UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede amministrativa: Università degli studi di Padova

Dipartimento di Matematica

SCUOLA DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE
INDIRIZZO MATEMATICA
CICLO XXV

COVERINGS OF GROUPS BY SUBGROUPS

Martino Garonzi

Direttore della scuola: Ch.mo Prof. Paolo Dai Pra

Coordinatore d'indirizzo: Ch.mo Prof. Franco Cardin

Supervisore: Ch.mo Prof. Andrea Lucchini

Dottorando: Martino Garonzi

January 17, 2013

I started writing about the first brick, and
the second brick, and then by the third brick
it all started to come and I couldn't stop.

They thought I was crazy, and they
kept kidding me, but here it all is. [1]

[1] [Robert Pirsig, Zen and the Art of Motorcycle Maintenance]

Contents

1. Abstract

Given a finite non-cyclic group G, a "cover" of G is a family $\mathcal{H}$ of proper subgroups of G such that $\bigcup_{H \in \mathcal{H}} H = G$. A "normal cover" of G is a cover $\mathcal{H}$ of G with the property that $gHg^{-1} \in \mathcal{H}$ for every $H \in \mathcal{H}$, $g \in G$. Define the "covering number" $\sigma(G)$ of G to be the smallest size of a cover of G, and the "normal covering number" $\gamma(G)$ of G to be the smallest number of conjugacy classes of a normal cover of G. If G is cyclic we pose $\sigma(G) = \gamma(G) = \infty$, with the convention that $n < \infty$ for every integer n. In this Ph.D. thesis we study these two invariants. Andrea Lucchini and Eloisa Detomi conjectured that if G is a finite non-abelian group such that $\sigma(G) < \sigma(G/N)$ for every non-trivial normal subgroup N of G then G is "monolithic", i.e. admits a unique minimal normal subgroup. In this thesis we deal with this conjecture and give a partial reduction to the almost-simple case. This requires good lower and upper bounds for the covering number of monolithic groups, which we prove along the way. We give an asymptotic estimate for the number of covering numbers of monolithic groups G with non-abelian minimal normal subgroup N such that G/N is cyclic. We also compute the covering number of a direct product of groups, and also its normal covering number in case the factors do not admit isomorphic abelian quotients. We prove several upper bounds for $\gamma(G)$ and deal with the following conjecture, formulated by me and Attila Maróti: if G is any non-cyclic finite group and p is the largest prime divisor of $|G|$ then $\gamma(G) \leq p + 1$. We reduce the conjecture to the almost-simple case and deal with alternating groups, sporadic groups and some linear groups.

2. Sommario

Dato un gruppo finito non ciclico G, un "ricoprimento" di G è una famiglia $\mathcal{H}$ di sottogruppi propri di G tale che $\bigcup_{H \in \mathcal{H}} H = G$. Un "ricoprimento normale" di G è un ricoprimento $\mathcal{H}$ di G tale che $gHg^{-1} \in \mathcal{H}$ per ogni $H \in \mathcal{H}$, $g \in G$. Definiamo "numero di ricoprimento" $\sigma(G)$ di G come la più piccola cardinalità di un ricoprimento di G, e definiamo "numero di ricoprimento normale" $\gamma(G)$ di G come il più piccolo numero di classi di coniugio di un ricoprimento normale di G. Se G è ciclico poniamo $\sigma(G) = \gamma(G) = \infty$, con la convenzione che $n < \infty$ per ogni intero n. In questa tesi di dottorato studiamo questi due invarianti. Andrea Lucchini ed Eloisa Detomi hanno congetturato che se G è un gruppo finito non abeliano tale che $\sigma(G) < \sigma(G/N)$ per ogni sottogruppo normale non banale N di G allora G è "monolitico", cioè ammette un unico sottogruppo normale minimale. In questa tesi affrontiamo questa congettura e diamo una riduzione parziale al caso almost-simple. Questo richiede buone stime da sopra e da sotto per il numero di ricoprimento dei gruppi monolitici, che trattiamo strada facendo. Diamo una stima asintotica del numero di numeri di ricoprimento di gruppi monolitici G con sottogruppo normale minimale N non abeliano tale che G/N è ciclico. Calcoliamo inoltre il numero di ricoprimento di un prodotto diretto di gruppi, e il suo numero di ricoprimento normale nel caso i fattori non ammettano quozienti abeliani isomorfi. Dimostriamo varie stime dall'alto per $\gamma(G)$ e affrontiamo la seguente congettura, formulata da me e Attila Maróti: se G è un qualsiasi gruppo finito non ciclico e p è il più grande divisore primo di $|G|$ allora $\gamma(G) \leq p+1$. Riduciamo la congettura al caso almost-simple e trattiamo i gruppi alterni, i gruppi sporadici e alcuni tra i gruppi lineari.

3. Basics and technical results

The following basic definitions and results will be used througout the thesis without pointing to this section for explainations. We give [**Rob**] as a reference. Let G be a finite group.

0.1. *$H \leq G$ will mean that H is a subgroup of G, and $H \trianglelefteq G$ will mean that H is a normal subgroup of G. "$H < G$ (respectively $H \triangleleft G$)" will mean "$H \leq G$ (respectively $H \trianglelefteq G$) and $H \neq G$".*

0.2 (Supplement, complement). *Let $H \leq G$, $N \trianglelefteq G$. We say that H is a **supplement** of N in G, or that H supplements N in G, if $HN = G$. We say that H is a **complement** of N in G, or that H complements N in G, if H supplements N and $H \cap N = \{1\}$. Note that if H complements N in G then $G/N \cong H$, and G is isomorphic to the semidirect product $N \rtimes H$ given by the conjugation action of H on N.*

0.3 (Normal core). *If $H \leq G$, H_G will denote the **normal core** of H in G, i.e. the intersection $H_G := \bigcap_{g \in G} g^{-1}Hg$. It is a normal subgroup of G contained in H with the following universal property: if $N \trianglelefteq G$ then $N \subseteq H$ if and only if $N \subseteq H_G$. H_G coincides with the kernel of the action of G of right (respectively, left) multiplication on the set $\{Hg \mid g \in G\}$ (respectively, $\{gH \mid g \in G\}$).*

0.4 (Commutator subgroup). *G' will denote the **commutator subgroup** , or **derived subgroup**, of G. It is the subgroup of G generated by the commutators, i.e. the elements of the form $[a, b] := aba^{-1}b^{-1}$, where $a, b \in G$. G' is a characteristic subgroup of G with the following universal property: if N is a normal subgroup of G then G/N is abelian if and only if $G' \subseteq N$.*

0.5 (Frattini subgroup). *$\Phi(G)$ will denote the **Frattini subgroup** of G, the intersection of the maximal subgroups of G. It is a characteristic subgroup of G with the following universal property: if N is a normal subgroup of G then $NH \neq G$ for every $H < G$ if and only if $N \subseteq \Phi(G)$. If $K \trianglelefteq G$ and $K \leq H \leq G$ then the factor group H/K is called "Frattini" if $H/K \trianglelefteq \Phi(G/K)$, it is called "non-Frattini" otherwise. Recall that the Frattini subgroup of a finite group is always nilpotent.*

0.6 (Minimal normal subgroup). *A normal subgroup N of G is said to be a **minimal normal subgroup** of G if $N \neq \{1\}$ and N does not contain non-trivial normal subgroups of G different from N. Any minimal normal subgroup of G is of the type $T^m = T \times \ldots \times T$ (m times) where T is a simple group. Recall that if T is a simple group then $\mathrm{Aut}(T^m) = GL(m, |T|)$ if T is abelian and $\mathrm{Aut}(T^m) \cong \mathrm{Aut}(T) \wr \mathrm{Sym}(m)$ if T is non-abelian.*

0.7 (Socle). *The **socle** of G, denoted $\mathrm{soc}(G)$, is the subgroup of G generated by the minimal normal subgroups of G. $\mathrm{soc}(G)$ is a characteristic subgroup of G, equal to the direct product of some of its minimal normal subgroups.*

0.8 (Monolithic group). *G is said to be **monolithic** if it admits exactly one minimal normal subgroup. In other words, G is monolithic if and only if $\mathrm{soc}(G)$ is a minimal normal subgroup of G.*

0.9 (Transitive group). *G is said to be **transitive** (of degree n) if it admits a subgroup (of index n) with trivial normal core. Equivalently, there exists a subgroup H of G of index n such that the action of right multiplication of G on the set $\{Hg \mid g \in G\}$ is faithful.*

0.10 (Imprimitivity block). *A "(imprimitivity) (G-)**block**" of an action of G on a set X is a subset $B \subseteq X$ with the property that for every $g \in G$, either $B^g = B$ or $B^g \cap B = \emptyset$. Clearly, X and $\{x\}$ - for every $x \in X$ - are always blocks, and they will be called the trivial blocks. G is said to be **imprimitive** if it admits a non-trivial block.*

0.11 (Invariant partition). *Suppose G acts on a set X. A G-**invariant partition** of X is a partition $\mathcal{U}$ of X such that $U^g \in \mathcal{U}$ for every $U \in \mathcal{U}$, $g \in G$. If G acts transitively then every G-invariant partition of X has the form $\{B^g \mid g \in G\}$ where B is a G-block.*

0.12 (Primitive group). *G is said to be **primitive** (of degree n) if it admits a maximal subgroup (of index n) with trivial normal core. Equivalently, there exists a subgroup H of G of index n such that the action of right multiplication of G on the set $\{Hg \mid g \in G\}$ is faithful and does not admit non-trivial blocks. If G is a primitive group,* $\mathrm{soc}(G)$ *can only be of one of the following types:*

- *(Type I) An abelian minimal normal subgroup of G;*
- *(Type II) A non-abelian minimal normal subgroup of G;*
- *(Type III) The product of exactly two non-abelian minimal normal subgroups of G.*

In primitive groups of type I or III the minimal normal subgroups have a common complement, which is a maximal subgroup.

0.13 (Composition factor). *A **composition factor** of a finite group G is a quotient H/K where H, K are subnormal subgroups of G, $K \lhd H$ and H/K is a simple group. Observe that a finite solvable group is precisely a finite group all of whose composition factors are abelian.*

0.14 (Chief factor). *A **chief factor** of a finite group G is a quotient H/K where $K \trianglelefteq G$ and H/K is a minimal normal subgroup of G/K. Observe that a nilpotent finite group is precisely a finite group all of whose chief factors are central. We say that H/K is "complemented" if it is complemented in G/K, i.e. if there exists a subgroup $R \leq G$ containing K such that $RH = G$ and $R \cap H = K$. Recall that an abelian chief factor of a finite group is non-Frattini if and only if it is complemented, and in this case each supplement is in fact a complement and a maximal subgroup.*

0.15. ***CFSG** will mean "Classification of the Finite Simple Groups", for which we refer to* [**Atl**].

3.1. Notations.

- If m is a positive integer, $\omega(m)$ will denote the number of distinct prime factors of m, and $\pi(m)$ will denote the number of prime numbers belonging to $\{1, \dots, m\}$.
- If G is a finite group, $m(G)$ will denote the minimal index of a proper subgroup of G.
- If G is a primitive monolithic group, $\ell_G(\mathrm{soc}(G))$ will denote the minimal index of a proper supplement of the socle $\mathrm{soc}(G)$ of G.
- Let G be a finite non-cyclic group. A "cover" of G will be a family $\mathcal{H}$ of proper subgroups of G with the property that $\bigcup_{H \in \mathcal{H}} H = G$. A "minimal cover" will be a cover $\mathcal{H}$ with $|\mathcal{H}|$ smallest possible. A "normal cover" will be a cover $\mathcal{H}$ with the property that for every $H \in \mathcal{H}$, $g \in G$ we have $g^{-1}Hg \in \mathcal{H}$. We define
  - $\sigma(G)$ to be the size of a minimal cover of G.
  - $\gamma(G)$ to be the smallest number of conjugacy classes of a normal cover of G.

4. Introduction

From now on every considered group will be assumed to be finite, unless specified otherwise. Given a non-cyclic group G, call $\sigma(G)$ - the **covering number** of G - the smallest number of proper subgroups of G whose union equals G. Note that there always exist minimal covers consisting of maximal subgroups. This notion has been introduced the first time by Cohn in 1994 [**Cohn**]. We usually call **cover** of G a family of proper subgroups of G which covers G, and **minimal cover** of G a cover of G consisting of exactly $\sigma(G)$ elements. If G is cyclic then $\sigma(G)$ is not well defined because no proper subgroup contains any generator of G; in this case we define $\sigma(G) = \infty$, with the convention that $n < \infty$ for every integer n.

REMARK 0.16. *If N is a normal subgroup of a group G then $\sigma(G) \leq \sigma(G/N)$, since every cover of G/N can be lifted to a cover of G.*

Given a family $\mathcal{H}$ of subsets of a group G which covers G, we say that $\mathcal{H}$ is "irredundant" if $\bigcup_{\mathcal{H} \ni K \neq H} K \neq G$ for every $H \in \mathcal{H}$. Clearly every minimal cover is irredundant, but the converse is false. Actually the notion of irredundant cover is much weaker than that of minimal cover: for example, if n is a positive integer then the cover of ${C_2}^n$ consisting of its non-trivial cyclic subgroups is irredundant of size $2^n - 1$ while ${C_2}^n$ has an epimorphic image isomorphic to $C_2 \times C_2$ so $\sigma({C_2}^n) = 3$.
We are interested in groups with finite covering number. The following result implies that in order to study the behaviour of the function which assigns to each group its covering number it is enough to consider finite groups.

THEOREM 0.17 (Neumann 1954). *Let G be an infinite group covered by a finite family $\mathcal{H}$ of cosets of subgroups of G, and suppose that $\mathcal{H}$ is irredundant. Then every $H \in \mathcal{H}$ has finite index in G.*

PROOF. For a proof see Lemma 4.17 in [**Neu**]. □

Indeed, if $\mathcal{H}$ is a minimal cover of G then by the Theorem $\bigcap_{H \in \mathcal{H}} H$ has finite index in G, hence its normal core N has also finite index and

$$\sigma(G/N) \leq |\mathcal{H}| = \sigma(G) \leq \sigma(G/N),$$

thus $\sigma(G) = \sigma(G/N)$. In other words we are reduced to consider the covering number of the finite group G/N.
Assume we want to compute the covering number of a group G. If there exists $N \trianglelefteq G$ with $\sigma(G) = \sigma(G/N)$ then we may consider as well the quotient G/N instead of G. This leads instantly to the following definition.

DEFINITION 0.18 (σ-elementary groups). *We say that a group G is "σ-elementary" if $\sigma(G) < \sigma(G/N)$ for every non-trivial normal subgroup N of G.*

Clearly, every group has a σ-elementary epimorphic image with the same covering number. It follows that the structure of the σ-elementary groups is of big interest. It was studied by Lucchini and Detomi in [**DLpr**]. They conjectured that every non-abelian σ-elementary group is monolithic (Conjecture 1.28).

4.1. New results obtained in the thesis.

In this Ph.D. thesis the following results are obtained.

(1) $\sigma(\mathrm{Alt}(5) \wr C_2) = 57$ (Theorem 2.71, cf. [**Gar2**]) and if G is a non-abelian σ-elementary group such that $\sigma(G) \leq 56$ then G is either affine or almost-simple (Corollary 2.16).
(2) The σ-elementary groups G with $\sigma(G) \leq 25$ are listed in Table 1 below, which assigns to each integer $3 \leq k \leq 25$ the list of σ-elementary groups with covering number k. In particular, it follows that there are no groups with covering number belonging to $\{19, 21, 22, 25\}$ (7 and 11 are not new: 7 was considered by Tomkinson [**Tom**], 11 by Lucchini and Detomi [**DLpr**]). This is what I proved in my master thesis (cf. [**Gar1**]).
(3) Let $\mathcal{G}$ be the family of monolithic groups G with non-abelian socle such that $G/\operatorname{soc}(G)$ is cyclic. Then there exists a constant C such that for every $x \in \mathbb{N}$, $|\{\sigma(G) \mid G \in \mathcal{G}, \sigma(G) \leq x\} \leq C\sqrt{x}$ (Theorem 2.21).
(4) If H_1, H_2 are two non-trivial groups then $H_1 \times H_2$ is either abelian or not σ-elementary, indeed either $\sigma(H_1 \times H_2) = \min(\sigma(H_1), \sigma(H_2))$ or there exists a prime p such that C_p is an epimorphic image of both H_1, H_2 and $\sigma(H_1 \times H_2) = p + 1$ (Theorem 2.22). This is the content of a joint work with A. Lucchini [**GL**].
(5) We obtain quite general upper bounds for $\sigma(G)$ when G is a monolithic group with non-abelian socle (Theorem 2.28 and Proposition 2.29).
(6) If all the non-abelian minimal sub-normal subgroups of a σ-elementary group G are either isomorphic to M_{11} or to $\mathrm{Alt}(n)$ where $n \geq 30$ admits a prime divisor smaller than or equal to $\sqrt[4]{n}$ then G is monolithic (Theorem 2.49). This is an instance of a more general result (Theorem 2.32).
(7) We give bounds and in some cases the exact value of $\sigma(G)$ when G is a primitive monolithic group with socle of the form $\mathrm{Alt}(n)^m$ and $G/\operatorname{soc}(G)$ cyclic (Theorem 2.50). This is part of a joint work with A. Maróti [**GM**] and my paper [**Gar2**].

Given a non-cyclic group G, call $\gamma(G)$ - the **normal covering number** of G - the smallest number of conjugacy classes of proper subgroups of G needed to cover G. In this thesis the following results are obtained.

(8) If the two groups H_1, H_2 have no common abelian factor group then
$$\gamma(H_1 \times H_2) = \min(\gamma(H_1), \gamma(H_2)).$$
(Theorem 3.6).
(9) We prove several upper bounds for $\gamma(G)$ (Propositions 3.7, 3.8, 3.9).
(10) Let G be a non-cyclic group, and suppose that whenever X is an almost simple section of G and $X/\operatorname{soc}(X)$ is cyclic, one of the following holds:
   - $\operatorname{soc}(X)$ is either alternating or sporadic,
   - $X = PSL(n, q)$ or $X = PGL(n, q)$ for some integer n and some prime-power q.

   Then $\gamma(G) \leq p + 1$, where p is the largest prime divisor of $|G|$ (Theorem 3.11).
(11) There exists a constant C such that for any group G, $\gamma(G) \leq Cp\log(p)$, where p is the largest prime divisor of $|G|$ (Theorem 3.16).

σ	Groups
3	$C_2 \times C_2$
4	$C_3 \times C_3, \mathrm{Sym}(3)$
5	$\mathrm{Alt}(4)$
6	$C_5 \times C_5, D_{10}, AGL(1,5)$
7	$\emptyset$
8	$C_7 \times C_7, D_{14}, 7:3, AGL(1,7)$
9	$AGL(1,8)$
10	$3^2:4, AGL(1,9), \mathrm{Alt}(5)$
11	$\emptyset$
12	$C_{11} \times C_{11}, 11:5, D_{22}, AGL(1,11)$
13	$\mathrm{Sym}(6)$
14	$C_{13} \times C_{13}, D_{26}, 13:3, 13:4, 13:6, AGL(1,13)$
15	$SL(3,2)$
16	$\mathrm{Sym}(5), \mathrm{Alt}(6)$
17	$2^4:5, AGL(1,16)$
18	$C_{17} \times C_{17}, D_{34}, 17:4, 17:8, AGL(1,17)$
19	$\emptyset$
20	$C_{19} \times C_{19}, AGL(1,19), D_{38}, 19:3, 19:6, 19:9$
21	$\emptyset$
22	$\emptyset$
23	M_{11}
24	$C_{23} \times C_{23}, D_{46}, 23:11, AGL(1,23)$
25	$\emptyset$

TABLE 1. The list of σ-elementary groups G with $3 \leq \sigma(G) \leq 25$.

