Maximal subgroups of finite groups avoiding the elements of a generating set

Andrea Lucchini

Università di Padova, Italy

Groups and Topological Groups 2017
Budapest, February 3rd, 4th

Joint work with Pablo Spiga

An easy theorem

Theorem

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 $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

An easy theorem

Theorem

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

Proof.

If G is cyclic the statement is clear. When $d > 1$, consider

$$H = \langle g_1 g_2, g_2 g_3, \dots, g_{d-1} g_d \rangle.$$

$$d(H) \leq d - 1 < d(G) \Rightarrow H \neq G.$$

Let M be a maximal subgroup of G containing H.

$$g_i \in M \text{ and } i \neq d \Rightarrow g_{i+1} = g_i^{-1}(g_i g_{i+1}) \in M.$$

$$g_i \in M \text{ and } i \neq 1 \Rightarrow g_{i-1} = (g_{i-1} g_i) g_i^{-1} \in M.$$

Thus $M \cap \{g_1, \dots, g_d\} \neq \emptyset$ implies $G = \langle g_1, \dots, g_d \rangle \leq M$, a contradiction.

This result does not remain true if we drop the assumption $d = d(G)$.

For example, let $G = \mathbb{F}_2^d$ be the additive group of a vector space of dimension $d \geq 2$ over the field $\mathbb{F}_2$ with 2 elements and let

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

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 $i \leq d$, 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 $i \leq d$. However $g_{d+1} \in \overline{M}$. Hence every maximal subgroup of G contains at least one of the $d+1$ elements $g_1, \ldots, g_{d+1}$.

This result does not remain true if we drop the assumption $d = d(G)$.

For example, let $G = \mathbb{F}_2^d$ be the additive group of a vector space of dimension $d \geq 2$ over the field $\mathbb{F}_2$ with 2 elements and let

$$g_1 = (1, 0, \dots, 0), \ \dots, g_d = (0, \dots, 0, 1), \ g_{d+1} = (1, 1, 0, \dots, 0).$$

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

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

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

Moreover, it is not sufficient to assume that $\{g_1, \dots, g_d\}$ is a minimal generating set of G (i.e. no proper subset of $\{g_1, \dots, g_d\}$ 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.

Theorem

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 $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

The proof of this theorem is extremely easy, but it does not give any insight on the freedom that we have in the choice of the maximal subgroup M.

THE SOLUBLE CASE

NOTATIONS

- M a maximal subgroup of a finite soluble group G,
- $Y_M = \bigcap_{g \in G} M^g$ the normal core of M in G,
- X_M/Y_M the socle of the primitive permutation group G/Y_M.
- $\frac{X_M}{Y_M}$ is a chief factor of G and $\frac{M}{Y_M}$ is a complement of $\frac{X_M}{Y_M}$ in $\frac{G}{Y_M}$.
- $\mathcal{V}$:= a set of representatives of the irreducible G-modules that are G-isomorphic to some chief factor of G having a complement.
- for every $V \in \mathcal{V}$, let $\mathcal{M}_V$ be the set of maximal subgroups M of G with $X_M/Y_M \cong_G V$.

QUESTION

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

It is useful to recall some results by Gaschütz. Given $V \in \mathcal{V}$, let

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

It is useful to recall some results by Gaschütz. Given $V \in \mathcal{V}$, let

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

- $R_G(V)$ 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 $G/R_G(V)$.

It is useful to recall some results by Gaschütz. Given $V \in \mathcal{V}$, let

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

- $R_G(V)$ 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.

It is useful to recall some results by Gaschütz. Given $V \in \mathcal{V}$, let

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

- $R_G(V)$ 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.

It is useful to recall some results by Gaschütz. Given $V \in \mathcal{V}$, let

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

- $R_G(V)$ 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.
- $G/R_G(V) \cong V^{\delta_G(V)} \rtimes G/C_G(V)$ where $G/C_G(V)$ acts diagonally on $V^{\delta_G(V)}$.

Let $G = \langle g_1, \ldots, g_d \rangle$. We want to check whether there exists $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$. We write $\overline{G} = G/R_G(V)$ and, for every $g \in G$, we denote by $\overline{g}$ the element $gR_G(V)$ of $\bar{G}$. Let $\delta = \delta_G(V)$.

CASE 1: V IS A TRIVIAL G-MODULE.

