle \sigma \rangle \), where \( \sigma = (1, \ldots, t) \in \text{Sym}(t) \). If \( X \) contains an element \( g \) of the form \( g = (c_1, \ldots, c_t) \sigma \), then \( d(X) \leq 2 \).

Let \( W = C_2^t \) be the base of the wreath product \( C_2 \wr \langle \sigma \rangle \) and let \( U = W \cap X \). We can view \( W \) as a cyclic \( \mathbb{F}_p[x] \)-module with \( x \) acting as \( g \) does. As \( \mathbb{F}_p[x] \) is polynomial ring, it is a principal ideal domain, therefore every submodule of \( W \) is cyclic: in particular there exists \( u \in U \) generating \( U \) an \( \mathbb{F}_p[x] \)-module. Thus \( X = \langle g, u \rangle \) and \( d(X) \leq 2 \).

Applying the previous claim with \( G/\text{soc}(G) \) and using [16, Theorem 1.1], we deduce \( d(G) = \max\{2, d(G/\text{soc}(G))\} = 2 \), but this contradicts \( d(G) = 3 \). \( \square \)

### 5. Direct product of non-abelian simple groups

Let \( S \) be a finite non-abelian simple group. Given a positive integer \( d \geq 3 \), consider the action of \( \text{Aut}(S) \) on \( S^d \) and let \( \Omega_d \) be the set of \( \text{Aut}(S) \)-orbits on the set of \( d \)-tuples \( (x_1, \ldots, x_d) \in S^d \) with the following properties:

1. \( S = \langle x_1, \ldots, x_d \rangle \);
2. for every maximal subgroup \( M \) of \( S \), there exists \( i \in \{1, \ldots, d\} \) with \( x_i \in M \).

Notice that, since \( d \geq 3 \), \( \Omega_3 \) is non-empty, there are several generating \( d \)-tuples in which at least one entry coincides with the identity element. (However, when \( d = 2 \), we have \( \Omega_2 = \emptyset \) by Theorem 1.1.)

We use the notation \( \left[ (x_1, \ldots, x_d) \right] \) to denote the \( \text{Aut}(S) \)-orbit containing \( (x_1, \ldots, x_d) \in \Omega_d \). We define the graph \( \Gamma_d \) with vertex set \( \Omega_d \) and where two distinct vertices \( \left[ (x_1, \ldots, x_d) \right] \) and \( \left[ (y_1, \ldots, y_d) \right] \) are declared to be adjacent if and only if, for every \( \gamma \in \text{Aut}(S) \), there exists \( i \in \{1, \ldots, d\} \) (which may depend on \( \gamma \)) such that \( y_i = x_i^\gamma \).
Theorem 5.1. Let $\omega(\Gamma_d)$ be the clique number of $\Gamma_d$ and let $P_S(k)$ be the probability of generating $S$ with $k$-elements. We have

$$\omega(\Gamma_d) \leq \frac{P_S(d-1)|S|^{d-1}}{|\text{Aut}(S)|}.$$  

Proof. Let $t = \frac{P_S(d-1)|S|^{d-1}}{|\text{Aut}(S)|} + 1$ and suppose, by contradiction, that

$$\omega_1 = [(x_{11}, \ldots, x_{d1}], \omega_2 = [(x_{12}, \ldots, x_{d2}], \ldots, \omega_t = [(x_{1t}, \ldots, x_{dt}]]$$

are $t + 1$ vertices of a clique of $\Gamma_d$. Consider the $d$ elements

$$g_1 = (x_{11}, \ldots, x_{1d}), g_2 = (x_{21}, \ldots, x_{2d}), \ldots, g_d = (x_{d1}, \ldots, x_{dt})$$

of $S^t$. We have that $S^t = \{g_1, \ldots, g_d\}$ and $S^t$ cannot be generated by $d - 1$ elements (by the way in which $t$ is defined, see for example [4] for some details). So $d(S^t) = d$ and we may apply Theorem 1.1: there exists a maximal subgroup $M$ of $S^t$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$. Now, there are two possibilities:

Case A: $M$ is of “product type”, i.e. there exists $i \in \{1, \ldots, t\}$ and a maximal subgroup $K$ of $S$ such that $M = \{(s_1, \ldots, s_t) \in S^t \mid s_i \in K\}$. In this case, as $M \cap \{g_1, \ldots, g_d\} = \emptyset$, we have $x_{ji} \notin K$ for every $j \in \{1, \ldots, d\}$, but then $\omega_i \notin \Omega_d$ because we are violating the condition (1) above, a contradiction.

Case B: $M$ is of “diagonal type”, i.e. there exist $i, j \in \{1, \ldots, t\}$ with $i \neq j$ and $\gamma \in \text{Aut}(S)$ such that $M = \{(s_1, \ldots, s_t) \in S^t \mid s_j = s_i^\gamma\}$. In this case, as $M \cap \{g_1, \ldots, g_d\} = \emptyset$, we have $x_{kj} \neq x_{ki}^\gamma$ for every $k \in \{1, \ldots, d\}$, in contradiction with the fact that $\omega$ and $\omega_i$ are adjacent vertices of $\Gamma_d$. □

References


Andrea Lucchini, Dipartimento di Matematica Pura e Applicata, University of Padova, Via Trieste 53, 35121 Padova, Italy
E-mail address: lucchini@math.unipd.it

Pablo Spiga, Dipartimento di Matematica Pura e Applicata, University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy
E-mail address: pablo.spiga@unimib.it