CHAPTER 1

Known facts about the covering number

1. Some preliminary remarks and results

LEMMA 1.1. *Let G be a group, $H, A_1, \ldots, A_n$ subgroups of G such that $H(A_1 \cap \ldots \cap A_n) = G$. Let $A := A_1 \cup \ldots \cup A_n$. Then $|G| \cdot |H \cap A| = |H| \cdot |A|$.*

PROOF. Consider the function $\varphi : H \times A \to G$ given by $(h, a) \mapsto ha$. For $\ell \in G$ we have $(h, a) \in \varphi^{-1}(\ell)$ if and only if $ha = \ell$, i.e. $\ell a^{-1} = h \in H$, in particular $a \in H\ell$. This means that (h, a) is determined by the choice of a in $H\ell$, so $\varphi^{-1}(\ell)$ is in bijective correspondence with $H\ell \cap A$. Now write $\ell = kx$ with $k \in H$, $x \in A_1 \cap \ldots \cap A_n$ and obtain $H\ell \cap A = (H \cap A)x$. In particular $|\varphi^{-1}(\ell)| = |H \cap A|$ for every $\ell \in G$ and the result follows. □

The following lemma is one of our main tools in the study of the covering number.

LEMMA 1.2 ([**Tom**], Lemma 3.2). *Let G be a group, let N be a proper normal subgroup of G, and let $U_1, \ldots, U_h, V_1, \ldots, V_k$ be proper subgroups of G such that $U_1, \ldots, U_h$ contain N, $V_1, \ldots, V_k$ supplement N, and $\beta_1 \leq \ldots \leq \beta_k$, where $\beta_i = |G : V_i|$ for $i = 1, \ldots, k$.*

$$\text{If } U_1 \cup \ldots \cup U_h \cup V_1 \cup \ldots \cup V_k = G \text{ and } U_1 \cup \ldots \cup U_h \neq G \text{ then } \beta_1 \leq k.$$

Moreover, if $\beta_1 = k$ then $\beta_1 = \ldots = \beta_k = k$ and $V_i \cap V_j \leq U_1 \cup \ldots \cup U_h$ for every $i \neq j$ in $\{1, \ldots, k\}$.

PROOF. We follow the proof of Tomkinson. Write $|U_1 \cup \ldots \cup U_h| = \gamma|G|$. Note that $\gamma < 1$. Fix $i \in \{1, \ldots, k\}$. Since $V_i N = G$ Lemma 1.1 implies

$$|V_i \cap (U_1 \cup \ldots \cup U_h)| = \gamma|V_i| = \frac{\gamma}{\beta_i}|G|.$$

Therefore

$$|V_i - (U_1 \cup \ldots \cup U_h)| = \frac{1 - \gamma}{\beta_i}|G|.$$

Since $G - (U_1 \cup \ldots \cup U_h) = (V_1 \cup \ldots \cup V_k) - (U_1 \cup \ldots \cup U_h)$, we have

$$|(V_1 \cup \ldots \cup V_k) - (U_1 \cup \ldots \cup U_h)| = (1 - \gamma)|G|,$$

so since $G - (U_1 \cup \ldots \cup U_h) \subseteq \bigcup_{i=1}^k (V_i - (U_1 \cup \ldots \cup U_h))$,

$$(1 - \gamma)|G| \leq (1 - \gamma)|G|(\frac{1}{\beta_1} + \ldots + \frac{1}{\beta_k}).$$

Since $1 - \gamma > 0$ we obtain $1 \leq \sum_{i=1}^k \frac{1}{\beta_i} \leq \frac{k}{\beta_1}$, so $\beta_1 \leq k$.
If $\beta_1 = k$ then $\beta_1 = \ldots = \beta_k = k$ and the sets $V_i - (U_1 \cup \ldots \cup U_h)$ are pairwise disjoint. That is, $V_i \cap V_j \subseteq U_1 \cup \ldots \cup U_h$ for every $i \neq j$ in $\{1, \ldots, k\}$. □

Lemma 1.3. *Let G be a non-cyclic group.*

(1) *Write $G = H_1 \cup \ldots \cup H_n$ as union of $n = \sigma(G)$ proper subgroups. Let $\beta_i := |G : H_i|$ for $i = 1, \ldots, n$ and suppose that $\beta_1 \leq \ldots \leq \beta_n$. Then $\beta_1 < \sigma(G)$.*

(2) *Let $\mathcal{M}$ be a minimal cover of G consisting of maximal subgroups. If N is a proper normal subgroup of G and β is the minimal index of a proper supplement of N in G belonging to $\mathcal{M}$ then $\beta < \sigma(G)$.*

Proof. We prove (1). Since $1 \in H_1 \cap \ldots \cap H_n$ we clearly have

$$|G| < \sum_{i=1}^{n} |H_i| = |G| \sum_{i=1}^{n} \frac{1}{\beta_i} \leq \frac{|G|n}{\beta_1}.$$

The result follows.
We prove (2). If all members of $\mathcal{M}$ are supplements of N the result follows from (1). If not, the result follows from Lemma 1.2. □

It is easy to prove that no group can be written as union of two proper subgroups, in other words $\sigma(G) > 2$ for every group G. The case $\sigma(G) = 3$ was considered for the first time by Scorza:

Theorem 1.4 (Scorza 1926 [**Sco**]). *Let G be a group. Then $\sigma(G) = 3$ if and only if there exists $N \trianglelefteq G$ such that $G/N \cong C_2 \times C_2$.*

With the results we have listed so far, this theorem is easy to prove, and even better, we prove the following result. I am grateful to professor Boaz Tsaban who pointed this out to me.

Theorem 1.5 (Scorza's theorem revisited). *Let p be the smallest prime divisor of the order of the finite group G. Then $\sigma(G) = p + 1$ if and only if there exists $N \trianglelefteq G$ with $G/N \cong C_p \times C_p$.*

Proof. Recall the following well-known fact: if p is the smallest prime divisor of the size of a finite group G then every subgroup of G of index p is normal in G. Now, $(\Leftarrow)$ is clear since $\sigma(C_p \times C_p) = p + 1$. Let us prove $(\Rightarrow)$. Suppose $G = H_1 \cup H_2 \cup \ldots \cup H_{p+1}$ is the union of $p + 1$ proper subgroups, and let $\beta_i := |G : H_i|$ for $i = 1, 2, \ldots, p + 1$, with $\beta_1 \leq \beta_2 \leq \ldots \leq \beta_{p+1}$. Since p is the smallest prime divisor of $|G|$, Lemma 1.3 implies that $\beta_1 = p$ so H_1 is normal in G. Lemma 1.2 applied to $U_1 = H_1$, $h = 1$, $V_1 = H_2$, $V_2 = H_3, \ldots, V_k = H_{p+1}$, $k = p$ implies that $\beta_2 = \ldots = \beta_{p+1} = p$, therefore $G/H_1 \cap H_2 \cong C_p \times C_p$. □

We sometimes call the following fact "the intersection argument".

Lemma 1.6. *Let G be a non-cyclic group, and let $\mathcal{M}$ be a minimal cover of G consisting of maximal subgroups. Let H be a maximal subgroup of G such that $\sigma(H) > \sigma(G)$. Then $H \in \mathcal{M}$. In particular:*

(1) *if H is non-normal in G then $\sigma(G) > |G : H|$.*

(2) *if N is a non-Frattini abelian minimal normal subgroup of G and $\sigma(G) < \sigma(G/N)$ then $\sigma(G) \geq c + 1$, where c is the number of complements of N in G.*

Proof. $H = \bigcup_{M \in \mathcal{M}} M \cap H$ is a union of less than $\sigma(H)$ subgroups, so at least one of them must be unproper (by definition of $\sigma(H)$): $H \cap M = H$ for some $M \in \mathcal{M}$, thus $H = M$, H being maximal. Every conjugate of H is a maximal subgroup of G isomorphic to H, thus if H is not

normal then in every minimal cover of G there are all the $|G : H|$ conjugates of H. In particular $\sigma(G) \geq |G : H|$, and this inequality is in fact strict by 3.1. This proves (1).
(2) follows easily from (1) and the well-known fact that the complements of an abelian minimal normal subgroup are maximal subgroups. $\square$

For example, $\sigma(\mathrm{Sym}(6))$ was computed in [**S6**] in the following way:

EXAMPLE 1.7. $\mathrm{Sym}(6)$ *is covered by* $\mathrm{Alt}(6)$ *and the twelve subgroups isomorphic to* $\mathrm{Sym}(5)$*, so* $\sigma(\mathrm{Sym}(6)) \leq 13$*. Since* $\sigma(\mathrm{Sym}(5)) = 16 > 13 \geq \sigma(\mathrm{Sym}(6))$*, Lemma 1.6 implies that the twelve subgroups isomorphic to* $\mathrm{Sym}(5)$ *belong to every minimal cover of* $\mathrm{Sym}(6)$ *consisting of maximal subgroups. Since their union is not* $\mathrm{Sym}(6)$*, we deduce that* $\sigma(\mathrm{Sym}(6)) = 13$*.*

The argument of Example 1.7 will be generalized in Proposition 2.37 (4).

LEMMA 1.8. *Let G be a non-cyclic group. If $\mathcal{M}$ is a minimal cover of G consisting of maximal subgroups and g is a central element of prime order p which does not belong to every $M \in \mathcal{M}$ then $N := \bigcap_{K \in \mathcal{M}} K \trianglelefteq G$, $G/N \cong C_p \times C_p$ and $\sigma(G) = \sigma(G/N) = p+1$.*

PROOF. Let $L := \langle g \rangle$, and let $\mathcal{U} := \{M \in \mathcal{M} \mid M \not\supseteq L\}$. Since L is central, each $M \in \mathcal{U}$ is normal of index p. By Lemma 1.2 $|\mathcal{U}| \geq p$ and if M_1, M_2 are two distinct elements of $\mathcal{U}$ then $G/M_1 \cap M_2 \cong C_p \times C_p$, so $p \leq |\mathcal{U}| \leq \sigma(G) \leq p+1$, therefore since no member of $\mathcal{U}$ contains g we have $|\mathcal{U}| = p$ and $\sigma(G) = p+1$. Let M be the unique element of $\mathcal{M} - \mathcal{U}$. By Lemma 1.2 $M_1 \cap M_2 \subseteq M$, so M is normal of index p. If there would exist an element of $\mathcal{M}$ not containing $M_1 \cap M_2$ then since M_1, M_2 contain $M_1 \cap M_2$ by Lemma 1.2 we would have $2 + p \leq \sigma(G) = p+1$, a contradiction. It follows that $G/N \cong C_p \times C_p$. $\square$

We now deduce from the discussion above some basic properties of σ-elementary groups.

PROPOSITION 1.9. *Let G be a σ-elementary group.*

(1) *The Frattini subgroup of G is trivial: $\Phi(G) = \{1\}$.*
(2) *If G is abelian then there exists a prime p such that $G \cong C_p \times C_p$.*
(3) *If G is non-abelian then $Z(G) = \{1\}$.*
(4) *If G is nilpotent then it is abelian.*

PROOF. Let us prove (1). Let $\mathcal{M}$ be a minimal cover of G consisting of maximal subgroups. Then $\{M/\Phi(G) \mid M \in \mathcal{M}\}$ is a cover of $G/\Phi(G)$ of size $\sigma(G)$, therefore $\sigma(G/\Phi(G)) \leq \sigma(G) \leq \sigma(G/\Phi(G))$, i.e. $\sigma(G) = \sigma(G/\Phi(G))$ and the result follows as G is σ-elementary.
Let us prove (2). By (1) and the structure theorem of finite abelian groups, G is a direct product of elementary abelian groups. Let p be a prime for which G admits two copies of C_p in a decomposition (i.e. admits $C_p \times C_p$ as an epimorphic image). Then by Lemma 1.6 $p+1 \leq \sigma(G) \leq \sigma(C_p \times C_p) = p+1$, so $\sigma(G) = p+1$ and $G \cong C_p \times C_p$.
(3) follows easily from Lemma 1.8, and since any nilpotent group has non-trivial center, (4) follows from (3). $\square$

1.1. The nilpotent case.

COROLLARY 1.10. *Let G a non-cyclic nilpotent group. Then $\sigma(G) = p+1$ where p is the smallest prime divisor of $|G|$ such that the Sylow p-subgroup of G is not cyclic.*

PROOF. Let G/N be a σ-elementary epimorphic image of G such that $\sigma(G) = \sigma(G/N)$. Since G is nilpotent, G/N is also nilpotent and Proposition 1.9 implies $G/N \cong C_q \times C_q$ for some prime divisor q of $|G|$, in particular $\sigma(G) = q+1$ and the Sylow q-subgroup of G is not cyclic. Now let P be a Sylow p-subgroup of G. Since P is a non-cyclic p-group (in particular nilpotent), $\sigma(P) = p+1$ by Proposition 1.9, and since P is an epimorphic image of G, $q+1 = \sigma(G) \leq \sigma(P) = p+1$, thus $q = p$ by minimality of p. $\square$

2. On the structure of σ-elementary groups

Recall that if G is any group, a G-group is a group A endowed with a homomorphism $f : G \to \mathrm{Aut}(A)$. If $a \in A$ and $g \in G$, the element $f(g)(a)$ is usually denoted a^g if no ambiguity is possible.

DEFINITION 1.11. *Let G be a group, and let A, B be two G-groups.*

- *A, B are said to be G-isomorphic (written $A \cong_G B$) if there exists an isomorphism $\varphi : A \to B$ such that $a^{\varphi g} = a^{g\varphi}$ for every $g \in G$.*
- *A, B are said to be G-equivalent (written $A \sim_G B$) if there exist isomorphisms*

$$\varphi : A \longrightarrow B\ , \quad \Phi : G \ltimes A \longrightarrow G \ltimes B$$

such that the following diagram commutes:

$$\begin{tikzcd} \{1\} \arrow[r] & A \arrow[r] \arrow[d, "\varphi"] & G \ltimes A \arrow[r] \arrow[d, "\Phi"] & G \arrow[r] \arrow[d, equal] & \{1\} \\ \{1\} \arrow[r] & B \arrow[r] & G \ltimes B \arrow[r] & G \arrow[r] & \{1\} \end{tikzcd}$$

EXAMPLE 1.12. *Suppose A, B are G-isomorphic via $\varphi : A \to B$. Then they are G-equivalent via $\Phi : G \ltimes A \to G \ltimes B$ defined by $(ga)^\Phi := ga^\varphi$.*

Recall that if B is a G-group then a 1-cocycle between G and B is a map $\beta : G \to B$ such that $(gh)^\beta = (g^\beta)^h h^\beta$ for any $g, h \in G$. The set of 1-cocycles between G and B is denoted $Z^1(G, B)$. Note that if $\beta \in Z^1(G, B)$ then the map $\nu : G \to \mathrm{Aut}(B)$ defined by $b^{\nu(g)} := b^{gg^\beta} = (g^\beta)^{-1} b^g (g^\beta)$ is a homomorphism which makes B a G-group. It will be denoted B_β. Note that if B is abelian then $B_\beta \cong_G B$.

LEMMA 1.13. *Let A, B be two G-groups. They are G-equivalent if and only if there exists a 1-cocycle $\beta \in Z^1(G, B)$ such that $A \cong_G B_\beta$.*

PROOF. If $A \sim_G B$ via $\varphi : A \to B$ and $\Phi : G \ltimes A \to G \ltimes B$ define $\beta \in Z^1(G, B)$ by $g^\beta := g^{-1} g^\Phi$. If $A \cong_G B_\beta$ via φ define $\Phi : G \ltimes A \to G \ltimes B$ by $(ga)^\Phi := gg^\beta a^\varphi$. $\square$

COROLLARY 1.14. *Two abelian G-groups are G-equivalent if and only if they are G-isomorphic.*

If A is a G-group denote by $C_G(A)$ the centralizer of A in G, i.e.
$C_G(A) := \{g \in G \mid a^g = a \ \forall a \in A\}$. Note that if A, B are two G-isomorphic groups then
$C_G(A) = C_G(B)$.

EXAMPLE 1.15. *Let $T_1 = T_2 = T$ be a non-abelian group with trivial center, and let $G := T_1 \times T_2$. G-conjugation gives $T_1 \times \{1\}$ and $\{1\} \times T_2$ the structure of G-groups. Observe that $C_G(T_1 \times \{1\}) = \{1\} \times T_2$ and $C_G(\{1\} \times T_2) = T_1 \times \{1\}$, in particular $T_1 \times \{1\}$ and $\{1\} \times T_2$ are not G-isomorphic. But they are G-equivalent: define*

$$\varphi : T_1 \times \{1\} \to \{1\} \times T_2, \qquad (t, 1) \mapsto (1, t),$$
$$\Phi : G \ltimes (T_1 \times \{1\}) \to G \ltimes (\{1\} \times T_2), \qquad (x, y) * (t, 1) \mapsto (x, y) * (1, y^{-1}xt).$$

In other words, $\{1\} \times T_2 \cong_G (T_1 \times \{1\})_\beta$ where $\beta \in Z^1(G, \{1\} \times T_2)$ is defined by $(x, y)^\beta := (1, y^{-1}x)$.

P. Jiménez-Seral and J. P. Lafuente [**SerLaf**] proved the following very interesting and useful result:

PROPOSITION 1.16. *Let A, B be two chief factors of a group G, with the structure of G-groups given by conjugation. They are G-equivalent if and only if either A, B are G-isomorphic between them or A, B are G-isomorphic to the two minimal normal subgroups of a primitive epimorphic image of type III of G.*

Let $A = H/K$ be a chief factor of a group G. Recall that H/K is called "Frattini" if $H/K \subseteq \Phi(G/K)$. Denote by:

- $I_G(A)$ the set of elements of G which induce by conjugation an inner automorphism of A;
- $R_G(A)$ the intersection of the normal subgroups N of G contained in $I_G(A)$ with the property that $I_G(A)/N$ is non-Frattini and G-equivalent to A.

The quotient $I_G(A)/R_G(A)$ is called the A-crown of G. Let us list some of its properties.

PROPOSITION 1.17 ([**DLpr**], Proposition 4). *Let A be a chief factor of a group G. If $R \neq I$ then $I/R = \mathrm{soc}(G/R)$ is a direct product of $\delta_G(A)$ minimal normal subgroups G-equivalent to A. If $R = I$ set $\delta_G(A) = 0$. If $\delta_G(A) \geq 2$ then any two different minimal normal subgroups of G/R have a common complement, which is a maximal subgroup of G/R. Every chief series of G contains exactly $\delta_G(A)$ non-Frattini chief factors G-equivalent to A. In particular, in a chief series passing through R and I, the unique non-Frattini chief factors G-equivalent to A are those between R and I. In particular, if H/K is a non-Frattini chief factor of G then $H/K \sim_G A$ if and only if $KR < HR \leq I$.*

Now we will list and prove some of the facts proved by Lucchini and Detomi in [**DLpr**] about σ-elementary groups.

PROPOSITION 1.18 ([**DLpr**], Proposition 7). *Let N be a non-solvable normal subgroup of a group G. Then $\sigma(G) \leq |N| - 1$. In particular, if N is complemented in G by a maximal subgroup then $\sigma(G) = \sigma(G/N)$.*

PROOF. The idea is to prove that $\bigcup_{1 \neq n \in N} C_G(n) = G$. If there exists $g \in G$ such that $n^g \neq n$ for every $1 \neq n \in N$ then $\langle g \rangle$ acts fixed-point-freely on N, and this contradicts the fact that N is non-solvable (cf. [**Wfpf**], and note that this result relies on CFSG).