- $G = C_G(V)$, $\overline{G} \cong \mathbb{F}_p^\delta$ and elements in $\mathcal{M}_V$ are in one-to-one correspondence with the hyperplanes of $\mathbb{F}_p^\delta$.
- For every i, we identify $\bar{g}_i$ with the vector $(x_{i1}, \ldots, x_{i\delta})$ of $\mathbb{F}_p^\delta$.
- A maximal subgroup M of $\bar{G}$ is determined by a linear equation $a_1x_1 + \cdots + a_\delta x_\delta = 0$ and $\bar{g}_i \in M$ if and only if $\sum_{j=1}^{\delta} a_j x_{ij} = 0$.
- The linear map $\phi : \mathbb{F}_p^\delta \to \mathbb{F}_p^d$ defined by setting

$$\phi(a_1, \ldots, a_\delta) = \left(\sum_{j=1}^{\delta} a_j x_{1j}, \ldots, \sum_{j=1}^{\delta} a_j x_{dj} \right)$$

  is injective.
- The existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ is equivalent to the existence of $(b_1, \ldots, b_d) \in \phi(\mathbb{F}_p^\delta)$ with $b_i \neq 0$ for every i.

CASE 2: V IS A NON-TRIVIAL G-MODULE.

- $H := G/C_G(V)$, $\mathbb{F} := \mathrm{End}_G(V)$. We have $\overline{G} \cong V^\delta \rtimes H$.
- We may write $\bar{g}_i = h_i w_i$ with $h_i \in H$ and $w_i = (v_{i1}, \ldots, v_{i\delta}) \in V^\delta$.
- $\Omega := V \times \mathbb{F}^\delta$ and $\Omega^* := \{(w, 0, \ldots, 0) \in \Omega \mid w \in V\}$.
- There is a one-to-one correspondence between the elements of $\mathcal{M}_V$ and the 1-dimensional subspaces of Ω contained in $\Omega \setminus \Omega^*$: for every $\omega = (w, \lambda_1, \ldots, \lambda_\delta) \in \Omega \setminus \Omega^*$, we associate the maximal subgroup $M_\omega = \{h(v_1, \ldots, v_\delta) \in \bar{G} \mid w - w^h + \sum_{j=1}^{\delta} \lambda_j v_j = 0\}$.
- An injective linear map $\phi : \Omega \to V^d$ is defined by setting

$$\phi(w, \lambda_1, \ldots, \lambda_\delta) = \left(\left(w - w^{h_1} + \sum_{j=1}^{\delta} \lambda_j v_{1j}\right), \ldots, \left(w - w^{h_d} + \sum_{j=1}^{\delta} \lambda_j v_{dj}\right)\right)$$

- The $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ correspond to the $\omega \in \Omega \setminus \Omega^*$ s.t. $\phi(\omega) = (v_1, \ldots, v_d)$ has all non-zero coordinates.

Theorem

Let $G = \langle g_1, \dots, g_d \rangle$ 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, $\mathbb{F}_V = \mathrm{End}_G(V)$, $q_V = |\mathbb{F}_V|$ and $n_V = \dim_{\mathbb{F}_V}(V)$. If

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

then there exists $M \in \mathcal{M}_V$ with $M \cap \{g_1, \dots, g_d\} = \emptyset$. 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 $(q_V, n_V) \in \{(3, 1), (2, 2)\}$.*

Lemma

Let $V_1, \dots, V_d$ be vector spaces of dimension n over $\mathbb{F}_q$. Assume $d \geq 2$ and, when $q = 2$, assume also $n \geq 2$. Let W be a subspace of $V_1 \times \cdots \times V_d$ and let U be a subspace of W with $\dim U = n$. If $\dim W > n(d-1)$, then there exists $(v_1, \dots, v_d) \in W \setminus U$ such that $v_i \neq 0$ for every i. When $(q, n, d) \notin \{(3, 1, 2), (2, 2, 2)\}$, there are at least two $\mathbb{F}$-linearly independent elements satisfying this property.

Corollary

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

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 $G'G^2$.

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

Corollary

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 $G'G^2$.

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

Corollary

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 $O_{2'}(G)$ is cyclic.

A FOLKLORE RESULT

- Assume that G is a soluble primitive permutation group on a finite set Ω with $d(G) = 2$. Observe that $G = V \rtimes H$ and that $\mathcal{M}_V = \{G_\omega \mid \omega \in \Omega\}$, where G_ω is the stabilizer of $\omega \in \Omega$.
- We denote by $\mathrm{supp}(g)$ the support $\{\omega \in \Omega \mid \omega^g \neq \omega\}$ of the permutation g. If $G = \langle g_1, g_2 \rangle$, then $\mathrm{supp}(g_1) \cap \mathrm{supp}(g_2) \neq \emptyset$.

$$\begin{aligned}\{M \in \mathcal{M}_V \mid M \cap \{g_1, g_2\} = \emptyset\} &= \{G_\omega \mid G_\omega \cap \{g_1, g_2\} = \emptyset\} \\ &= \{G_\omega \mid \omega \in \mathrm{supp}(g_1) \cap \mathrm{supp}(g_2)\}\end{aligned}$$

  hence the number of maximal subgroups $M \in \mathcal{M}_V$ avoiding $\{g_1, g_2\}$ is exactly $|\mathrm{supp}(g_1) \cap \mathrm{supp}(g_2)|$.
- When $|\mathrm{supp}(g_1) \cap \mathrm{supp}(g_2)| = 1$, we have a unique choice for M and, by the previous theorem, either $G \cong \mathrm{Sym}(3)$ or $G \cong \mathrm{Sym}(4)$.