Let now M be a maximal subgroup of G complementing N, and suppose by contradiction $\sigma(G) < \sigma(G/N) = \sigma(M)$. By Lemma 1.6 $|N| = |G : M| \leq \sigma(G) \leq |N| - 1$, a contradiction. $\square$

2.1. Abelian minimal normal subgroups.

LEMMA 1.19. *Let A, B be two abelian minimal normal subgroups of a group G, with the structure of G-groups given by conjugation. If A, B have a common complement M in G then they are G-isomorphic.*

PROOF. Note that $M \cap AB$ is a common complement of A, B in AB, indeed by the Dedekind rule $A(M \cap AB) = AM \cap AB = G \cap AB = AB$ and $(M \cap AB)B = MB \cap AB = G \cap AB = AB$, and $(M \cap AB) \cap A = (M \cap A) \cap AB = \{1\} \cap AB = \{1\}$, $(M \cap AB) \cap B = (M \cap B) \cap AB = \{1\} \cap AB = \{1\}$. Since A, B are abelian, and $A \cap B = \{1\}$, $AB \cong A \times B$ is abelian and $M \cap AB \trianglelefteq AB$. The (canonical) G-isomorphism is given by $A \cong_G AB/(M \cap AB) \cong_G B$. $\square$

PROPOSITION 1.20 ([**DLpr**], Proposition 10). *Let G be a group. If V is a complemented normal abelian subgroup of G and $V \cap Z(G) = \{1\}$ then $\sigma(G) \leq 2|V| - 1$. In particular, if V is a minimal normal subgroup, then $\sigma(G) \leq 1 + q + \ldots + q^n$ where $q = |\operatorname{End}_G(V)|$ and $|V| = q^n$.*

PROOF. Let H be a complement of V in G. The idea is to show that G is covered by the family $\{H^v \mid v \in V\} \cup \{C_H(v)V \mid 1 \neq v \in V\}$. We omit the details. $\square$

COROLLARY 1.21. *Let G be a non-abelian σ-elementary group, and let N be an abelian minimal normal subgroup of G. Then $\delta_G(N) = 1$ and N is the unique abelian minimal normal subgroup of G.*

PROOF. By Proposition 1.9 (1) and (3), $\Phi(G) = Z(G) = \{1\}$. Suppose by contradiction that $\delta_G(N) \geq 2$. By a result in [**AGco**], the number c of complements of N in G is

$$\begin{aligned} c &= |\operatorname{Der}(G/N, N)| = |\operatorname{End}_{G/N}(N)|^{\delta_G(N)-1} |\operatorname{Der}(G/C_G(N), N)| \geq \\ &\geq |\operatorname{End}_{G/N}(N)| \cdot |\operatorname{Der}(G/C_G(N), N)| \geq 2|N|. \end{aligned}$$

Since $\sigma(G) < \sigma(G/N)$, by Lemma 1.6 and Proposition 1.20

$$2|N| < c + 1 \leq \sigma(G) < 2|N|,$$

a contradiction. We conclude that $\delta_G(N) = 1$. Assume now by contradiction that W is an abelian minimal normal subgroup of G such that $W \neq N$. Since $\delta_G(N) = 1$, W and N are not G-equivalent, in particular they do not have a common complement by Lemma 1.19. Observe that N has at least $|N|$ complements, W has at least $|W|$ complements, $\sigma(G) < \sigma(G/N)$ and $\sigma(G) < \sigma(G/W)$. We deduce from Lemma 1.6 and Proposition 1.20 that

$$\min\{2|N|, 2|W|\} \leq |N| + |W| \leq \sigma(G) < \min\{2|N|, 2|W|\},$$

a contradiction. $\square$

2.2. The solvable case. Tomkinson [**Tom**, Theorem 2.2] computed the covering number of solvable groups:

THEOREM 1.22 (Tomkinson). *If G is a solvable non-cyclic group then $\sigma(G) = q + 1$ where q is the order of the smallest chief factor of G with more than one complement.*

Let us re-interpret and re-prove this result using the notion of σ-elementary group. We first recall a very useful result of Gaschütz about solvable groups.

THEOREM 1.23 (Gaschütz [**Gasc**]). *Let G be a solvable group acting faithfully and irreducibly on an elementary abelian p-group V. Then every chief factor of G has size strictly smaller than $|V|$.*

THEOREM 1.24. *If G is a solvable non-abelian and σ-elementary group then $\sigma(G) = |\operatorname{soc}(G)| + 1$, $G/\operatorname{soc}(G)$ is cyclic, $\operatorname{soc}(G)$ is complemented in G, the complements of $\operatorname{soc}(G)$ in G are pairwise conjugated and a minimal cover of G consists of $\operatorname{soc}(G)$ together with its $|\operatorname{soc}(G)|$ complements.*

PROOF. We argue by induction on $|G|$. By Corollary 1.21 G is monolithic, i.e. $\operatorname{soc}(G)$ is a minimal normal subgroup of G. The inequality $|\operatorname{soc}(G)| + 1 \leq \sigma(G)$ follows then from Proposition 1.9(1) and Lemma 1.6, since the conjugacy classes of complements of $\operatorname{soc}(G)$ have size $|\operatorname{soc}(G)|$. Suppose $G/\operatorname{soc}(G)$ is non-cyclic. Then by the induction hypothesis there exists a chief factor V of $G/\operatorname{soc}(G)$ such that $|\operatorname{soc}(G)| + 1 \leq \sigma(G) < \sigma(G/\operatorname{soc}(G)) = |V| + 1$. It follows that $|\operatorname{soc}(G)| < |V|$, and this contradicts Theorem 1.23. Therefore $G/\operatorname{soc}(G)$ is cyclic. Let $k = |\operatorname{soc}(G)|$, and let $\{M_1, M_2, \ldots, M_k\}$ be a conjugacy class of complements of $\operatorname{soc}(G)$ in G. Fix $i \neq j$ in $\{1, \ldots, k\}$. Since M_i, M_j are maximal and cyclic, $M_i \cap M_j \trianglelefteq \langle M_i, M_j \rangle = G$ so $M_i \cap M_j = \{1\}$. It follows that

$$|\operatorname{soc}(G) \cup M_1 \cup \ldots \cup M_k| = |\operatorname{soc}(G)| + |\operatorname{soc}(G)| \cdot (|G|/|\operatorname{soc}(G)| - 1) = |G|,$$

therefore $\{\operatorname{soc}(G), M_1, \ldots, M_k\}$ is a cover of G consisting of $|\operatorname{soc}(G)| + 1$ subgroups, and hence $\sigma(G) = |\operatorname{soc}(G)| + 1$. In particular if c denotes the number of complements of $\operatorname{soc}(G)$ in G then Lemma 1.6 implies that $|\operatorname{soc}(G)| + 1 \leq c + 1 \leq \sigma(G) = |\operatorname{soc}(G)| + 1$, hence $c = |\operatorname{soc}(G)|$, i.e. the complements of $\operatorname{soc}(G)$ in G are pairwise conjugated. $\square$

2.3. The main conjecture.

THEOREM 1.25. *Let G be a non-abelian σ-elementary group, and let N be a minimal normal subgroup of G. Then $\delta_G(N) = 1$. In particular the minimal normal subgroups of G are pairwise non-G-equivalent.*

PROOF. If N is abelian the result is Corollary 1.21. So suppose N is non-abelian. If $\delta_G(N) \geq 2$ then there exists a maximal subgroup M of G such that M/M_G is a common complement of the two minimal normal subgroups NM_G/M_G and HM_G/M_G of G/M_G, primitive of type III. In particular $M \cap N \subseteq M_G$ and $M \cap H \subseteq M_G$. Now, if $N \cap M_G \neq \{1\}$ then by minimality $N \subseteq M_G \subseteq M$, a contradiction, and similarly for H. This implies that M complements both N and H in G, so since $G/N \cong M$ we have $\sigma(G) < \sigma(G/N) = \sigma(M)$, thus by Lemma 1.6 $|N| + 1 \leq \sigma(G)$, contradicting Proposition 1.18. $\square$

Let us examine an important consequence of this fact.

PROPOSITION 1.26. *If G is a non-abelian σ-elementary group and $N_1, \dots, N_k$ are minimal normal subgroups of G such that $\mathrm{soc}(G) = N_1 \times \ldots \times N_k$ then $X_i := G/R_G(N_i)$ is a monolithic group with socle G-equivalent to N_i for every $i \in \{1, \dots, k\}$ and G is a subdirect product of $X_1, \dots, X_k$, in other words the canonical map $G \to X_1 \times \ldots \times X_k$ is injective.*

PROOF. The fact that X_i is monolithic with socle G-equivalent to N_i is clear from Proposition 1.17 and Theorem 1.25. Consider the canonical map

$$G \to X_1 \times \ldots \times X_k.$$

Its kernel is $R := R_G(N_1) \cap \ldots \cap R_G(N_k)$. We want to prove that $R = \{1\}$. Suppose by contradiction that $R \neq \{1\}$, and let N be a minimal normal subgroup of G contained in R. Then there exists $i \in \{1, \dots, k\}$ such that $N \sim_G N_i$, and Proposition 1.17 implies that $R_G(N_i)N \neq R_G(N_i)$, contradicting $N \subseteq R \subseteq R_G(N_i)$. □

DEFINITION 1.27. *Let G be a non-abelian σ-elementary group, and let N be a minimal normal subgroup of G. The quotient $G/R_G(N)$ will be called the* ***primitive monolithic group associated to*** *N.*

A natural question arises: how far is G from being a monolithic group? No example of a non-σ-elementary non-abelian non-monolithic group is known.

CONJECTURE 1.28 (Lucchini, Detomi [**DLpr**]). *Every non-abelian σ-elementary group is monolithic.*

CHAPTER 2

The new results about the covering number

1. Technical results deduced from the CFSG

In the following Lemma we collect some useful technical results about finite simple groups deduced from the CFSG.

LEMMA 2.1. *There exists an universal constant C such that for every non-abelian simple group S,*

(1) $2|\operatorname{Out}(S)| < m(S)$,
(2) $|\operatorname{Out}(S)| \le C\log(m(S))$ *and*
(3) $m(S)^2 \le |S|$.

PROOF. By inspection, using tables 5.1 in [**KL**] and Table 1 in [**DaLdp**] (about $m(S)$ see [**Coo**]). □

2. General notations for monolithic groups

We will use the following notations when necessary (the main reference is [**BEcl**, Remark 1.1.40]).

NOTATIONS 2.2. *Let G be a monolithic group with socle $N = \operatorname{soc}(G) = S_1 \times \cdots \times S_m$, where $S_1, \dots, S_m$ are pairwise isomorphic non-abelian simple groups. $X := N_G(S_1)/C_G(S_1)$ is an almost-simple group with socle $S := S_1C_G(S_1)/C_G(S_1) \cong S_1$. The minimal normal subgroups of $S^m = S_1 \times \ldots \times S_m$ are precisely its factors, $S_1, \dots, S_m$. Since automorphisms send minimal normal subgroups to minimal normal subgroups, it follows that G acts on the m factors of N. Let $\rho : G \to \operatorname{Sym}(m)$ be the homomorphism induced by the conjugation action of G on the set $\{S_1, \dots, S_m\}$. $K := \rho(G)$ is a transitive permutation group of degree m. By* [**BEcl**, Remark 1.1.40.13] *G embeds in the wreath product $X \wr K$. Let L be the subgroup of X generated by the following set:*

$$S \cup \{x_1 \cdots x_m \mid \exists k \in K : \ (x_1, \dots, x_m)k \in G\}.$$

Let T be a normal subgroup of X containing S and contained in L with the property that L/T has prime order if $L \neq S$, and $T = L$ if $L = S$. Let $c : L \to L/T$ be the canonical projection.

2.1. Maximal subgroups of primitive monolithic groups.

DEFINITION 2.3 ([**BEcl**], Definition 1.1.37). *Let $G = \prod_{i=1}^{n} S_i$ be a direct product of groups. A subgroup H of G is said to be "diagonal" (respectively, "full diagonal") if each projection $\pi_i : H \to S_i$ is injective (respectively, an isomorphism).*

2.4. *What follows is part of the O'Nan-Scott theorem (reference:* [**BEcl**, Remark 1.1.40]*). Let G be a primitive monolithic group with non-abelian socle $N = S^m$. Let H be a maximal subgroup of G such that $N \not\subseteq H$, i.e. $HN = G$, i.e. H supplements N. Suppose $N \cap H \neq \{1\}$, i.e. H does not complement N. Since N is the unique minimal normal subgroup of G and H is a maximal subgroup of G not containing N, $H = N_G(N \cap H)$. In the following let $X := N_G(S_1)/C_G(S_1)$ (it is an almost simple group with socle $S_1C_G(S_1)/C_G(S_1) \cong S$). There are two possibilities for the intersection $N \cap H$:*

(1) ***Product type***. *Suppose the projections $H \to S_i$ are not surjective. Then there exists a subgroup M of S such that $N_X(M)$ supplements S in X and elements $a_2, \dots, a_m \in S$ such that $H \cap N$ equals*
$$M \times M^{a_2} \times \ldots \times M^{a_m}.$$
(2) ***Diagonal type***. *Suppose the projections $H \to S_i$ are surjective. Then there exists an H-invariant partition Δ of $\{1, \dots, m\}$ into blocks for the action of H on $\{1, \dots, m\}$ such that $H \cap N$ equals*
$$\prod_{D \in \Delta} (H \cap N)^{\pi_D}$$
and for each $D \in \Delta$ the projection $(H \cap N)^{\pi_D}$ is a full diagonal subgroup of $\prod_{i \in D} S_i$.

The following is Lemma 2.1 in [**DaLpm**].

Lemma 2.5. *Let G be a primitive monolithic group with non-abelian socle, and let us use Notations 2.2. Let V be a maximal subgroup of X supplementing S, and let $M := V \cap S$. Then $N_G(M^m)$ is a maximal subgroup of G supplementing* $\mathrm{soc}(G)$.

Proposition 2.6. *Let G be a primitive monolithic group, and let N be its socle. If N is abelian then $\ell_G(N) = |N|$. Suppose N is non-abelian, and write $N = S^r$ with S a non-abelian simple group. Let H be a maximal subgroup of G supplementing N.*

- *If H complements N then $|G : H| = |N| = |S|^r$.*
- *If H has product type, $H = N_G(M \times M^{a_2} \times \ldots \times M^{a_r})$ for some subgroup M of S of the form $V \cap S$ where V is a maximal subgroup of X supplementing S, then $|G : H| = |S : M|^r$.*
- *If H has diagonal type, $H = N_G(\Delta)$, where Δ is a product of r/c diagonal subgroups of length c, a divisor of r larger than 1, then $|G : H| = |S|^{r-r/c}$.*

Moreover $\ell_G(N) \geq m(S)^r$.

Proof. Suppose N is abelian. Since G is primitive, N is non-Frattini, so it is complemented and each of its complements have index $\ell_G(N) = |N|$.
Suppose N is non-abelian. The three listed facts in the statement follow easily from the fact that $|G : H| = |N : H \cap N|$. Now let us prove that $\ell_G(N) \geq m(S)^r$. Since $m(S)^r \leq |S : M|^r$ for every proper subgroup M of S, we are reduced to show that $m(S)^r \leq |S|^{r-r/c}$ for every divisor $c > 1$ of r, and for this it is enough to show that $m(S)^r \leq |S|^{r/2}$, i.e. $m(S)^2 \leq |S|$. This is true by Lemma 2.1(3). ∎

2.2. The cyclic quotient case. Let G be a primitive monolithic group with $G/\operatorname{soc}(G)$ cyclic, and let us use Notations 2.2. Call $\pi_G : G \to G/\mathrm{soc}(G)$, $\pi_X : X \to X/S$ the natural projections.

LEMMA 2.7. *X/S is cyclic and $L = X$. More precisely, let $g \in G$ be such that $\pi_G(g)$ generates $G/soc(G)$, and write $g = (x_1, \dots, x_m)\delta$ with $x_1, \dots, x_m \in X$, $\delta \in Sym(m)$ an m-cycle. Then $\pi_X(x_1 x_{\delta(1)} \cdots x_{\delta(m-1)})$ generates X/S and $|G| = |S|^m \cdot m \cdot |X/S|$.*

PROOF. $N_G(S_1)/\mathrm{soc}(G)$ is a subgroup of $G/\mathrm{soc}(G)$, hence cyclic, and it projects onto $N_G(S_1)/S_1 C_G(S_1) = X/S$. Thus X/S is cyclic. Let $x \in X$ be such that $X/S = \langle xS \rangle$. For $i = 1, \dots, m$ write $x_i = s_i x^{k_i}$ for $s_i \in S$ and $k_i \in \mathbb{N}$. Let $k := \sum_{i=1}^m k_i$. Note that there exist $s_1', \dots, s_m' \in S$ such that $g^m = (s_1', \dots, s_m')(x^k, \dots, x^k)$. Therefore $(x^k, \dots, x^k)\mathrm{soc}(G)$ generates $G \cap X^m/\mathrm{soc}(G)$. Since $N_G(S_1) \subseteq X^m \cap G$, this implies that $x^k S = \pi_X(x^k)$ generates X/S, and the result follows. □

We may assume that there exists $g \in G$ such that $\langle g\,\mathrm{soc}(G) \rangle = G/\operatorname{soc}(G)$ and g has the form $(1, \dots, 1, x)\delta$ where $\delta = (1 \dots m) \in K$ and $x \in X$ is such that $X/S = \langle xS \rangle$.
Indeed, let $(x_1, \dots, x_m)\delta \in G$ generate G modulo $\mathrm{soc}(G)$, where $x_1, \dots, x_m \in X$ and $\delta \in K$ is an m-cycle. Up to conjugate by a suitable element of $\mathrm{Sym}(m)$ we may assume that δ is the m-cycle $(1 \dots m)$. We want to find $y_1, \dots, y_m \in \mathrm{Aut}(S)$ such that $((x_1, \dots, x_m)\delta)^{(y_1, \dots, y_m)} = (1, \dots, 1, x)\delta$ as required. We have

$$\begin{aligned}((x_1, \dots, x_m)\delta)^{(y_1, \dots, y_m)} &= (y_1^{-1}x_1, \dots, y_m^{-1}x_m)(y_2, \dots, y_m, y_1)\delta = \\ &= (y_1^{-1}x_1y_2, y_2^{-1}x_2y_3, \dots, y_{m-1}^{-1}x_{m-1}y_m, y_m^{-1}x_my_1)\delta.\end{aligned}$$

It suffices to choose $y_1 = 1$, $y_2 = x_1^{-1}$, $y_3 = (x_1x_2)^{-1}$, ..., $y_m = (x_1 \cdots x_{m-1})^{-1}$, and $x = x_1 \cdots x_m$.

3. Determining small σ-elementary groups

We start by listing some known results.

PROPOSITION 2.8 ([**DLcr**] Proposition 11). *Let A be a chief factor of a group G and let X be a direct product of minimal normal subgroups G-equivalent to A. If H is a subgroup of G such that $HX = HR_G(A) = G$ then $H = G$.*

DEFINITION 2.9 ([**DLpr**], Definition 15). *Let X be a monolithic primitive group with socle N. If Ω is an arbitrary union of cosets of N in X define $\sigma_\Omega(X)$ to be the smallest number of supplements of N in X needed to cover Ω. Define*

$$\sigma^*(X) := \min\{\sigma_\Omega(X) \mid \Omega = \bigcup_i \omega_i N,\ \langle \Omega \rangle = X\}. \tag{1}$$

This useful notion provides a lower bound of a σ-elementary group in terms of the primitive monolithic groups associated to its minimal normal subgroups. The following is the best lower bound known so far.

Proposition 2.10 ([**DLpr**], Proposition 16). *Let G be a non-abelian σ-elementary group, and let $\mathrm{soc}(G) = N_1 \times \ldots \times N_n$, $X_1, \ldots, X_n$ the primitive monolithic groups associated to $N_1, \ldots, N_n$ respectively. Then*

$$\sigma^*(X_1) + \ldots + \sigma^*(X_n) \leq \sigma(G).$$

Proof. Let $\mathcal{M}$ be a minimal cover of G. For $i \in \{1, \ldots, n\}$ define

$$\mathcal{M}_{\neg N_i} := \{M \in \mathcal{M} \mid M \not\geq N_i\}.$$

Note that each $\mathcal{M}_{\neg N_i}$ is non-empty (otherwise every $M \in \mathcal{M}$ would contain N_i, so $\sigma(G) = \sigma(G/N_i)$). Moreover if $i \neq j$ then $\mathcal{M}_{\neg N_i} \cap \mathcal{M}_{\neg N_j} = \emptyset$. Indeed, if $M \in \mathcal{M}$ does not contain N_i and N_j with $i \neq j$ then $N_i M_G/M_G$ and $N_j M_G/M_G$ are minimal normal subgroups of the primitive groups G/M_G, in particular $N_i \sim_G N_j$, contradicting Theorem 1.25.
We are reduced to prove that $|\mathcal{M}_{\neg N_i}| \geq \sigma^*(X_i)$ for $i = 1, \ldots, n$. Fix $i \in \{1, \ldots, n\}$, and let $N := N_i$, $X := X_i$, $R := R_G(N)$ and $\pi : G \to G/R = X$ the canonical projection. Let $\mathcal{M}_i := \mathcal{M} - \mathcal{M}_{\neg N_i}$ and

$$\Omega := \bigcup_{g \in G - \bigcup_{M \in \mathcal{M}_i} M} \pi(g).$$

Since $\mathcal{M}$ is a minimal cover of G we have $\Omega \neq \emptyset$. Moreover, Ω is a union of cosets of N in X. Suppose $\langle \Omega \rangle = H < X$ is a proper subgroup of X. Then G is covered by $\mathcal{M}_i \cup \{\pi^{-1}(H)\}$, and each element of this family contains N_i, so $|\mathcal{M}_i| + 1 \leq \sigma(G) < \sigma(G/N_i) \leq |\mathcal{M}_i| + 1$, contradiction. We deduce that $\langle \Omega \rangle = X$.
Since $\sigma_\Omega(X) \geq \sigma^*(X)$, it is enough to prove that $|\mathcal{M}_{\neg N_i}| \geq \sigma_\Omega(X)$. By Proposition 2.8 every $M \in \mathcal{M}_{\neg N_i}$ contains R, so M/R is a maximal subgroup of X supplementing N_i. Clearly, as $\bigcup_{M \in \mathcal{M}_{\neg N_i}} M$ covers $G - \bigcup_{M \in \mathcal{M}_i} M$, we have that $\bigcup_{M \in \mathcal{M}_{\neg N_i}} M/R$ covers Ω. Therefore $|\mathcal{M}_{\neg N_i}| = |\{M/R \mid M \in \mathcal{M}_{\neg N_i}\}| \geq \sigma_\Omega(X)$. ☐

This yields a couple of interesting corollaries. For a primitive monolithic group X with socle N denote by $\ell_X(N)$ the minimal index of a proper supplement of N in X.

Corollary 2.11. *Let X be a primitive monolithic group. Then*

$$\sigma^*(X) \geq \ell_X(\mathrm{soc}(X)).$$

In particular, if G is a non-abelian σ-elementary group and $N_1, \ldots, N_n$ are its minimal normal subgroups, $X_1, \ldots, X_n$ are the primitive monolithic groups associated to $N_1, \ldots, N_n$ respectively then

$$\sum_{i=1}^{n} \ell_{X_i}(N_i) \leq \sum_{i=1}^{n} \sigma^*(X_i) \leq \sigma(G).$$

In particular, for every $i \in \{1, \ldots, n\}$ X_i has a primitivity degree at most $\sigma(G)$.

Proof. Let $N := \mathrm{soc}(G)$, $x \in X$, and let M be a supplement of N in X such that $xN \cap M \neq \emptyset$. Then $|xN \cap M| = |N \cap M| = |xN|/|X : M| \leq |xN|/\ell_X(N)$, therefore we need at least $\ell_X(N)$ supplements of N to cover xN. ☐

The following result was proved for the first time in [**Bha**].

COROLLARY 2.12. *For every fixed positive integer k, the set of σ-elementary groups G with $\sigma(G) = k$ is finite.*

PROOF. Let G be a σ-elementary group, and write $\mathrm{soc}(G) = N_1 \times \ldots \times N_n$. Let $X_1, \ldots, X_n$ be the primitive monolithic groups associated to $N_1, \ldots, N_n$ respectively. By Proposition 1.26 G embeds in $X_1 \times \ldots \times X_n$, so in order to conclude it suffices to bound the number of possibilities for n and each X_i in terms of $\sigma(G)$. By Corollary 2.11

$$n \leq \sum_{i=1}^{n} \ell_{X_i}(N_i) \leq \sum_{i=1}^{n} \sigma^*(X_i) \leq \sigma(G).$$

Since there are finitely many primitive groups with a given primitivity degree, the result follows. $\square$

COROLLARY 2.13. *Let H be a σ-elementary group and let N be a non-abelian minimal normal subgroup of H. Let G be the primitive monolithic group associated to N. If G/N has prime-power order then H is monolithic.*

PROOF. Suppose that $|G/N|$ is a power of the prime p. Note that if N is non-abelian, $N = S^r$ for some non-abelian simple group S, then considering the (transitive!) conjugation action of G on the r direct factors of N we find that r must be a power of p. If G/N is non-cyclic then $\sigma(G/N) = p + 1$ by Proposition 1.9, so Proposition 2.6 implies that

$$\sigma(H) \leq \sigma(G) \leq \sigma(G/N) = p + 1 \leq 2^p \leq \ell_G(N),$$

thus $H = G$ by Corollary 2.11. Suppose now that G/N is cyclic. In particular G/N admits only one maximal subgroup. In other words, a subgroup K of G generates G modulo N if and only if it contains an element $g \in G$ with the property that $\langle gN \rangle = G/N$. This implies that $\sigma(G) \leq \sigma^*(G) + \omega(|G/N|) = \sigma^*(G) + 1$. The result follows by Corollary 2.11. $\square$

The following is Lemma 18 in [**DLpr**].

LEMMA 2.14. *Let N be a normal subgroup of a group X. If a set of subgroups of X covers a coset yN of N in X, then it also covers every coset $y^\alpha N$ with α prime to $|y|$.*

PROOF. Let s be an integer such that $s\alpha \equiv 1 \mod |y|$. As s is prime to $|y|$, by Dirichlet's theorem there exist infinitely many primes in the arithmetic progression $\{s + |y|n \mid n \in \mathbb{N}\}$; we choose a prime $p > |X|$ in $\{s + |y|n \mid n \in \mathbb{N}\}$. Clearly, $y^p = y^s$. As p is prime to $|X|$, there exists an integer r such that $pr \equiv 1 \mod |X|$. Hence, if $yN \subseteq \cup_{i\in I} M_i$, for every $g \in y^\alpha N$ we have that $g^p \in (y^\alpha)^p N = (y^\alpha)^s N = yN \subseteq \cup_{i\in I} M_i$ and therefore also $g = (g^p)^r$ belongs to $\cup_{i\in I} M_i$. $\square$

LEMMA 2.15. *Let G be a monolithic group with non-abelian socle N. Then there exists a set $\{g_1 N, \ldots, g_k N\}$ generating G/N with the property that*

$$\sigma(\langle g_i, N \rangle) \leq \sigma^*(G) + \omega(|g_i N|_{G/N})$$

for every $i \in \{1, \ldots, k\}$, where $|g_i N|_{G/N}$ denotes the order of $g_i N$ in G/N.

Proof. There exists a set $\{g_1N, \dots, g_kN\}$ generating G/N with the property that $\sigma^*(G)$ is realized by the union $g_1N \cup \dots \cup g_kN$. In particular for $i \in \{1, \dots, k\}$ we have $\sigma_G(g_iN) \leq \sigma^*(G)$. If H is a proper supplement of N in G then $H \cap \langle g_i, N \rangle$ is a proper supplement of N in $\langle g_i, N \rangle$, therefore $\sigma_{\langle g_i, N \rangle}(g_iN) \leq \sigma_G(g_iN) \leq \sigma^*(G)$. By Lemma 2.14, in order to cover $\langle g_i, N \rangle$ with proper subgroups it suffices to use a family of proper subgroups covering g_iN and the maximal subgroups containing N. We obtain that $\sigma(\langle g_i, N \rangle) \leq \sigma_G(g_iN) + \omega(|g_iN|_{G/N}) \leq \sigma^*(G) + \omega(|g_iN|_{G/N})$. □

Corollary 2.16. *Let H be a non-abelian σ-elementary group and assume that $\sigma(H) \leq 56$. Then H is primitive and monolithic.*

Proof. By Corollary 1.21 we may assume that there exists a non-abelian minimal normal subgroup N of H. Let G be the monolithic group associated to N. If G has a primitivity degree at most 27 then either $\ell_G(\mathrm{soc}(G)) \geq 10$ and $G/\mathrm{soc}(G) \in \{C_2 \times C_2, \mathrm{Sym}(3), D_8\}$ - contradicting the inequality $\ell_G(\mathrm{soc}(G)) \leq \sigma(H) \leq \sigma(G)$ - or $G/\mathrm{soc}(G)$ is cyclic of prime-power order, so Corollary 2.13 implies $H = G$. Therefore we may assume that $\ell_G(N) \geq 28$. Suppose H has at least two minimal normal subgroups $N_1, N_2 = N$. If N_1 is abelian then $\ell_{X_1}(N_1) + 28 = |N_1| + 28 \leq \sigma(H)$, so by Proposition 1.20 $\sigma(H) - 28 \geq |N_1| > \frac{1}{2}\sigma(H)$, thus $\sigma(H) > 56$, contradiction. If N_1 is non-abelian then $2 \cdot 28 \leq \sigma(H) \leq 56$, so we may assume that $\sigma(H) = 56$ and that G has 28 as primitivity degree, in particular it is almost-simple. The only 28-primitive group Y such that $Y/\mathrm{soc}(Y)$ is not of prime-power order is $\mathrm{Aut}(PSL(2, 27))$, so by Corollary 2.13 we may assume that $G = \mathrm{Aut}(PSL(2, 27))$. In particular $G/\mathrm{soc}(G) \cong C_6$. Lemma 2.15 implies that either $\sigma(G) \leq \sigma^*(G) + 2$, and in this case $H = G$, or $56 = \sigma(H) \geq \sigma^*(G) \geq \sigma(PGL(2, 27)) - 3 = 376$ (cf. Appendix B), a contradiction. □

We are now in position to determine some σ-elementary groups with small covering number. Suppose G is a σ-elementary group with $\sigma(G) \leq 25$. Then G is primitive monolithic and by Lemma 1.3 G has a primitivity degree at most $\sigma(G) - 1 = 24$. The results listed in Appendix A and Appendix B imply that G is one of the groups appearing in Table 1 in the Introduction.
We can also deduce the following.

Theorem 2.17. $\sigma(\mathrm{Alt}(5) \wr C_2) = 57$ *and if G is a non-abelian σ-elementary group such that* $\sigma(G) \leq 56$ *then G is either affine or almost-simple.*

Proof. The statement about $\mathrm{Alt}(5) \wr C_2$ is Theorem 2.71.
Let G be a group such that $\sigma(G) \leq 56$. Corollary 2.16 implies that G is primitive and monolithic. Let $N := \mathrm{soc}(G)$. The only monolithic primitive non-almost-simple non-affine groups of primitivity degree at most 55 are $\mathrm{Alt}(7) \wr C_2$, $PSL_3(2) \wr C_2$, which have covering number larger than 56 by Proposition 2.37, the four subgroups between $\mathrm{Alt}(5) \times \mathrm{Alt}(5)$ and $\mathrm{Aut}(\mathrm{Alt}(5) \times \mathrm{Alt}(5))$ and $\mathrm{Alt}(6) \wr C_2$.
Two of the subgroups between $\mathrm{Alt}(5) \times \mathrm{Alt}(5)$ and $\mathrm{Aut}(\mathrm{Alt}(5) \times \mathrm{Alt}(5))$ have as quotient over the socle a non-cyclic 2-group, so they have covering number 3. The other two are $\mathrm{Alt}(5) \wr C_2$ and $(\mathrm{Alt}(5) \times \mathrm{Alt}(5)) \rtimes C_4$. We have $\sigma(\mathrm{Alt}(5) \wr C_2) = 57$ and Proposition 2.37 implies that $\sigma((\mathrm{Alt}(5) \times \mathrm{Alt}(5)) \rtimes C_4) = 126$.

Let now $G := \mathrm{Alt}(6) \wr C_2$. Since $\mathrm{Alt}(6)$ has twelve maximal subgroups isomorphic to $\mathrm{Alt}(5)$, G has $2 \cdot 6^2$ maximal subgroups isomorphic to $H := \mathrm{Alt}(5) \wr C_2$. If $\sigma(G) < 57 = \sigma(H)$ then by Lemma 1.6 we would have $\sigma(G) \geq 2 \cdot 6^2$, contradiction. Therefore $\sigma(G) \geq 57$. □

3.1. A density result. In this section we show that the density of the values $\sigma(G)$ for G a monolithic group with $G/\operatorname{soc}(G)$ cyclic is zero.

LEMMA 2.18 (Powers' density). *Let A be a subset of $\mathbb{N}$, and for $x \in \mathbb{R}$ let*

$$\theta(x) := |\{n \in A \mid n \leq x\}|.$$

If there exists a constant C such that $\log(x)\theta(\sqrt{x}) \leq C\theta(x)$ for every $x > 0$ then there exists a constant C' such that

$$|\{n^k \mid n \in A,\ k \in \mathbb{N},\ n^k \leq x\}| \leq C'\theta(x)$$

for every $x > 0$.

PROOF. Let $N(x)$ be the smallest natural number such that $2^{N(x)} > x$. Clearly there exists a constant c such that $N(x) \leq c\log(x)$, and

$$\begin{aligned} |\{n^k \mid n \in A,\ k \in \mathbb{N},\ n^k \leq x\}| &\leq \theta(x) + \theta(x^{1/2}) + \ldots + \theta(x^{1/N(x)}) \\ &\leq \theta(x) + N(x)\theta(x^{1/2}) \leq C'\theta(x), \end{aligned}$$

where $C' = 1 + cC$. □

Let $\mathcal{G}$ be a family of monolithic σ-elementary groups with non-abelian socle, and for $G \in \mathcal{G}$ let $\operatorname{soc}(G) = S^k$ for S a non-abelian simple group and $n_\sigma(G) := m(S)^k$. By Proposition 2.6 and Lemma 1.2, $n_\sigma(G) \leq \ell_G(\operatorname{soc}(G)) \leq \sigma(G)$. Define

$$A := \{\sigma(G) \mid G \in \mathcal{G}\}, \qquad B := \{n_\sigma(G) \mid G \in \mathcal{G}\}.$$

REMARK 2.19. *Let $g(x)$ be a function such that*

$$|\{G \in \mathcal{G} \mid n_\sigma(G) = n\}| \leq g(x) \qquad \forall n \leq x.$$

Then

$$|\{n \in A \mid n \leq x\}| \leq g(x) \cdot |\{n \in B \mid n \leq x\}|.$$

Let now $\mathcal{S}$ be the family of non-altenating non-abelian simple groups non isomorphic to $PSL(2,q)$.

LEMMA 2.20. *There exists a constant C such that $|\{1,\ldots,x\} \cap \{m(S) \mid S \in \mathcal{S}\}| \leq C\sqrt{x}/\log(x)$ for all $x \in \mathbb{N}$.*

PROOF. By inspection, using for example Table 1 in [**DaLdp**], [**Coo**] (cf. e.g. the proof of Lemma 9.1 in [**LMkn**]). □

THEOREM 2.21. *Let $\mathcal{G}$ be the family of monolithic groups G with non-abelian socle and such that $G/\operatorname{soc}(G)$ is cyclic. Then there exists a constant C such that for every $x > 0$,*

$$|\{\sigma(G) \mid G \in \mathcal{G},\ \sigma(G) \leq x\}| \leq C\sqrt{x}.$$

Proof. Let us use Notations 2.2. In $\mathcal{G}$ there are at most $|\operatorname{Out}(S)|$ (isomorphism classes of) groups G with given socle S^k (up to conjugacy, there exists a generator of $G/\operatorname{soc}(G)$ of the form $(1,\dots,1,x)\sigma$ where $x\in X/S$ and $\langle\sigma\rangle = K$), and the number of simple groups S with given $m(S)$ is bounded by a constant (to see this, observe that the numerical entries in Table 1 of [**DaLdp**] are either constants or infinite sequences of strictly increasing positive integers), so by Lemma 2.1 (2) there exists a positive constant d such that setting $g(x) = d\log(x)$ we have

$$|\{G\in\mathcal{G} \mid n_\sigma(G) = n\} \leq g(n) \leq g(x)$$

for every $n\leq x$.
Let $\mathcal{A}$ be the family of the alternating groups $\operatorname{Alt}(n)$ with $n\geq 5$, let $\mathcal{P}_1$ be the set of the simple groups isomorphic to $PSL(2,p)$ with p a prime, and let $\mathcal{P}_2$ be the set of simple groups isomorphic to $PSL(2,q)$ with q a prime-power, not a prime.
Let

$$\mathcal{G}_1 := \{G\in\mathcal{G} \mid k\geq 1,\ S\in\mathcal{S}\},\ \mathcal{G}_2 := \{G\in\mathcal{G} \mid k=1,\ S\in\mathcal{A}\},$$

$$\mathcal{G}_3 := \{G\in\mathcal{G} \mid k=2,\ S\in\mathcal{A}\},\ \mathcal{G}_4 := \{G\in\mathcal{G} \mid k\geq 3,\ S\in\mathcal{A}\},$$

$$\mathcal{G}_5 := \{G\in\mathcal{G} \mid k=1,\ S\in\mathcal{P}_1\},\ \mathcal{G}_6 := \{G\in\mathcal{G} \mid k\geq 2,\ S\in\mathcal{P}_1\}\cup\{G\in\mathcal{G} \mid k\geq 1,\ S\in\mathcal{P}_2\}.$$

Clearly $\mathcal{G}$ equals the disjoint union $\cup_{i=1}^6\mathcal{G}_i$.
In the following discussion recall the inequality $n_\sigma(G)\leq\sigma(G)$. Using Lemma 2.18 and Lemma 2.20 we see that

$$|\{n_\sigma(G) \mid G\in\mathcal{G}_1,\ \sigma(G)\leq x\}| \leq C_1\sqrt{x}/\log(x).$$

Using the fact that $n^3\leq\sigma(\operatorname{Alt}(n)),\sigma(\operatorname{Sym}(n))$ for n large (cf. [**MarS**, Theorem 3.1] and [**LMkn**, Theorem 9.2]) and the fact that $\operatorname{Aut}(\operatorname{Alt}(n)) = \operatorname{Sym}(n)$ for n large we see that

$$|\{G\in\mathcal{G}_2 \mid \sigma(G)\leq x\}| \leq C_2\sqrt[3]{x}.$$

Since $m(\operatorname{Alt}(n)) = n$, we clearly have

$$|\{G\in\mathcal{G}_3 \mid \sigma(G)\leq x\}| \leq C_3\sqrt{x},\ |\{n_\sigma(G) \mid G\in\mathcal{G}_4,\ \sigma(G)\leq x\}| \leq C_4\sqrt[3]{x}.$$

Using the fact that $p^2/2\leq\sigma(PSL(2,p)),\sigma(PGL(2,p))$ for p a large prime (Theorem A.4), the fact that $\operatorname{Aut}(PSL(2,p)) = PGL(2,p)$ and the Prime Number Theorem we see that

$$|\{G\in\mathcal{G}_5 \mid \sigma(G)\leq x\}| \leq C_5\sqrt{x}/\log(x).$$

Using the Prime Number Theorem and Lemma 2.18 we see that

$$|\{n_\sigma(G) \mid G\in\mathcal{G}_6,\ \sigma(G)\leq x\}| \leq C_6\sqrt{x}/\log(x).$$

Using Remark 2.19 we conclude that there exists a constant C such that for any $x\in\mathbb{N}$,

$$|\{\sigma(G) \mid G\in\mathcal{G},\ \sigma(G)\leq x\}| \leq C\sqrt{x}.$$

The proof is completed. $\square$

4. The covering number of a direct product

If Conjecture 1.28 is true then of course the direct product of two non-trivial groups cannot be σ-elementary and non-abelian. In this section we deal with this case. The following result was obtained in [**GL**], a joint work with A. Lucchini.

THEOREM 2.22. *Let $\mathcal{M}$ be a minimal cover of a direct product $G = H_1 \times H_2$ of two groups. Then one of the following holds:*

(1) *$\mathcal{M} = \{X \times H_2 \mid X \in \mathcal{X}\}$ where $\mathcal{X}$ is a minimal cover of H_1. In this case $\sigma(G) = \sigma(H_1)$.*
(2) *$\mathcal{M} = \{H_1 \times X \mid X \in \mathcal{X}\}$ where $\mathcal{X}$ is a minimal cover of H_2. In this case $\sigma(G) = \sigma(H_2)$.*
(3) *There exist $N_1 \trianglelefteq H_1$, $N_2 \trianglelefteq H_2$ with $H_1/N_1 \cong H_2/N_2 \cong C_p$ and $\mathcal{M}$ consists of the maximal subgroups of $H_1 \times H_2$ containing $N_1 \times N_2$. In this case $\sigma(G) = p + 1$.*

First let us recall a description of the maximal subgroups of a direct product $H_1 \times H_2$.

- We will say that a maximal subgroup M of $H_1 \times H_2$ is of *standard type* if either $M = X_1 \times H_2$ with X_1 a maximal subgroup of H_1 or $M = H_1 \times X_2$ with X_2 a maximal subgroup of H_2.
- We will say that a maximal subgroup M of $H_1 \times H_2$ is of *diagonal type* if there exist a maximal normal subgroup N_1 of H_1, a maximal normal subgroup N_2 of H_2 and an isomorphism $\phi : H_1/N_1 \to H_2/N_2$ such that $M = \{(h_1, h_2) \in H_1 \times H_2 \mid \phi(h_1N_1) = h_2N_2\}$.