A folklore result

If $G = \langle g_1, g_2 \rangle$ is a soluble primitive permutation group and $|\operatorname{supp}(g_1) \cap \operatorname{supp}(g_2)| = 1$, then either $G \cong \operatorname{Sym}(3)$ or $G \cong \operatorname{Sym}(4)$.

A folklore result

If $G = \langle g_1, g_2 \rangle$ is a soluble primitive permutation group and $|\operatorname{supp}(g_1) \cap \operatorname{supp}(g_2)| = 1$, then either $G \cong \operatorname{Sym}(3)$ or $G \cong \operatorname{Sym}(4)$.

This has a rather remarkable application.

A FOLKLORE RESULT

If $G = \langle g_1, g_2 \rangle$ is a soluble primitive permutation group and $|\operatorname{supp}(g_1) \cap \operatorname{supp}(g_2)| = 1$, then either $G \cong \operatorname{Sym}(3)$ or $G \cong \operatorname{Sym}(4)$.

This has a rather remarkable application.

- Fix $n \in \mathbb{N}$ and $a \in \{2, \ldots, n-1\}$.
- Consider the two cycles $g_1 = (1, \ldots, a)$ and $g_2 = (a+1, \ldots, n)$,
- $G = \langle g_1, g_2 \rangle$ is a primitive subgroup of $\operatorname{Sym}(n)$.
- Since $\operatorname{supp}(g_1) \cap \operatorname{supp}(g_2) = \{a\}$, we deduce that either $n \leq 4$ or G is insoluble.

In this way we prove that $\operatorname{Sym}(n)$ is insoluble for $n \geq 5$ using an argument that relies only on linear algebra.

Remark 1

Let $\mathcal{W} := \{V \in \mathcal{V} \mid \delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1\}$. Our theorem states that the condition $V \in \mathcal{W}$ is sufficient to ensure the existence of a maximal subgroup in $\mathcal{M}_V$ avoiding $g_1, \ldots, g_d$.

Remark 1

Let $\mathcal{W} := \{V \in \mathcal{V} \mid \delta_G(V) \geq (d-1-\theta_G(V))n_V + 1\}$. Our theorem states that the condition $V \in \mathcal{W}$ is sufficient to ensure the existence of a maximal subgroup in $\mathcal{M}_V$ avoiding $g_1, \ldots, g_d$.

Question

Is $\mathcal{W}$ a non-empty set?

Remark 1

Let $\mathcal{W} := \{V \in \mathcal{V} \mid \delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1\}$. Our theorem states that the condition $V \in \mathcal{W}$ is sufficient to ensure the existence of a maximal subgroup in $\mathcal{M}_V$ avoiding $g_1, \ldots, g_d$.

Question

Is $\mathcal{W}$ a non-empty set?

- Let $\mathcal{N}$ be the set of normal subgroups N of G with $d(G/N) = d$ and $d(G/K) < d$ whenever $N < K \trianglelefteq G$.
- Let $N \in \mathcal{N}$, let K/N be an arbitrary minimal normal subgroup of G/N and let $V = K/N$. It follows easily that $V \in \mathcal{V}$.
- The irreducible G-module V satisfies:

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

  (II) $d(G/C_G(V)) < d(G)$.

  In other words, for each $N \in \mathcal{N}$, the minimal normal subgroups of G/N give rise to irreducible G-modules $V \in \mathcal{W}$.

Remark 2

Observe that $d(G/C_G(V)) \leq d(G) = d$. When $d(G/C_G(V)) < d$, 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 $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

Remark 2

Observe that $d(G/C_G(V)) \leq d(G) = d$. When $d(G/C_G(V)) < d$, 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 $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

Indeed, if $\delta_G(V) \leq (d - 1 - \theta_G(V))n_V$ and $d(G/C_G(V)) < d$, then $d(G/R_G(V)) \leq d - 1$ and hence there exist $x_1, \ldots, x_{d-1} \in G$ with $G = \langle x_1, \ldots, x_{d-1}, R_G(V)\rangle$. By a result of Gaschütz, there exist $r_1, \ldots, r_d \in R_G(V)$ with $G = \langle x_1 r_1, \ldots, x_{d-1} r_{d-1}, r_d\rangle$: since $R_G(V) = \bigcap_{M \in \mathcal{M}_V} M$, we have $r_d \in M \cap \{x_1 r_1, \ldots, x_{d-1} r_{d-1}, r_d\}$ for every $M \in \mathcal{M}_V$.

REMARK 3

The condition $\delta_G(V) \geq (d - 1 - \theta_G(V))n_V + 1$ in general is not necessary when $d(G/C_G(V)) = d$. Indeed, let $\tilde{G}$ be the soluble primitive permutation group $V \rtimes G/C_G(V)$: $d(\tilde{G}) = d$ and a sufficient condition for the existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ is that $\cap_{1 \leq i \leq d} \operatorname{supp}(\tilde{g}_i) \neq \emptyset$. This always holds true when $d = 3$:

REMARK 3

The condition $\delta_G(V) \geq (d-1-\theta_G(V))n_V + 1$ in general is not necessary when $d(G/C_G(V)) = d$. Indeed, let $\tilde{G}$ be the soluble primitive permutation group $V \rtimes G/C_G(V)$: $d(\tilde{G}) = d$ and a sufficient condition for the existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ is that $\cap_{1 \leq i \leq d} \mathrm{supp}(\tilde{g}_i) \neq \emptyset$. This always holds true when $d = 3$:

THEOREM

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

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 $\delta_G(V) \geq (d-1-\theta_G(V))n_V + 1$ holds or not.

Remark 3

The condition $\delta_G(V) \geq (d-1-\theta_G(V))n_V + 1$ in general is not necessary when $d(G/C_G(V)) = d$. Indeed, let $\tilde{G}$ be the soluble primitive permutation group $V \rtimes G/C_G(V)$: $d(\tilde{G}) = d$ and a sufficient condition for the existence of $M \in \mathcal{M}_V$ with $M \cap \{g_1, \ldots, g_d\} = \emptyset$ is that $\cap_{1 \leq i \leq d} \operatorname{supp}(\tilde{g}_i) \neq \emptyset$. This always holds true when $d = 3$:

Theorem

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

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 $\delta_G(V) \geq (d-1-\theta_G(V))n_V + 1$ holds or not.

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 $M \cap \{g_1, \ldots, g_d\} = \emptyset$.

Question

Let G be a primitive permutation group and let $d = d(G)$. Does $G = \langle g_1, \ldots, g_d \rangle$ implies $\bigcap_{1 \leq i \leq d} \mathrm{supp}(g_i) = \emptyset$?

Question

Let G be a primitive permutation group and let $d = d(G)$. Does $G = \langle g_1, \ldots, g_d \rangle$ implies $\bigcap_{1 \le i \le d} \operatorname{supp}(g_i) = \emptyset$?

A weaker result in this direction is the following:

Theorem

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

This does not remain true if we replace "primitive" with "transitive".
Take $g_1 = (1,2,3,4)$, $g_2 = (5,7)$, $g_3 = (1,5)(2,6)(3,7)(4,8)$:
$G = \langle g_1, g_2, g_3 \rangle$ is a Sylow 2-subgroup of $\operatorname{Sym}(8)$: in particular $d(G) = 3$ but $\operatorname{supp}(g_1) \cap \operatorname{supp}(g_2) = \emptyset$.

THEOREM

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

Ingredients of the proof:

- O'Nan-Scott theorem.
- J. McLaughlin's classification of irreducible finite dimensional linear groups generated by transvections over the field of 2 elements (1969).
- Classification of finite primitive groups admitting a non-identity element fixing at least half of the points of the domain (R. Guralnick and K. Magaard, 1998).
- If N is the unique minimal normal subgroup of a finite group G then $d(G) \leq \max\{2, d(G/N)\}$ (AL, F. Menegazzo, 1997).

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 $\mathrm{Aut}(S)$ on S^d and let Ω_d be the set of $\mathrm{Aut}(S)$-orbits on the set of d-tuples $(x_1, \ldots, x_d) \in S^d$ such that:

- $S = \langle x_1, \ldots, x_d \rangle$;
- for every maximal subgroup M of S, there exists i with $x_i \in M$.

We use the notation $[(x_1, \ldots, x_d)]$ to denote the $\mathrm{Aut}(S)$-orbit containing $(x_1, \ldots, x_d) \in \Omega_d$. We define the graph Γ_d with vertex set Ω_d and where two distinct vertices $[(x_1, \ldots, x_d)]$ and $[(y_1, \ldots, y_d)]$ are declared to be adjacent if and only if, for every $\gamma \in \mathrm{Aut}(S)$, there exists $i \in \{1, \ldots, d\}$ (which may depend on γ) such that $y_i = x_i^\gamma$.

THEOREM

Let $\omega(\Gamma_d)$ be the clique number of Γ_d and let $P_S(k)$ be the probability of generating S with k-elements. We have

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