By [**Suz**, Chap. 2, (4.19)], the following holds.

LEMMA 2.23. *A maximal subgroup of $H_1 \times H_2$ is either of standard type or of diagonal type.*

LEMMA 2.24. *Let $\mathcal{M} = \{M_1, \dots, M_\sigma\}$ be a minimal cover of $G = H_1 \times H_2$. If all the subgroups in $\mathcal{M}$ are maximal and $\mathcal{M}$ contains a subgroup of diagonal type whose index is a prime number p, then $\sigma(G) = p + 1$ and all the subgroups in M are normal of index p.*

PROOF. First notice that if $\mathcal{M}$ contains a maximal subgroup of diagonal type and index p, then $C_p \times C_p$ is an epimorphic image of G and consequently

$$\sigma(G) \leq \sigma(C_p \times C_p) = p + 1.$$

We argue by induction on the order of G. We may assume that there exists no nontrivial normal subgroup N of G such that $N \leq M$ for all $M \in \mathcal{M}$ and $N \leq H_1$. Otherwise $\{M_1/N, \dots, M_\sigma/N\}$ would be a minimal cover of $(H_1/N) \times H_2$ containing a maximal diagonal subgroup of index p and the conclusion follows by induction. For the same reason, there is no nontrivial normal subgroup N of G such that $N \leq M$ for all $M \in \mathcal{M}$ and $N \leq H_2$. In particular

$$\Phi(G) = \Phi(H_1) \times \Phi(H_2) = \{1\}.$$

First assume that $Z(G)$ has order divisible by p. This implies that there exists a central subgroup, say N, of order p, which is contained either in H_1 or in H_2. Let $\mathcal{U}$ be the set of subgroups in $\mathcal{M}$ not containing N. By our assumption $\mathcal{U} \neq \emptyset$, moreover if $M \in \mathcal{U}$, then $G = M \times N$ and in particular M is a normal subgroup of G and has index p. By Lemma 1.2, $p \leq |\mathcal{U}| \leq \sigma(G) \leq p + 1$. Moreover N is not contained in the union of the subgroups in $\mathcal{U}$, so we must have $|\mathcal{U}| = p$ and $\sigma(G) = p + 1$.

Let M be unique element of $\mathcal{M} \setminus \mathcal{U}$. By Lemma 1.2, M contains the intersection $M_i \cap M_j$ of any two different subgroups in $\mathcal{U}$, but $G/(M_i \cap M_j) \cong C_p \times C_p$, so M is a normal subgroup of index p. Now assume that p does not divide $|Z(G)|$. Write $\mathrm{soc}(G) = N_1 \times \cdots \times N_t$ as a product of minimal normal subgroups. We may assume that each N_i is contained either in H_1 or in H_2 and that N_i is abelian if and only if $i < u$. Let $C = \bigcap_{1 \le i \le t} C_G(N_i)$. Since $\Phi(G) = \{1\}$, the socle of G coincides with the generalized Fitting subgroup of G and, by the Bender F^*-Theorem (see for example [**Asch**, (31.13)]),

$$C = C_G(\mathrm{soc}\, G) = Z(\mathrm{soc}\, G) = \prod_{i<u} N_i.$$

Since p does not divide $|Z(G)|$, if N_i is a p-group, then $N_i = [N_i, G] \le G' \cap C$. In particular p does not divide $|C : G' \cap C| = |CG' : G'|$. On the other hand p divides $|G : G'| = |G : CG'||CG' : G'|$, hence G/C has C_p as an epimorphic image. Since G/C is a subdirect product of $\prod_{1 \le i \le t} G/C_G(N_i)$, there must exist a minimal normal subgroup N of G which is contained in either H_1 or H_2 and with the property that $A = G/C_G(N)$ has a chief factor of order p. By our assumption the set $\mathcal{U}$ of the subgroups in $\mathcal{M}$ not containing N is non empty. By Lemma 1.2, $p + 1 \ge \sigma(G) \ge |\mathcal{U}| \ge \beta$, with $\beta = \min_{M \in \mathcal{U}} |G : M|$. Fix a maximal subgroup M in $\mathcal{U}$ with $|G : M| = \beta$.
If N is abelian, then the subgroups in $\mathcal{U}$ are complements of N, hence $\beta = |N|$. Moreover N is not contained in the union of the subgroups in $\mathcal{U}$, hence $p + 1 \ge \sigma(G) \ge |N| + 1$. However p must be a prime divisor of $|A|$, but $A \le \mathrm{GL}(N)$ and this implies $p < |N|$, a contradiction.
If N is a non-abelian simple group, then C_p is isomorphic to a chief factor of a subgroup of $\mathrm{Out}(N)$ hence $p \le |\mathrm{Out}(N)|$. However $\beta = |G : M| = |N : M \cap N|$ is the index of a proper subgroup of N and Lemma 2.1 implies $\beta > 2p$. But then $p + 1 \ge \beta > 2p$, a contradiction.
We are left with the case $N = S_1 \times \cdots \times S_r \cong S^r$ where S is a nonabelian simple group. Let $\pi_i : N \to S_i$ the projection to the i-th factor of N. Since $MN = G$ and N is a minimal normal subgroup of G, the maximal subgroup M permutes transitively the minimal normal subgroups $S_1, \ldots, S_r$ of N and normalizes $M \cap N$. This implies that $\pi_1(M \cap N) \cong \ldots \cong \pi_r(M \cap N)$ so by 2.4 either $M \cap N \le T_1 \times \cdots \times T_r$ with $T_i < S_i$ for each $i \in \{1, \ldots, r\}$ or $M \cap N \cong S^u$ with u a proper divisor of r. Therefore, by Lemma 2.1,

$$p + 1 \ge \beta = |N : M \cap N| \ge \min\{2^r q^r, |S|^{r/2}\}$$

with q the largest prime divisor of $|\mathrm{Out}(S)|$. Moreover C_p is isomorphic to a chief factor of a subgroup of $\mathrm{Out}(N) \cong \mathrm{Out}(S) \wr \mathrm{Sym}(r)$, so either p divides $|\mathrm{Sym}(r)|$, in which case $p \le r$, or p divides $|\mathrm{Out}\, S|$ and consequently $p \le q$. Both these cases lead to a contradiction. $\square$

Lemma 2.25. *If $\mathcal{M}$ is a minimal cover of a group G and N is a normal subgroup of G such that $NM \ne G$ for each $M \in \mathcal{M}$, then $N \le M$ for each $M \in \mathcal{M}$.*

Proof. Let $\mathcal{M} = \{M_1, \ldots, M_n\}$. By our assumption, $\{M_1N, \ldots, M_nN\}$ is also a minimal cover of G. In particular, for each i, there exists $x_i \in M_iN$ such that $x_i \notin M_jN$ if $j \ne i$. Assume by contradiction $N \not\le M_i$ and take $y \in N \setminus M_i$: we have $x_i \cdot g \in M_i$ for some $g \in N$ and consequently $x_i \cdot g \cdot y \notin M_i$: this implies $x_i \cdot g \cdot y \in M_j$ for some $j \ne i$, but then $x_i \in M_jN$, a contradiction. $\square$

Proposition 2.26. *Let $\mathcal{X} = \{X_1, \dots, X_\sigma\}$ be a minimal cover of $G = H_1 \times H_2$. If a subgroup of $\mathcal{X}$ is contained in a maximal subgroup of diagonal type whose index is a prime number p, then $\sigma(G) = p + 1$, X_i is a normal subgroup of index p for each $i \in \{1, \dots, \sigma\}$ and $\bigcap_i X_i$ has index p^2 in G.*

Proof. For each $i \in \{1, \dots, \sigma\}$, let M_i be a maximal subgroup of G containing X_i, chosen is such a way that M_i is a maximal subgroup of diagonal type and index p when X_i is contained in such a maximal subgroup. The cover $\mathcal{M} = \{M_1, \dots, M_\sigma\}$ satisfies the hypothesis of Lemma 2.24, so $\sigma = p + 1$ and M_i is a maximal normal subgroup of index p for each $i \in \{1, \dots, \sigma\}$. Let $N = M_1 \cap M_2$. If, by contradiction, there exists $i \in \{3, \dots, \sigma\}$ such that M_i does not contain N, then, by Lemma 1.2, $\sigma \geq 2 + p$. So for each $i \in \{1, \dots, \sigma\}$, we have $N \leq M_i$ but then $X_i N \leq M_i \neq G$, hence $N \leq X_i$ by Lemma 2.25. In particular $\{X_1/N, \dots, X_\sigma/N\}$ is a cover of $G/N \cong C_p \times C_p$. Since $\sigma(C_p \times C_p) = p + 1 = \sigma$, $X_i \neq N$ for each $i \in \{1, \dots, \sigma\}$. □

Proposition 2.27. *Let $\mathcal{X} = \{X_1, \dots, X_\sigma\}$ be a minimal cover of $G = H_1 \times H_2$. If $\mathcal{X}$ contains no subgroup of diagonal type whose index is a prime number, then either $H_1 \times 1$ or $1 \times H_2$ is contained in $\bigcap_{1 \leq i \leq \sigma} X_i$.*

Proof. For each $i \in \{1, \dots, \sigma\}$, let M_i be a maximal subgroup of G containing X_i. We have that $\mathcal{M} = \{M_1, \dots, M_\sigma\}$ is a minimal cover of G given by $\sigma = \sigma(G)$ maximal subgroups of G. We set:

$$\begin{aligned}
\mathcal{M}_1 &= \{M \in \mathcal{M} \mid M \geq H_2\} = \{L \times H_2 \mid L \text{ a maximal subgroup of } H_1\}, \\
\mathcal{M}_2 &= \{M \in \mathcal{M} \mid M \geq H_1\} = \{H_1 \times L \mid L \text{ a maximal subgroup of } H_2\}, \\
\mathcal{M}_3 &= \mathcal{M} \setminus (\mathcal{M}_1 \cup \mathcal{M}_2).
\end{aligned}$$

Then we define the two sets

$$\Omega_1 = H_1 \setminus \left(\bigcup_{L \times H_2 \in \mathcal{M}_1} L \right), \quad \Omega_2 = H_2 \setminus \left(\bigcup_{H_1 \times L \in \mathcal{M}_2} L \right)$$

If $\Omega_1 = \emptyset$, then $G = H_1 \times H_2 = \bigcup_{L \times H_2 \in \mathcal{M}_1} L \times H_2$, hence $\mathcal{M} = \mathcal{M}_1$. In the same way, if $\Omega_2 = \emptyset$, then $\mathcal{M} = \mathcal{M}_2$.

So we may assume $\Omega_1 \times \Omega_2 \neq \emptyset$. For $i \in \{1, 2\}$, let K_i be the intersection of the maximal normal subgroups of H_i. Notice that H_i/K_i is isomorphic to a direct product of simple groups and K_i is the smallest subgroup of H_i with this property. To fix our notation assume

$$H_1/K_1 = \prod_{1 \leq a \leq \alpha} S_a, \qquad H_2/K_2 = \prod_{1 \leq b \leq \beta} T_b$$

with S_a, T_b simple groups. To each $a \in A = \{1, \dots, \alpha\}$ there corresponds the projection $\pi_{1,a} : H_1 \to S_a$ and to each $b \in B = \{1, \dots, \beta\}$ there corresponds the projection $\pi_{2,b} : H_2 \to T_b$. For $i \in \{1, 2\}$, consider the projection $\rho_i : H_i \to H_i/K_i$ and the image

$$\Delta_i = \{\rho_i(\omega) \mid \omega \in \Omega_i\}$$

of Ω_i under this projection.

By Lemma 2.23, to any $M \in \mathcal{M}_3$ we may associate a triple (a, b, ϕ) with $a \in A$, $b \in B$ and $\phi : S_a \to T_b$ a group isomorphism such that

$$M = M(a, b, \phi) = \{(h_1, h_2) \in H_1 \times H_2 \mid \phi(\pi_{1,a}(h_1)) = \pi_{2,b}(h_2)\}.$$

Now let Λ be the set of the triples (a, b, ϕ) such that $M(a, b, \phi) \in \mathcal{M}_3$. By hypothesis, $\mathcal{M}_3$ contains no subgroup of index a prime number; this implies that if $(a, b, \phi) \in \Lambda$, then $S_a \cong T_b$ is a nonabelian simple group.
Now fix an element $(s_1, \dots, s_\alpha) \in \Delta_1$ and an element $x \in \Omega_1$ with $\rho_1(x) = (s_1, \dots, s_\alpha)$ and for each $(a, b, \phi) \in \Lambda$ let

$$U(a, b, \phi) = \{h \in H_2 \mid \pi_{2,b}(h) \in \langle \phi(s_a) \rangle\}.$$

Clearly, since T_b is a nonabelian simple group, $\langle \phi(s_a) \rangle \neq T_b$ and $U(a, b, \phi)$ is a proper subgroup of H_2. Consider the following family of subgroups of H_2 :

$$\mathcal{T} = \{M \mid H_1 \times M \in \mathcal{M}_2\} \cup \{U(a, b, \phi) \mid (a, b, \phi) \in \Lambda\}.$$

We claim that $\mathcal{T}$ is a cover of H_2. We have to prove that if $h_2 \in \Omega_2$, then $h_2 \in U(a, b, \phi)$ for some $(a, b, \phi) \in \Lambda$. Observe that the elements of the set $\Omega_1 \times \Omega_2$ do not belong to any of the subgroups in $\mathcal{M}_1$ or $\mathcal{M}_2$, thus the set $\Omega_1 \times \Omega_2$ has to be covered by the subgroups in $\mathcal{M}_3$. In particular if $h_2 \in \Omega_2$, then $(x, h_2) \in M(a, b, \phi)$ for some $(a, b, \phi) \in \Lambda$. This implies that $\pi_{2,b}(h_2) = \phi(\pi_{1,a}(x)) = \phi(s_a) \in \langle \phi(s_a) \rangle$, hence $h_2 \in U(a, b, \phi)$ and the claim is proved. But this implies $|\mathcal{M}_1| + |\mathcal{M}_2| + |\mathcal{M}_3| = \sigma(G) \leq \sigma(H_2) \leq |\mathcal{T}| \leq |\mathcal{M}_2| + |\mathcal{M}_3|$ and, consequently, $\mathcal{M}_1 = \emptyset$. With a similar argument we deduce $\mathcal{M}_2 = \emptyset$. So if $\mathcal{M}_3 \neq \emptyset$, then $\mathcal{M} = \mathcal{M}_3$. By Lemma 1.3 there exists $M \in \mathcal{M}_3$ with $\sigma(G) \geq |G : M| + 1$; however $|G : M| = |S|$ for some nonabelian simple group S which is an epimorphic image of G. This implies $\sigma(G) \leq \sigma(S) \leq |S| = |G : M| \leq \sigma(G) - 1$, a contradiction.
Let $\overline{H}_1 = H_1 \times 1$ and $\overline{H}_2 = 1 \times H_2$. We have proved that there exists $j \in \{1, 2\}$, such that $\overline{H}_j \leq \bigcap_{1 \leq i \leq \sigma} M_i$. In particular $\overline{H}_j X_i \leq M_i$ for each $i \in \{1, \dots, \sigma\}$ hence, by Lemma 2.25, we can conclude $\overline{H}_j \leq \bigcap_{1 \leq i \leq \sigma} X_i$. □

5. Covering some monolithic groups

THEOREM 2.28. *Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2. Assume that X/S is abelian. Let $\mathcal{M}$ be a set of maximal subgroups of X supplementing S and such that $\bigcup_{M \in \mathcal{M}} M$ contains a coset $xS \in L$ with the property that $\langle x, T \rangle = L$.*
Then $\sigma(G) \leq 2^{m-1} + \sum_{M \in \mathcal{M}} |S : S \cap M|^{m-1}$.

Unfortunately the hypothesis "X/S abelian" does not seem easy to bypass.

PROOF. If $L \neq T$ define

$$R := \{(x_1, \dots, x_m)k \in G \mid x_1 \cdots x_m \in T\}.$$

Since X/S is abelian, R is a proper subgroup of G.
Let $\delta \in K$ be an m-cycle, $1 = a_1, a_2, \dots, a_m \in X$ and $M \in \mathcal{M}$. An element $(x_1, \dots, x_m)\delta \in X \wr K$ normalizes $(M \cap S) \times (M \cap S)^{a_2} \times \cdots \times (M \cap S)^{a_m}$ if and only if

$$(M \cap S)^{a_{\delta^{-1}(1)} x_{\delta^{-1}(1)}} \times (M \cap S)^{a_{\delta^{-1}(2)} x_{\delta^{-1}(2)}} \times \cdots \times (M \cap S)^{a_{\delta^{-1}(m)} x_{\delta^{-1}(m)}} =$$

$$= (M \cap S) \times (M \cap S)^{a_2} \times \cdots \times (M \cap S)^{a_m},$$

if and only if

$$a_{\delta^{-1}(1)} x_{\delta^{-1}(1)} a_1^{-1},\ a_{\delta^{-1}(2)} x_{\delta^{-1}(2)} a_2^{-1}, \ldots, a_{\delta^{-1}(m)} x_{\delta^{-1}(m)} a_m^{-1} \in N_X(M \cap S) = M. \tag{2}$$

If $x_1 x_{\delta(1)} \cdots x_{\delta^{m-1}(1)} \in M$ then there exist $a_2, \ldots, a_m \in X$ such that (2) is true. Since M supplements S in X, $a_2, \ldots, a_m$ can be chosen in S. Therefore every element $(x_1, \ldots, x_m)\delta \in G$ such that δ is an m-cycle and $x_1 x_{\delta(1)} \cdots x_{\delta^{m-1}(1)} \in xS$ belongs to a subgroup of G of the form $N_G((M \cap S) \times (M \cap S)^{a_2} \times \cdots \times (M \cap S)^{a_m})$ where $M \in \mathcal{M}$ and $a_2, \ldots, a_m \in S$. It follows that G is covered by these subgroups together with R (if $L \neq T$) and the pre-images through ρ of $2^{m-1} - 1$ maximal intransitive subgroups of K (corresponding to the subsets of $\{1, \ldots, m\}$ of size from 1 to $[m/2]$). $\square$

5.1. The cyclic case: an upper bound.

PROPOSITION 2.29 (An upper bound). *Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2. Suppose that $G/\operatorname{soc}(G)$ is cyclic. Then X/S is cyclic, let $x \in X$ be such that $X/S = \langle xS \rangle$. Let $\mathcal{X}$ be a family of maximal subgroups of X supplementing S and which cover the coset xS of S, and let $\mathcal{M} := \{H \cap S \mid H \in \mathcal{X}\}$. Then*

$$\sigma(G) \leq \omega(m \cdot |X/S|) + \sum_{M \in \mathcal{M}} |S : M|^{m-1}.$$

A cover is provided by the $\omega(|G/\operatorname{soc}(G)|) = \omega(m \cdot |X/S|)$ normal subgroups of prime index containing $\operatorname{soc}(G)$ and the subgroups of the form $N_G(M \times M^{a_2} \times \ldots \times M^{a_m})$ where $M \in \mathcal{M}$ and $a_2, \ldots, a_m \in S$.

We now prove Proposition 2.29. Call $\pi_G : G \to G/\operatorname{soc}(G)$, $\pi_X : X \to X/S$ the canonical projections.

The elements of G which do not generate G modulo $\operatorname{soc}(G)$ are covered by the $\omega(|G/\operatorname{soc}(G)|) = \omega(|X/S| \cdot m)$ maximal subgroups of G of prime index containing $\operatorname{soc}(G)$. Let $g = (x_1, \ldots, x_m)\delta \in G$ be such that $\pi_G(g)$ generates $G/\operatorname{soc}(G)$, where $\delta \in \operatorname{Sym}(m)$ is an m-cycle. We may assume that δ is the m-cycle $(1 \ldots m)$. We want g to belong to a subgroup of G of the form $N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ where $M = H \cap S$ for some $H \in \mathcal{X}$ and $a_2, \ldots, a_m \in S$. g belongs to such a subgroup if and only if

$$x_1 a_2^{-1},\ a_2 x_2 a_3^{-1},\ a_3 x_3 a_4^{-1},\ \ldots,\ a_m x_m \in N_X(M).$$

In particular $y := x_1 \cdots x_m \in N_X(M)$ and we may choose $a_2 = x_1$, $a_3 = x_1 x_2$, $\ldots$, $a_m = x_1 x_2 \cdots x_{m-1}$. By Lemma 2.14 $\mathcal{X}$ covers all the elements of X whose image in X/S generates X/S, so since by Lemma 2.7 $\pi_X(y)$ generates X/S, there exists $H \in \mathcal{X}$ containing y, in particular $HS = X$ and $H \cap S =: M$ is a non-trivial (CFSG) proper subgroup of S, thus since H is maximal in X and normalizes M, $H = N_X(M)$. It follows that G is covered by the maximal subgroups of G containing $\operatorname{soc}(G)$ together with the family

$$\mathcal{F} := \{N_G(M \times M^{a_2} \times \cdots \times M^{a_m}) \mid M \in \mathcal{M},\ a_2, \ldots, a_m \in X\}.$$

Since every element of $\mathcal{F}$ supplements $\mathrm{soc}(G)$, its X^m-conjugacy class in $X \wr C_m$ coincides with its S^m-class and hence, since $S^m \leq G$, it is contained in its G-class. This means that in the definition of $\mathcal{F}$ the elements $a_2, \ldots, a_m$ can be taken in S, and this implies the result.

5.2. The cyclic case: a lower bound. The following notion (introduced in [**MarS**]) is our main tool to provide lower bounds for the covering number.

Definition 2.30 (Definite unbeatability). *Let X be a group. Let $\mathcal{H}$ be a set of proper subgroups of X, and let $\Pi \subseteq X$. Suppose that the following four conditions hold for $\mathcal{H}$ and Π.*

(1) $\Pi \cap H \neq \emptyset$ *for every* $H \in \mathcal{H}$;
(2) $\Pi \subseteq \bigcup_{H \in \mathcal{H}} H$;
(3) $\Pi \cap H_1 \cap H_2 = \emptyset$ *for every distinct pair of subgroups* H_1 *and* H_2 *of* $\mathcal{H}$;
(4) $|\Pi \cap K| \leq |\Pi \cap H|$ *for every* $H \in \mathcal{H}$ *and* $K < X$ *with* $K \notin \mathcal{H}$.

Then $\mathcal{H}$ is said to be definitely unbeatable on Π.

For $\Pi \subseteq X$ let $\sigma_X(\Pi)$ be the least cardinality of a family of proper subgroups of X whose union contains Π. The following lemma is straightforward so we state it without proof.

Lemma 2.31. *If $\mathcal{H}$ is definitely unbeatable on Π then $\sigma_X(\Pi) = |\mathcal{H}|$.*

It follows that if $\mathcal{H}$ is definitely unbeatable on Π then $|\mathcal{H}| = \sigma_X(\Pi) \leq \sigma(X)$.

Theorem 2.32. *Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2. Suppose that G/N is cyclic, generated by γN for $\gamma \in G$. Let $x \in X$ be such that $X = \langle x, S \rangle$. Without loss of generality assume that $\rho(\gamma) = \delta = (1, \ldots, m)$ and that $\gamma = (1, \ldots, 1, x)\delta$. Let $\mathcal{X}$ be a family of maximal subgroups of X supplementing S and let $\mathcal{M} := \{V \cap S \mid V \in \mathcal{X}\}$, $\Pi \subseteq xS$, $C \subseteq X - xS$. Let r be the smallest prime divisor of m, and let r' be the smallest prime divisor of m such that some element of Π admits a r'-th root in X. Suppose that*

(1) $N_X(M) \cap \Pi \neq \emptyset$ *for every* $M \in \mathcal{M}$;
(2) $N_X(M_1) \cap N_X(M_2) \cap \Pi = \emptyset$ *for every* $M_1 \neq M_2$ *in* $\mathcal{M}$;
(3) $\Pi \subseteq \bigcup_{M \in \mathcal{M}} N_X(M)$.

Consider the following condition:

(4) *Whenever $M \in \mathcal{M}$ and V is a maximal subgroup of X supplementing S such that $V \cap S \notin \mathcal{M}$,*

$$(i) \qquad |M|^{m-1} \cdot |N_X(M) \cap \Pi| \geq |V \cap S|^{m-1} \cdot |V \cap (\Pi \cup C)|,$$

$$(ii) \qquad \text{If } m \geq 2,\ |M|^{m-1} \cdot |N_X(M) \cap \Pi| \geq m \cdot |X/S| \cdot |S|^{m/r},$$

$$(iii) \qquad \text{If } m \geq 2,\ |M|^{m-1} \cdot |N_X(M) \cap \Pi| \geq \min\{z_{r'}(\Pi), |S|\} \cdot |S|^{m/r'-1},$$

where $z_{r'}(\Pi)$ is the number of elements $y \in X$ such that $y^{r'} \in \Pi$.

Denote by $\sigma_{N\gamma}(G)$ the smallest number of supplements of N in G needed to cover $N\gamma$. Suppose conditions (4)(i), (4)(iii) hold. If $m = 1$ then $|\mathcal{M}| \leq \sigma(G)$, if $m \geq 2$ then

$$\sum_{M \in \mathcal{M}} |S : M|^{m-1} \leq \sigma_{N\gamma}(G) \leq \sigma(G),$$

and if $\mathcal{X}$ covers xS then

$$\sum_{M\in\mathcal{M}} |S:M|^{m-1} \leq \sigma(G) \leq \omega(m|X/S|) + \sum_{M\in\mathcal{M}} |S:M|^{m-1}.$$

Suppose from now on that conditions (4)(i), (4)(ii) hold. Let $A, B \subseteq X$, and assume that the following conditions also hold.

(5) *$\mathcal{X}$ covers xS;*
(6) *If $m \geq 2$ then for every $a \in A$, $b \in B$, $\alpha, \beta \in S$, $\langle a^\alpha, b^\beta\rangle \supseteq S$;*
(7) *If $m \geq 2$ then $C \cap N_X(M) = \emptyset$ for every $M \in \mathcal{M}$;*
(8) *If $m \geq 2$ then whenever V is a maximal subgroup of X supplementing S such that $V \cap S \notin \mathcal{M}$,*

$$|A| \cdot |B| \cdot |S|^{m-2} \geq \max\{|V \cap S|^{m-1} \cdot |V \cap (\Pi \cup C)|, m|X/S| \cdot |S|^{m/r}\}$$

and if $C \neq \emptyset$

$$|C| \cdot |S|^{m-1} \geq \max\{|V \cap S|^{m-1} \cdot |V \cap (\Pi \cup C)|, m|X/S| \cdot |S|^{m/r}\}.$$

Then $\sigma(G) = \sum_{M\in\mathcal{M}} |S:M|^{m-1} + \omega(m|X/S|)$.

Before the proof of Theorem 2.32 we state two lemmas.

Lemma 2.33. *Let $1 \leq k < m$ be an integer. In the following let the subscripts be identified with their reductions modulo m, and let $b_1 := 1$, b_2, $\ldots$, $b_m \in X$, s_1, $\ldots$, $s_m \in S$. Let M be a proper non-trivial subgroup of S.*
For $d \in \{1, \ldots, m\}$ define x_d to be x if $d > m-k$, and 1 if $d \leq m-k$. Let $y_1, \ldots, y_m \in X$. The element $(y_1, \ldots, y_m)\gamma^k \in X \wr \mathrm{Sym}(m)$ normalizes $M \times M^{a_2} \times \cdots \times M^{a_m}$ if and only if

$$\eta_d := a_d y_d x_d a_{d+k}^{-1} \in N_X(M), \qquad \forall d = 1, \ldots, m.$$

Moreover in this case

$$\begin{aligned} \eta &:= \eta_1\eta_{1+k}\eta_{1+2k}\cdots\eta_{1+(m-1)k} = \\ &= y_1x_1y_{1+k}x_{1+k}\cdots y_{1+(m-1)k}x_{1+(m-1)k} \in N_X(M). \end{aligned}$$

Proof. The element

$$(y_1, \ldots, y_m)\gamma^k = (y_1, \ldots, y_{m-k}, y_{m-k+1}x, \ldots, y_m x)\delta^k$$

belongs to $N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ if and only if

$$\begin{aligned} (M^{y_1} \times M^{a_2y_2} \times \cdots \times M^{a_{m-k}y_{m-k}} \times M^{a_{m-k+1}y_{m-k+1}x} \times \cdots \times M^{a_my_mx})^{\delta^k} = \\ = M \times M^{a_2} \times \cdots \times M^{a_m}, \end{aligned}$$

if and only if

$$\begin{aligned} M^{a_{m-k+1}y_{m-k+1}x} \times \cdots \times M^{a_my_mx} \times M^{y_1} \times M^{a_2y_2} \times \cdots \times M^{a_{m-k}y_{m-k}} = \\ = M \times M^{a_2} \times \cdots \times M^{a_m}. \end{aligned}$$

In other words:

$$a_{m-k+1}y_{m-k+1}x, a_{m-k+2}y_{m-k+2}xa_2^{-1}, \ldots, a_my_mxa_k^{-1},$$

$$y_1 a_{k+1}^{-1}, a_2 y_2 a_{k+2}^{-1}, \dots, a_{m-k} y_{m-k} a_m^{-1} \in N_X(M).$$

This implies the result. □

LEMMA 2.34. *Let G be as in the hypotheses of Theorem 2.32. Let ℓ be a divisor of m. The element $(s_1, \dots, s_m)\gamma \in N\gamma$ normalizes*

$$\Delta := \{(y_1, \dots, y_{m/\ell}, y_1^{b_{21}}, \dots, y_{m/\ell}^{b_{2,m/\ell}}, \dots, y_1^{b_{\ell,1}}, \dots, y_{m/\ell}^{b_{\ell,m/\ell}}) \mid y_1, \dots, y_{m/\ell} \in S\}$$

if and only if (here $b_{1i} = 1$ for all $i = 1, \dots, m/\ell$)

$$b_{\ell,m/\ell} s_m \tau b_{i1} = b_{i-1,m/\ell} s_{(i-1)m/\ell} \qquad \forall i = 2, \dots, \ell$$

and

$$s_j b_{i,j+1} = b_{i,j} s_{(i-1)(m/\ell)+j} \qquad \forall i = 2, \dots, \ell,\ j = 1, \dots, m/\ell - 1.$$

In particular

$$s_1 \cdots s_m \tau = [s_1 \cdots s_{m/\ell-1}(b_{\ell,m/\ell} s_m \tau)]^\ell.$$

Moreover for a given $b \in X$,

$$|\{(s_1, \dots, s_m)\gamma \in N_G(\Delta) \mid s_1 \cdots s_m \tau = b\}| = z_\ell(b) \cdot |S|^{m/\ell - 1},$$

where $z_\ell(b)$ is the number of elements $y \in X$ such that $y^\ell = b$.

PROOF. It is a direct computation. The element $(s_1, \dots, s_m)\gamma$ belongs to $N_G(\Delta)$ if and only if for every $y_1, \dots, y_{m/\ell} \in S$ the element

$$(y_{m/\ell}^{b_{\ell,m/\ell} s_m \tau}, y_1^{x_1}, \dots, y_{m/\ell}^{s_{m/\ell}}, y_1^{b_{21} s_{m/\ell+1}}, \dots, y_{m/\ell}^{b_{2,m/\ell} s_{2m/\ell}}, \dots, y_1^{b_{\ell,1} s_{(\ell-1)m/\ell+1}}, \dots, y_{m/\ell-1}^{b_{\ell,m/\ell-1} s_{m-1}})$$

belongs to Δ, and this leads to the stated conditions.
Using these conditions we see that for every $1 \le i \le \ell - 1$,

$$s_1 \cdots s_{m/\ell-1} b_{\ell,m/\ell} s_m \tau = b_{i,1} s_{(i-1)m/\ell+1} s_{(i-1)m/\ell+2} \cdots s_{(i-1)m/\ell+m/\ell-1} s_{im/\ell} b_{i+1,1}^{-1},$$

and

$$s_1 \cdots s_{m/\ell-1} b_{\ell,m/\ell} s_m \tau = b_{\ell,1} s_{(\ell-1)m/\ell+1} \cdots s_{m-1} x_m \tau.$$

It follows that

$$(s_1 \cdots s_{m/\ell-1} b_{\ell,m/\ell} s_m \tau)^\ell = s_1 \cdots s_m \tau.$$

The last statement follows easily from the first two. □

We now prove Theorem 2.32.
For every prime divisor ℓ of $|X/S|$ which does not divide m write $\ell = mq + k$ with q, k integers and $0 < k < m$ and define (notations are as in Lemma 2.33)

$$\Omega_\ell := \{(s_1, \dots, s_m)\gamma^\ell \mid s_1 x^q x_1 s_{1+k} x^q x_{1+k} \dots s_{1+(m-1)k} x^q x_{1+(m-1)k} \in C\}.$$

Note that since m and k are coprime, $\{x_1, x_{1+k}, \dots, x_{1+(m-1)k}\} = \{x_1, \dots, x_m\}$ and so

$$s_1 x^q x_1 s_{1+k} x^q x_{1+k} \dots s_{1+(m-1)k} x^q x_{1+(m-1)k} \in x^\ell S.$$

For every prime divisor ℓ of m define

$$\Omega_\ell := \{(s_1, \dots, s_m)\gamma^\ell \mid s_1 s_{1+\ell} s_{1+2\ell} \cdots s_{1+m-\ell} x \in A,\ s_2 s_{2+\ell} s_{2+2\ell} \cdots s_{2+m-\ell} x \in B\}.$$

Let

$$\Omega_1 := \{(s_1,\dots,s_m)\gamma \in G \mid s_1\cdots s_m x \in \Pi\},$$
$$\mathcal{L} := \{N_G(M \times M^{a_2} \times \cdots \times M^{a_m}) \mid M \in \mathcal{M},\ a_2,\dots,a_m \in S\}.$$

Moreover, for every prime divisor ℓ of $m|X/S|$ let H_ℓ be the pre-image of $\langle \gamma^\ell N\rangle$ through the canonical projection $G \to G/N = \langle \gamma N\rangle$. Note that $H_\ell \supseteq \Omega_\ell$. Let

$$\mathcal{H} := \mathcal{L} \cup \{H_\ell \mid \ell \text{ is a prime divisor of } m|X/S|\},$$
$$\Omega := \Omega_1 \cup \bigcup_{\ell \textit{ prime dividing } m|X/S|} \Omega_\ell.$$

Let H be a maximal subgroup of G of product type supplementing N, say $H = N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$, where M is a subgroup of S such that $N_X(M)$ is a maximal subgroup of X supplementing S and $a_2,\dots,a_m \in S$.

Lemma 2.35. *The following facts are true.*

(1) $|H \cap \Omega_1| = |M|^{m-1} \cdot |N_X(M) \cap \Pi|$.
(2) *If ℓ is a prime dividing $|X/S|$ and not m then either $H \cap \Omega_\ell = \emptyset$ or $|H \cap \Omega_\ell| = |M|^{m-1} \cdot |N_X(M) \cap C|$. In particular $H \cap \Omega_\ell = \emptyset$ if $H \in \mathcal{L}$.*
(3) *If ℓ is a prime divisor of m then $H \cap \Omega_\ell = \emptyset$.*

Proof. An element $(s_1,\dots,s_m)(1,\dots,1,x)\delta \in \Omega_1$ belongs to H if and only if

$$a_m s_m x, s_1 a_2^{-1}, a_2 s_2 a_3^{-1}, \dots, a_{m-1} s_{m-1} a_m^{-1} \in N_X(M).$$

This implies that

$$s_1 \in M a_2,\ s_2 \in M^{a_2} a_3,\ \dots,\ s_{m-1} \in M^{a_{m-1}} a_m,$$
$$N_X(M) \ni (s_1 a_2^{-1}) \cdot (a_2 s_2 a_3^{-1}) \cdot \cdots \cdot (a_{m-1} s_{m-1} a_m^{-1}) \cdot (a_m s_m x) = s_1 \dots s_m x \in \Pi.$$

This gives $|M|$ choices for s_i, $i = 1,\dots,m-1$, and $|N_X(M) \cap \Pi|$ choices for s_m.
Let now ℓ be a prime dividing $|X/S|$ and not m. Let q and $0 < k < m$ be the two integers such that $\ell = mq + k$. By Lemma 2.33, $(s_1,\dots,s_m)\gamma^\ell \in \Omega_\ell$ belongs to H if and only if $a_d s_d x^q x_d a_{d+k}^{-1} \in N_X(M)$ for $d = 1,\dots,m$, where the subscripts are modulo m, $x_d = 1$ if $1 \le d \le m-k$ and $x_d = x$ if $m-k < d \le m$. This gives 0 or $|M|$ choices for $s_1, s_{1+k}, \dots, s_{1+(m-2)k}$ and 0 or $|N_X(M) \cap C|$ choices for $s_{1+(m-1)k}$. So $|H \cap \Omega_\ell|$ is either 0 or $|M|^{m-1} \cdot |N_X(M) \cap C|$.
Let now ℓ be a prime divisor of m. Note that $(s_1,\dots,s_m)\gamma^\ell$ belongs to $H = N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ if and only if

$$(M \times M^{a_2} \times \cdots \times M^{a_m})^{(s_1,\dots,s_{m-\ell},s_{m-\ell+1}x,\dots,s_m x)\delta^\ell} = M \times M^{a_2} \times \cdots \times M^{a_m},$$

in other words

$$M^{a_{m-\ell+1}s_{m-\ell+1}x} \times \cdots \times M^{a_m s_m x} \times M^{s_1} \times M^{a_2 s_2} \times \cdots \times M^{a_{m-\ell}s_{m-\ell}} =$$
$$= M \times M^{a_2} \times \cdots \times M^{a_m},$$

in other words

$$a_{m-\ell+i}s_{m-\ell+i}x a_i^{-1} \in N_{S_n}(M) \qquad \forall i = 1,\dots,\ell;$$
$$a_i s_i a_{\ell+i}^{-1} \in N_{S_n}(M) \qquad \forall i = 1,\dots,m-\ell.$$

In particular

$$s_i s_{i+\ell} s_{i+2\ell} \cdots s_{i+m-\ell} x \in N_{S_n}(M)^{a_i} \qquad \forall i = 1, \dots, \ell.$$

This implies the result thanks to condition (7). □

Proposition 1.18 implies that the maximal subgroups of G supplementing N are not complements. So they are either of product type or of diagonal type.
If ℓ, s are two distinct prime divisors of $m|X/S|$ then clearly $H_\ell \cap \Omega = \Omega_\ell$ and $H_\ell \cap H_s \cap \Omega = \emptyset$. This together with Lemma 2.35 implies that conditions (1), (2), (3) of Definition 2.30 hold for $\mathcal{H}$ if they hold for $\mathcal{L}$. We now prove that they hold for $\mathcal{L}$.

(1) $\Omega_1 \cap H \neq \emptyset$ for every $H \in \mathcal{L}$. This follows from Lemma 2.35 and condition (1).
(2) We show that $\Omega_1 \subseteq \bigcup_{H \in \mathcal{L}} H$. Given $(s_1, \dots, s_m)\gamma \in \Omega_1$, choose $M \in \mathcal{M}$ such that $s_1 \cdots s_m x \in N_X(M)$ (it exists thanks to condition (2)) and $a_2 := s_1$, $a_3 := s_1 s_2, \dots, a_m := s_1 s_2 \cdots s_{m-1}$. Choose $H := N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$.
(3) We show that $\Omega_1 \cap N_G(M \times M^{a_2} \times \cdots \times M^{a_m}) \cap N_G(K \times K^{b_2} \times \cdots \times K^{b_m}) = \emptyset$ for $N_G(M \times M^{a_2} \times \cdots \times M^{a_m}) \neq N_G(K \times K^{b_2} \times \cdots \times K^{b_m})$ belonging to $\mathcal{L}$. If $(s_1, \dots, s_m)\gamma$ belongs to the stated intersection then either $s_1 \cdots s_m x \in N_X(M) \cap N_X(K) \cap \Pi$ with $M \neq K$, contradicting condition (3), or $M = K$ and

$$s_i \in a_i^{-1} M a_{i+1} \cap b_i^{-1} M b_{i+1}$$

for $i = 1, \dots, m-1$, where $a_1 = b_1 = 1$. This easily implies that $M^{a_i} = M^{b_i}$ for $i = 2, \dots, m$, contradiction.

We now prove that if conditions (4)(i), (4)(ii) hold then $|H \cap \Omega| \geq |K \cap \Omega|$ for $H \in \mathcal{H}$, K maximal subgroup of G outside $\mathcal{H}$. Note that this inequality being true implies condition (4) of Definition 2.30 for both $\mathcal{H}$ and $\mathcal{L}$ since for every prime divisor ℓ of $m|X/S|$ and every $H \in \mathcal{L}$ we have $H_\ell \cap \Omega_1 = \emptyset$ and $H \cap \Omega_\ell = \emptyset$.
We also prove that if conditions (4)(i), (4)(iii) hold then $|H \cap \Omega_1| \geq |K \cap \Omega_1|$ for $H \in \mathcal{H}$, K maximal subgroup of G outside $\mathcal{H}$.

(1) Case I: $H \in \mathcal{L}$ and K is of product type. Let $M \in \mathcal{M}$ and V is a maximal subgroup of S supplementing S such that $V \cap S \notin \mathcal{M}$. We want to show that

$$|\Omega \cap N_G(M \times M^{a_2} \times \cdots \times M^{a_m})| \geq |\Omega \cap N_G((V \cap S) \times (V \cap S)^{b_2} \times \cdots \times (V \cap S)^{b_m})|.$$

In other words

$$|M|^{m-1} \cdot |N_X(M) \cap (\Pi \cup C)| \geq |V \cap S|^{m-1} \cdot |V \cap (\Pi \cup C)|.$$

This follows from condition (4)(i).
(2) Case II: $H \in \mathcal{L}$, K is of diagonal type. Let $K = N_G(\Delta)$ be a maximal subgroup of G of diagonal type and $H = N_G(M \times M^{a_2} \times \cdots \times M^{a_m}) \in \mathcal{L}$. If condition (4)(ii) holds then since $|\Omega \cap N_G(\Delta)| \leq |N_G(\Delta)| \leq m \cdot |X/S| \cdot |S|^{m/r}$, we have $|\Omega \cap H| \geq |\Omega \cap N_G(\Delta)|$. By Lemma 2.34 $|\Omega_1 \cap N_G(\Delta)| \leq \min\{z_{r'}(\Pi), |S|\} \cdot |S|^{m/r'-1}$, so if condition (4)(iii) holds then $|\Omega_1 \cap N_G(\Delta)| \leq |\Omega_1 \cap H|$ whenever $H \in \mathcal{H}$.

(3) Case III: $H = H_\ell$ for some prime divisor r of $m|X/S|$. Note that $|H_\ell \cap \Omega| = |\Omega_\ell|$. If ℓ divides m then $|\Omega_\ell| = |A| \cdot |B| \cdot |S|^{m-2}$, otherwise $|\Omega_\ell| = |C| \cdot |S|^{m-1}$. The result follows from condition (8).

Summarizing, if conditions (1), (2), (3), (4)(i), (4)(iii) hold then $\mathcal{L}$ is definitely unbeatable on $\Omega_1 \subseteq N\gamma$, so $|\mathcal{L}| \leq \sigma_{N\gamma}(G) \leq \sigma(G)$. If further condition (4)(ii) holds and $\mathcal{X}$ covers xS then $\mathcal{L}$ covers $N\gamma$, so it covers $N\gamma^k$ for every integer k coprime to $m|X/S|$ (by Lemma 2.14), and $\mathcal{H}$ covers G, so $\sigma(G) \leq |\mathcal{H}| = |\mathcal{L}| + \omega(m|X/S|)$. If also conditions (5), (6), (7), (8) hold then $\mathcal{H}$ is definitely unbeatable on Ω, so $\sigma(G) \geq |\mathcal{H}|$ and the result follows. The proof of Theorem 2.32 is completed.
Let us give a couple of easy applications of Theorem 2.32 (some of which we need in the proof of Theorem 2.17).

Observation 2.36. *Let $\mathcal{K}$ be a minimal cover of the finite group X, so that $|\mathcal{K}| = \sigma(X)$, and let $\mathcal{K}_1$ be a subset of $\mathcal{K}$. Let Ω be a subset of $X - \bigcup_{K \in \mathcal{K}_1} K$. Then $|\mathcal{K}_1| + \sigma_X(\Omega) \leq \sigma(X)$, where $\sigma_X(\Omega)$ denotes the least number of proper subgroups of X needed to cover Ω.*

Proposition 2.37. *The following facts hold.*

(1) $15^m \leq \sigma(\mathrm{Alt}(7) \wr C_m) \leq \omega(m) + 15 \cdot 21^{m-1} + 15^m + 7^{m-1}$,
$8^m \leq \sigma(PSL(3,2) \wr C_m) \leq \omega(m) + 7^m + 8^m$.
(2) $10^m \leq \sigma(\mathrm{Alt}(5)^m \rtimes C_{2m}) \leq \omega(2m) + 5^m + 10^m$.
(3) *If every prime divisor of m belongs to $\{2,3\}$ and $m \neq 3$ then* $\sigma(\mathrm{Alt}(5)^m \rtimes C_{2m}) = \omega(2m) + 5^m + 10^m$.
(4) $\sigma(\mathrm{Alt}(6)^m \rtimes C_{2m}) = \omega(2m) + 2 \cdot 6^m$.

Proof. The groups we are considering are monolithic primitive groups G with non-abelian socle S^m and $G/\operatorname{soc}(G)$ cyclic. Let us use Notations 2.2. In case $X = S$ we have $G = S \wr C_m$. In case $S = \mathrm{Alt}(n)$ and $X = \mathrm{Sym}(n)$ we have $G \cong S^m \rtimes C_{2m}$. The upper bounds follow from Proposition 2.29 and the following facts:

- $\mathrm{Alt}(7)$ is covered by 15 subgroups isomorphic to $SL(3,2)$, 15 subgroups isomorphic to $\mathrm{Sym}(5)$ and one subgroup isomorphic to $\mathrm{Alt}(6)$ (cfr. [**KR**]).
- $PSL(3,2)$ is covered by the 8 normalizers of the Sylow 7-subgroups and 7 subgroups isomorphic to $\mathrm{Sym}(4)$ (cfr. [**BFS**]).
- $\mathrm{Sym}(5) - \mathrm{Alt}(5)$ is covered by the $10+5$ intransitive maximal subgroups of $\mathrm{Sym}(5)$.
- $\mathrm{Sym}(6) - \mathrm{Alt}(6)$ is covered by the 12 subgroups of $\mathrm{Sym}(6)$ isomorphic to $\mathrm{Sym}(5)$.

From now on we only deal with the lower bounds.
We prove (1). Let $S \in \{\mathrm{Alt}(7), PSL(3,2)\}$. If $S = \mathrm{Alt}(7)$ let $\mathcal{M}$ be a conjugacy class of subgroups of S isomorphic to $PSL(3,2)$ (so that $|\mathcal{M}| = 15$), if $S = PSL(3,2)$ let $\mathcal{M}$ be the family of the 8 normalizers of Sylow 7-subgroups of S, and let Π be the set of elements of order 7 in S. Let $C = \emptyset$. Recall that $|\mathrm{Alt}(7)| = 2520$ and $|PSL(3,2)| = 168$. Note that:

- $|\Pi| = 720$ if $S = \mathrm{Alt}(7)$, $|\Pi| = 48$ if $S = PSL(3,2)$;
- if $M \in \mathcal{M}$ then $|M \cap \Pi| = 48$ if $S = \mathrm{Alt}(7)$, $|M \cap \Pi| = 6$ if $S = PSL(3,2)$;
- all the maximal subgroups of S containing elements of Π are isomorphic;
- $|\Pi|/|\mathcal{S}| = |M \cap \Pi|$ for every $M \in \mathcal{M}$, thus two distinct elements of $\mathcal{M}$ do not have elements of Π in common.

This implies that conditions (1), (2), (3) and (4)(i) of Theorem 2.32 are fulfilled. The result follows if we can show that condition (4)(iii) is also fulfilled. Since the largest order of an element of S is 7, $r_q(\Pi) \leq 1$, thus we are reduced to show that $|M|^{m-1} \cdot |M \cap \Pi| \geq |\Pi| \cdot |S|^{m/r-1}$ for $M \in \mathcal{M}$. Since $|\Pi|/|M \cap \Pi| = |S : M|$, we need to show that $|M|^m \geq |S|^{m/r}$, i.e. $|M|^r \geq |S|$. Since $r \geq 2$, this follows from $|S : M|^2 \leq |S|$.

We prove (2). The group $G = \mathrm{Alt}(5)^m \rtimes C_{2m}$ is described in Theorem 2.32 when $S = \mathrm{Alt}(5)$ and $X = \mathrm{Sym}(5)$. Suppose this holds. Let Π be the set of the $(3,2)$-cycles in $\mathrm{Sym}(5)$, and let $\mathcal{M}$ be the set of the intransitive maximal subgroups of $\mathrm{Alt}(5)$ of type $(3,2)$. It is easy to see that conditions (1), (2), (3), (4)(i) of Theorem 2.32 are fulfilled, so we are left with condition (4)(iii). Since the elements of Π have no square roots nor cubic roots in $\mathrm{Sym}(5)$, we may assume that $q \geq 5$. It suffices to prove that $6^{m-1} \cdot 2 \geq 2m \cdot 60^{m/5}$, which is clearly true.

We prove (3). Suppose that all the prime divisors of m belong to $\{2,3\}$, and let $G := \mathrm{Alt}(5)^m \rtimes C_{2m}$. Fix a minimal cover $\mathcal{K}$ of G consisting of maximal subgroups. Let $\mathcal{K}_0$ be the family of the maximal subgroups of G of the form $N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ with $a_2, \ldots, a_m \in \mathrm{Alt}(5)$ and M an intransitive maximal subgroup of $\mathrm{Alt}(5)$ of type $(3,2)$. Note that $|\mathcal{K}_0| = 10^m$. Since the $(3,2)$-cycles are not of the form x^2 or x^3 for $x \in \mathrm{Sym}(5)$, by Lemma 2.34 the only maximal subgroups of G which contain elements of the form $(s_1, \ldots, s_m)\gamma$ where $s_1 \cdots s_m x$ is a $(3,2)$-cycle are the subgroups in $\mathcal{K}_0$. In particular $\mathcal{K}_0 \subset \mathcal{K}$. Let A be the set of the $(3,2)$-cycles in $\mathrm{Sym}(5)$, let B the set of the 4-cycles in $\mathrm{Sym}(5)$ and let C be the set of the 5-cycles in $\mathrm{Sym}(5)$ if m is odd, while if m is even let $C = \emptyset$. Moreover, let

$$\Pi := \{(2354), (4521), (4132), (1253), (4531), (3245), (1352), (2314), (4125), (3541)\}.$$

For any prime divisor ℓ of $2m$ let Ω_1, Ω_ℓ, H_ℓ, r, r', $\mathcal{L}$ be defined as in the proof of Theorem 2.32. Note that $r' \geq 3$ and $|\mathcal{L}| = 5^m$.

Note that if H is a maximal subgroup of G of diagonal type and ℓ is a prime divisor of $2m$ then $|H \cap \Omega_\ell| \leq |H \cap \mathrm{soc}(G)| \leq |S|^{m/2}$. Moreover $K \cap \Omega_\ell = \emptyset$ for every maximal subgroup K of product type and $|A| \cdot |B| \leq |C| \cdot |\mathrm{Alt}(5)|$. Therefore if $H_\ell \notin \mathcal{K}$ then the elements of $\mathcal{K}$ which intersect Ω_ℓ non-trivially are at least $|\Omega_\ell|/60^{m/2} \geq 20 \cdot 30 \cdot 60^{m-2}/60^{m/2} = 10 \cdot 60^{m/2-1}$. Therefore since the elements of $\mathcal{K}_0$ intersect Ω_ℓ trivially we obtain $10 \cdot 60^{m/2-1} \leq \sigma(G) - 10^m \leq 5^m + \omega(2m)$, contradiction. Let $\mathcal{K}_1 := \mathcal{K}_0 \cup \{H_2, H_3\}$. We have proven that $\mathcal{K}_1 \subset \mathcal{K}$.

Let us prove that (*) "$\mathcal{L}$ is definitely unbeatable on Ω_1". By Observation 2.36 this implies the result. Note that conditions (1), (2), (3) of Theorem 2.32 are fulfilled. Using the ideas in the proof of Theorem 2.32 we see that if conditions (4)(i) and (4)(iii) are also fulfilled then (*) holds.

Let us deal with condition (4)(i). Let $M \in \mathcal{M}$ and let V be a maximal subgroup of $\mathrm{Sym}(5)$ supplementing $\mathrm{Alt}(5)$ and such that $V \cap \mathrm{Alt}(5) \notin \mathcal{M}$. Note that if $V \cap \Pi \neq \emptyset$ then $|V \cap \mathrm{Alt}(5)| = 10$. The only intransitive maximal subgroups of $\mathrm{Alt}(5)$ whose normalizers in $\mathrm{Sym}(5)$ intersect Π non-trivially are the five point stabilizers, which have order 12. If m is even then $C = \emptyset$ and $|N_{\mathrm{Sym}(5)}(M) \cap \Pi| = |V \cap \Pi| = 2$ for every $M \in \mathcal{M}$, hence the result follows. If $m \notin \{5,7\}$ is odd then $|V \cap (\Pi \cup C)| = 6$ and we have to show that $12^{m-1} \cdot 2 \geq 10^{m-1} \cdot 6$, which is true for $m \geq 8$. If $m \in \{5,7\}$ then $|N_{\mathrm{Sym}(n)}(K) \cap (\Pi \cup C)| = 4$ and we have to show that $12^{m-1} \cdot 2 \geq 10^{m-1} \cdot 4$, which is true.

Let us deal with condition (4)(iii). Since $r' \geq 3$ what we need to show is $2 \cdot 12^{m-1} \geq 60^{m/3}$, which is clearly true for $m \geq 3$.
We prove (4). The case $m = 1$ has been discussed in Example 1.7, so let us assume that $m \geq 2$. The group $G = \mathrm{Alt}(6)^m \rtimes C_{2m}$ is described in Theorem 2.32 when $S = \mathrm{Alt}(6)$ and $X = \mathrm{Sym}(6)$. Let $\mathcal{K}$ be a minimal cover of G. Let $\mathcal{K}_0$ be the family of the maximal subgroups of G of product type $N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ where $M \cong \mathrm{Sym}(5)$. Note that $|\mathcal{K}_0| = 12 \cdot 6^{m-1}$. By Lemma 1.6 $\mathcal{K}_0 \subseteq \mathcal{K}$: indeed, every member of $\mathcal{K}_0$ is isomorphic to $\mathrm{Alt}(5)^m \rtimes C_{2m}$ so by (2) its covering number is at least $10^m > 12 \cdot 6^{m-1} + \omega(2m) \geq \sigma(G)$.
Let A be the set of the $(3,2)$-cycles in $\mathrm{Sym}(6)$, let B be the set of the 6-cycles in $\mathrm{Sym}(6)$, and let C be the set of the 3-cycles in $\mathrm{Sym}(6)$. For any prime divisor ℓ of $2m$ let Ω_ℓ, H_ℓ be defined as in the proof of Theorem 2.32. Since no subgroup of $\mathrm{Sym}(6)$ intersects both A and B non-trivially, $H \cap \Omega_\ell = \emptyset$ for every prime divisor ℓ of m and every maximal subgroup H of G of product type. Let $\mathcal{K}_1$ be the family consisting of the members of $\mathcal{K}_0$ together with the subgroups H_ℓ for ℓ a prime divisor of m. If H is a maximal subgroup of G of diagonal type then $|H \cap \Omega_\ell| \leq |H \cap \mathrm{soc}(G)|$. Therefore if ℓ is a prime divisor of m and $H_\ell \notin \mathcal{M}$ then in order to cover Ω_ℓ we need at least

$$\frac{|\Omega_\ell|}{|H \cap \mathrm{soc}(G)|} \geq \frac{40 \cdot 360^{m-1}}{360^{m/2}} = 40 \cdot 360^{m/2-1}$$

subgroups. Since the subgroups of product type intersect Ω_ℓ trivially we obtain that $40 \cdot 360^{m/2-1} \leq \sigma(G) - 12 \cdot 6^{m-1} \leq \omega(2m)$, contradiction. Therefore $\mathcal{K}_1 \subseteq \mathcal{K}$. If m is even then $\mathcal{K}_1$ covers G, thus $\mathcal{K}_1 = \mathcal{K}$ and we are done. Suppose m is odd. Since the subgroups of $\mathrm{Sym}(6)$ isomorphic to $\mathrm{Sym}(5)$ do not intersect C, the family $\mathcal{K}_1$ does not cover Ω_2. Since $\Omega_2 \subset H_2$ and $\mathcal{K}_1 \cup \{H_2\}$ covers G, we obtain $\sigma(G) = |\mathcal{M}| = \omega(2m) + 2 \cdot 6^m$. □

5.3. Attacking conjecture 1.28. Let us fix the notations of this section. Whenever H is a σ-elementary group, we denote by $N_1, \ldots, N_k$ its minimal normal subgroups, and by $G_1, \ldots, G_k$ the primitive monolithic groups associated to $N_1, \ldots, N_k$ respectively.

Definition 2.38. *Let G be a primitive monolithic group with non-abelian socle. We say that G is "excluded" if it satisfies the following property:*

- *Whenever H is a non-monolithic σ-elementary group, if $i \in \{1, \ldots, k\}$ is such that $\sigma^*(G_i) \leq \sigma^*(G_j)$ for every $j \in \{1, \ldots, k\}$ such that N_j is non-abelian then $G_i \not\cong G$.*

By Corollary 1.21, Conjecture 1.28 is equivalent to the statement that every primitive monolithic group with non-abelian socle is excluded. So what we need in order to attack Conjecture 1.28 are sufficient conditions for a monolithic primitive group G to be excluded.
The following lemma is a fair generalization of Corollary 2.13.

Proposition 2.39. *Let G be a primitive monolithic group with non-abelian socle. If $\sigma(G) < 2\sigma^*(G)$ then G is excluded.*

Proof. Let H be a σ-elementary group. Suppose by contradiction that there exists $i \in \{1, \ldots, k\}$ such that $\sigma^*(G_i) \leq \sigma^*(G_j)$ for every $j \in \{1, \ldots, k\}$ such that N_j is non-abelian and $G_i \cong G$. Without loss of generality assume $i = 1$. By Proposition 2.10 we have

$\sum_{j=1}^{k} \sigma^*(G_j) \le \sigma(G) < 2\sigma^*(G)$, therefore $\sigma^*(G_j) < \sigma^*(G)$ for $j = 2, \dots, k$ and by minimality of $\sigma^*(G)$ and Corollary 1.21 this implies that either $k = 1$ (i.e. H is monolithic) or $k = 2$ and N_2 is abelian. In the latter case, since $\ell_{G_2}(N_2) = |N_2|$, Proposition 2.10 implies that

$$|N_2| + \sigma^*(G) = \ell_{G_2}(N_2) + \sigma^*(G) \le \sigma(H) \le \min\{\sigma(G), \sigma(G_2)\}.$$

Now by hypothesis $\sigma(G) < 2\sigma^*(G)$, and Proposition 1.20 implies that $\sigma(G_2) < 2|N_2|$. This leads to a contradiction. □

Proposition 2.40. *Let G be a primitive monolithic group with non-abelian socle, and let us use Notations 2.2. Suppose that X/S is abelian. If L/S is non-cyclic then G is excluded.*

Proof. Let $\mathcal{K}$ be a minimal covering of L/S. For each $K \in \mathcal{K}$ define

$$R_K := \{(x_1, \dots, x_m)k \in G \mid x_1 \cdots x_m S \in K\}.$$

Since X/S is abelian, R_K is a (proper) subgroup of G for each $K \in \mathcal{K}$, and since $\mathcal{K}$ covers L/S, $\bigcup_{H \in \mathcal{H}} R_H = G$, so $\sigma(G) \le \sigma(L/S) \le |X/S| \le |\operatorname{Out}(S)| < m(S)$. If G was not excluded, this would contradict Corollary 2.11. □

Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2 and Definition 2.9. Let $\mathcal{Z}$ be the set of pairs (z, w) in $X \times X$ such that $\langle z^a, w^b \rangle \supseteq S$ for every $a, b \in S$. By [**KLS**], $\mathcal{Z} \cap (S \times S) \neq \emptyset$. Let k be a non-m-cycle in K, let $O_1 = (i_1, \dots, i_r)$, $O_2 = (j_1, \dots, j_s)$ be two cycles in the cyclic decomposition of k, and for $\rho^{-1}(k) \ni h = (x_1, \dots, x_m)k$, with $x_1, \dots, x_m \in X$, let $h_{O_1} := x_{i_1} \cdots x_{i_r}$ and $h_{O_2} := x_{j_1} \cdots x_{j_s}$.
The following lemma is crucial.

Lemma 2.41. *Let $\mathcal{E}_k := \{(h_{O_1}, h_{O_2}) \mid h \in \rho^{-1}(k)\} \cap \mathcal{Z}$. Let r be the smallest prime divisor of m. If $g \in \rho^{-1}(k)$ then $\sigma_{Ng}(G) \ge |\mathcal{E}_k| \cdot |S|^{m-m/r-2}$.*

Proof. Let

$$\mathfrak{X} := \{h \in Ng \mid (h_{O_1}, h_{O_2}) \in \mathcal{E}_k\}.$$

Note that if $h \in Ng$, θ, $\varphi \in X$ are such that $h_{O_1} \equiv \theta \mod S$ and $h_{O_2} \equiv \varphi \mod S$ then there exists $t \in N$ such that $(th)_{O_1} = \theta$, $(th)_{O_2} = \varphi$. This implies that $|\mathfrak{X}| \ge |\mathcal{E}_k| \cdot |S|^{m-2}$. It is easy to show that if $a_2, \dots, a_m \in S$ and $h \in \rho^{-1}(k) \cap N_G(M \times M^{a_2} \times \cdots \times M^{a_m})$ then $h_{O_1} \in N_X(M)^{a_{i_1}}$, $h_{O_2} \in N_X(M)^{a_{j_1}}$. By the definition of $\mathcal{E}_k$, we deduce that $\mathfrak{X} \cap H = \emptyset$ whenever H is a supplement of N of product type. Since the maximal subgroups of G complementing N intersect Ng in at most one point, this implies that in order to cover $\mathfrak{X}$ with supplements of N we need at least $|\mathcal{E}_k| \cdot |S|^{m-2}/|S|^{m/r}$ of them. □

The statement of the following theorem is roughly the following: a primitive monolithic group G with non-abelian socle (let us use Notations 2.2) is excluded if X/S is abelian and there exists a family of "big" maximal subgroups of X "not so far" from covering xS and definitely unbeatable on a subset Π of xS.

Theorem 2.42. *Let G be a primitive monolithic group with non-abelian socle, let us use Notations 2.2. Assume that X/S is abelian. Call r the smallest prime divisor of m. Suppose that if $m \ge 2$*

then for every $x \in X$ such that $L = \langle T, x\rangle$ there exist two families $\mathcal{M}$, $\mathcal{J}$ of proper subgroups of S and a subset Π of xS such that:

(0) *for every two cosets rS, tS of S in X there exist two elements $z \in rS$, $w \in tS$ such that $\langle z^a, w^b\rangle \supseteq S$ for every $a, b \in S$. Let $E_{nc} := \min\{|\mathcal{E}_k| \mid k \in K \text{ non-m-cycle}\}$ where $\mathcal{E}_k$ is defined as in Lemma 2.41.*

(1) *Every element of $\mathcal{M} \cup \mathcal{J}$ is of the form $V \cap S$ where V is a maximal subgroup of X supplementing S (so that $N_X(V \cap S) = V$);*

(2) $\bigcup_{M\in\mathcal{M}} N_{S\langle x\rangle}(M) \supseteq \Pi$ *and* $\bigcup_{M\in\mathcal{J}} N_{S\langle x\rangle}(M) \supseteq xS - \Pi$*;*

(3) $N_{S\langle x\rangle}(M) \cap \Pi \neq \emptyset$ *for every* $M \in \mathcal{M}$*;*

(4) $\Pi \cap N_{S\langle x\rangle}(M_1) \cap N_{S\langle x\rangle}(M_2) = \emptyset$ *for every* $M_1 \neq M_2$ *in* $\mathcal{M}$*;*

(5) $\sum_{M\in\mathcal{M}\cup\mathcal{J}} |S : M|^{m-1} \leq E_{nc} \cdot |S|^{m-m/r-2}$*;*

(6) $|M|^{m-1}|N_{S\langle x\rangle}(M) \cap \Pi| \geq |K|^{m-1}|N_{S\langle x\rangle}(K) \cap \Pi|$ *for every $M \in \mathcal{M}$ and for every proper non-trivial subgroup K of S outside $\mathcal{M}$ such that $N_{\langle S,x\rangle}(K)$ is a maximal subgroup of $\langle S, x\rangle$ supplementing S;*

(7) $|M|^{m-1} \cdot |N_{S\langle x\rangle}(M) \cap \Pi| \geq m \cdot |S\langle x\rangle/S| \cdot |S|^{m/r}$ *for every* $M \in \mathcal{M}$*;*

(8) $\sum_{M\in\mathcal{J}} |S : M|^{m-1} + 2^{m-1} < \sum_{M\in\mathcal{M}} |S : M|^{m-1}$.

Then G is excluded.

Remark 2.43. *Condition (0) of Theorem 2.42 is always fulfilled if $X = S$ by* [**KLS**, Theorem 1.3]. *Condition (8) is always fulfilled if $\mathcal{J} = \emptyset$.*

Observation 2.44. *Let the hypotheses of Theorem 2.42 hold. For $x, y \in X$ let $E_{x,y}$ be the number of elements $(z, w) \in xS \times yS$ with the property that $\langle z^a, w^b\rangle \supseteq S$ for every $a, b \in S$. Then $E_{nc} \geq \min_{x,y\in X} E_{x,y}$.*

We now prove Theorem 2.42. By Proposition 2.39 it is enough to prove that $\sigma(G) < 2\sigma^*(G)$.

Lemma 2.45. $\sigma^*(G) \geq \sum_{M\in\mathcal{M}} |S : M|^{m-1}$.

Proof. Fix a family Ω of generators of $G/\operatorname{soc}(G)$ such that $\sigma_\Omega(G) = \sigma^*(G)$. By definition of L, Ω must contain a coset Ng such that, writing $g = (x_1, \dots, x_m)k$ with $k \in K$, $\langle T, x_1 \cdots x_m\rangle = L$. Moreover by Lemma 2.41 and conditions (0), (5) we may assume that k is an m-cycle. Let $x := x_1 \cdots x_m$. By Lemma 2.7 we have

$$\frac{N_{N\langle g\rangle}(S_1)/C_{N\langle g\rangle}(S_1)}{S_1 C_{N\langle g\rangle}(S_1)/C_{N\langle g\rangle}(S_1)} \cong \langle xS\rangle \subseteq X/S.$$

We are reduced to prove that $\sigma_{Ng}(N\langle g\rangle) \geq \sum_{M\in\mathcal{M}} |S : M|^{m-1}$, and this follows from Theorem 2.32. □

Lemma 2.45, Theorem 2.28 and condition (8) imply that

$$\sigma(G) \leq \sum_{M\in\mathcal{M}\cup\mathcal{J}} |S : M|^{m-1} + 2^{m-1} < 2\sigma^*(G).$$

5.4. Application: $X = S = M_{11}$. Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2. Suppose $X = S = M_{11}$ and $m \geq 10$. Recall that $|M_{11}| = 7920$. We want to apply Theorem 2.32 (in case $G/\operatorname{soc}(G)$ is cyclic) and Theorem 2.42 to G.
Let $\mathcal{M}$ be the set of all 11 conjugates of the maximal subgroup M_{10} of M_{11} together with all 12 conjugates of the maximal subgroup $PSL(2,11)$ of M_{11}. It is easy to check that $\mathcal{M}$ is a covering for M_{11}. Let $\mathcal{J} = \emptyset$.
Let A be the set of elements of order 8 in M_{11}, let B be the set of elements of order 11 in M_{11}, let $C := \emptyset$, and let $\Pi := A \cup B$. We have $|A| = 1980$, $|B| = 1440$ and $|\Pi| = 1980 + 1440 = 3420$.
By [**GAP**] we know that the maximal subgroups of M_{11} are: M_{10}, $PSL(2,11)$, $M_9 : 2$, S_5, and $M_8 : S_3$, and that for these we have the following.

- M_{10} has order 720, it contains 180 elements of order 8 and no element of order 11; no element of order 8 is contained in two distinct conjugates of M_{10};
- $PSL(2,11)$ has order 660, it contains no element of order 8 and 120 elements of order 11; no element of order 11 is contained in two distinct conjugates of $PSL(2,11)$;
- $M_9 : 2$ has order 144, it contains 36 elements of order 8 and no element of order 11;
- S_5 has order 120, it contains no element of order 8 and no element of order 11;
- $M_8 : S_3$ has order 48, it contains 12 elements of order 8 and no element of order 11.

This implies that conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled. It also implies that $E_{nc} \geq |A| \cdot |B|$. Conditions (5), (6), (7) translate (respectively) as follows:

- $11^m + 12^m \leq 1980 \cdot 1440 \cdot 7920^{m-m/r-2}$, true for $m \geq 2$;
- $\min\{720^{m-1} \cdot 180, 660^{m-1} \cdot 120\} \geq \max\{144^{m-1} \cdot 36, 120^{m-1} \cdot 0, 48^{m-1} \cdot 12\}$, true for $m \geq 1$.
- $\min\{720^{m-1} \cdot 180, 660^{m-1} \cdot 120\} \geq m \cdot 7920^{m/2}$, true for $m \geq 1$;

Thus Theorem 2.42 applies if $m \geq 2$. In particular using Corollary 2.13 (to solve the case $m = 1$) we obtain that

Proposition 2.46. *Let $m \geq 1$, and let K be a transitive subgroup of* $\mathrm{Sym}(m)$*. Then $M_{11} \wr K$ is excluded.*

Suppose now that $G/\operatorname{soc}(G)$ is cyclic, i.e. $G = M_{11} \wr C_m$. In order to prove that $\sigma(G) = \omega(m) + 11^m + 12^m$ for every $m \geq 1$ we are left to show that condition (8) of Theorem 2.32 is fulfilled. So suppose $m \geq 2$. Condition (8) is reduced to the following inequality:

$$1980 \cdot 1440 \cdot 7920^{m-2} \geq \max\{144^{m-1} \cdot 36, m \cdot 7920^{m/2}\}.$$

This is true for every $m \geq 2$.

5.5. Application: $S = PSL(2,q)$. Let us use Notations 2.2. Under the hypotheses of Theorem 2.42, suppose $S = PSL(2,q)$, $X \in \{PSL(2,q), PGL(2,q)\}$, $q \geq 11$ an odd prime power, $m > 5$ and $r \geq 5$. Recall that $|PSL(2,q)| = q(q^2-1)/2$. Write $q = p^f$ with p an odd prime, and if $f = 1$ suppose that $X = S$. We want to apply Theorem 2.42 to G. We also want to apply Theorem 2.32 to G in case $G/\operatorname{soc}(G)$ is cyclic and $f = 1$ (so when checking the requirements of Theorem 2.32 we are assuming $f = 1$).
Let G act on the projective line, which is a set of size $q+1$. If $f = 1$ let $\mathcal{M}$ be the set of all the $q+1$ point stabilizers (which is a conjugacy class of subgroups isomorphic to $C_p^f \rtimes C_{(q-1)/2}$)

together with the Singer cycles normalizers (a conjugacy class of $q(q-1)/2$ maximal subgroups isomorphic to D_{q+1}). If $f > 1$ let $\mathcal{M}$ be the family of all the Singer cycles normalizers. It is easy to check that $\mathcal{M}$ is a covering for $PSL(2,q)$ if $f = 1$, so let $\mathcal{J} = \emptyset$ in this case. If $f > 1$ let $\mathcal{J}$ be the family of the $q+1$ point stabilizers.
Let $A \subseteq PSL(2,q)$ be a set of $(q+1)(p-1)$ elements conjugate to some non-trivial power of the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It is a set of elements of order p fixing a unique point on the projective line and it has the property that $(A \cap M) \cup \{1\}$ is a group of order p for every point stabilizer M.
Let A' be the subset of $PGL(2,q)$ consisting of the diagonal matrices $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ with x of multiplicative order $q-1$ and $xy \neq 1$.
Let B be the set of all irreducible elements of $PGL(2,q)$ of order $(q+1)/\varepsilon$, where $\varepsilon = 1$ if $X = PGL(2,q)$ and $\varepsilon = 2$ if $X = PSL(2,q)$ (the Singer cycles). Note that $|B| = \frac{1}{2}q(q-1)\varphi(\frac{q+1}{\varepsilon})$.
Let $C = \emptyset$, and put $\Pi = A \cup B$ if $k = 1$, $\Pi = B$ if $k > 1$.
Note that $\min\{|A|, |A'|\} \cdot |B| \geq |S|$.
By [**Dlg**] the maximal subgroups of $PSL(2,q)$ are the following (for p odd).

- $C_p^f \rtimes C_{(q-1)/2}$ (the point stabilizers);
- D_{q-1} if $q \geq 13$;
- D_{q+1} if $q \neq 7, 9$ (the Singer cycles);
- $PGL(2,q_0)$ for $q = q_0^2$ (two conjugacy classes);
- $PSL(2,q_0)$ for $q = q_0^\ell$ where ℓ is an odd prime;
- $\mathrm{Alt}(5)$ for $q \equiv \pm 1 \mod (10)$ where either $q = p$ or $q = p^2$ and $p \equiv \pm 3 \mod (10)$ (two conjugacy classes);
- $\mathrm{Alt}(4)$ for $q = p \equiv \pm 3 \mod (8)$ and $q \not\equiv \pm 1 \mod (10)$;
- $\mathrm{Sym}(4)$ for $q = p \equiv \pm 1 \mod (8)$ (two conjugacy classes).

The maximal subgroups of $PGL(2,q)$ not containing $PSL(2,q)$ are the following (for p odd).

- $C_p^f \rtimes C_{q-1}$ (the point stabilizers);
- $D_{2(q-1)}$ for $q \neq 5$;
- $D_{2(q+1)}$ (the Singer cycles);
- $\mathrm{Sym}(4)$ for $q = p \equiv \pm 3 \mod (8)$;
- $PGL(2,q_0)$ for $q = q_0^\ell$ with ℓ an odd prime.

Since no Singer cycle normalizer contains elements of order $(q-1)/\varepsilon$ or p, it follows easily that condition (0) of Theorem 2.42 is fulfilled for X: consider the pairs (z,w) where $z \in A, w \in B$ if $X = S$, and $z \in A$, $w \in B$ or $z \in A'$, $w \in B$ if $X \neq S$.
Since $q \geq 11$, no element of Π is contained in a subgroup of the form $\mathrm{Alt}(5)$, $\mathrm{Alt}(4)$, or $\mathrm{Sym}(4)$. Moreover since $(q+1)/2$ and q do not divide $q-1$, no element of Π is contained in a subgroup of the form $D_{2(q-1)}$. Similarly, it is easy to see that no element of A is contained in a Singer cycle normalizer and no element of B is contained in a point stabilizer. Moreover if M is a Singer cycle normalizer then $|\Pi \cap M| = |B \cap M| = \varphi((q+1)/2)$ where φ is Euler's function, and if M is a point stabilizer then $|\Pi \cap M| = q-1$.

This implies that conditions (0), (1), (2), (3), (4) of Theorem 2.42 and conditions (1), (2), (3), (5), (6), (7) of Theorem 2.32 are fulfilled. Moreover $E_{nc} \geq \min\{|A|, |A'|\} \cdot |B| \geq |S|$.
Let us deal with conditions (5), (6), (7) of Theorem 2.42.

- Condition (5): $(q+1)^m + (q(q-1)/2)^m \leq (q(q^2-1)/2)^{m-m/r-1}$. Since $q \geq 11$, $q+1 \leq q(q-1)/2$ and since $r \geq 5$ we are reduced to show that
$$2(q(q-1)/2)^m \leq (q(q^2-1)/2)^{4m/5-1}.$$
This is easily seen to be true if $m \geq 8$.
- Condition (6) is trivially fulfilled since the right-hand side is always zero.
- Condition (7) is implied by $\min\{(q(q-1)/2)^{m-1}, (q+1)^{m-1}\} \geq m \cdot (q(q^2-1)/2)^{m/5}$ (we used that $r \geq 5$), in other words
$$(q+1)^{m-1} \geq m \cdot (q(q^2-1)/2)^{m/5}.$$
Since $m^{1/m} \leq 3/2$ we are reduced to show that
$$\frac{q+1}{(q+1)^{1/m}} \geq (3/2)(q(q^2-1)/2)^{1/5}.$$
Since $m \geq 5$ we are reduced to $(q+1)^5 \geq (3/2)^5(1/2)q(q^2-1)(q+1)$, and this is clearly implied by $q+1 \geq (3/2)^5(1/2)$, i.e. $q \geq 5$.

This also implies condition (4) of Theorem 2.32. Condition (8) of Theorem 2.32 is implied by
$$((p/2)(p^2-1))^{m-1} \geq m \cdot ((p/2)(p^2-1))^{m/5}.$$
Condition (8) of Theorem 2.42 translates as follows:
$$(q+1)^m + 2^{m-1} < (q(q-1)/2)^m.$$
This is clearly true.
We obtain the following:

PROPOSITION 2.47. *Let G be a monolithic group with non-abelian socle, and let us use Notations 2.2. If $X \in \{PSL(2,q), PGL(2,q)\}$, $q \geq 11$ is an odd prime power, and the smallest prime divisor of m is at least 5, then G is excluded.*

6. The main application: $S = \mathrm{Alt}(n)$

In this section we will prove the following result.

THEOREM 2.48. *Let G be a primitive monolithic group with non-abelian socle, and let us use Notations 2.2. Suppose that $S = \mathrm{Alt}(n)$ for some integer $n \geq 5$. Suppose that $m \geq 3$ and $m \neq 4$. Then G is excluded in each of the following cases:*

(1) *$n \geq 15$ is odd and $X = \mathrm{Sym}(n)$.*
(2) *$n \geq 30$ is even and $X = \mathrm{Sym}(n)$.*
(3) *$n \geq 5$ is odd with a prime divisor at most $\sqrt[4]{n}$ and $X = \mathrm{Alt}(n)$.*
(4) *$n \geq 20$ is divisible by 4 and $X = \mathrm{Alt}(n)$.*
(5) *$n \geq 20$ is congruent to 2 modulo 4 and $X = \mathrm{Alt}(n)$.*

The following result follows as a corollary.

THEOREM 2.49. *Let H be a non-abelian σ-elementary group, and suppose that all the non-abelian minimal subnormal subgroups of H are either isomorphic to M_{11} or to $\mathrm{Alt}(n)$ where $n \geq 30$ admits a prime divisor smaller than or equal to $\sqrt[4]{n}$. Then H is monolithic.*

PROOF. Let $\mathrm{soc}(H) = N_1 \times \cdots \times N_k$, with $N_1, \ldots, N_k$ minimal normal subgroups of H, and call G_i the monolithic primitive group associated to N_i for $i = 1, \ldots, k$. We need to prove that $k = 1$, so assume by contradiction that $k \geq 2$. Let $G := G_1$, and suppose without loss of generality that N_1 is non-abelian (this assumption is allowed by Corollary 1.21) and $\sigma^*(G) \leq \sigma^*(G_i)$ for every $i \in \{1, \ldots, k\}$ such that N_i is non-abelian. Let us use Notations 2.2 for G. If $S = M_{11}$ then since $\mathrm{Out}(M_{11}) = \{1\}$ the result follows by Proposition 2.46, so assume that $S = \mathrm{Alt}(n)$ with $n \geq 30$ admitting a prime divisor at most $\sqrt[4]{n}$. Theorem 2.48 implies that $m \in \{1, 2, 4\}$. But recall that $G/\mathrm{soc}(G)$ embeds in $X \wr K$, and K is a transitive subgroup of $\mathrm{Sym}(m)$. Since $X/\mathrm{soc}(X)$ has order 1 or 2, if $|K|$ is a power of 2 the result follows by Corollary 2.13. If $|K|$ is not a power of 2 then K is a non-cyclic transitive subgroup of $\mathrm{Sym}(4)$, i.e. $K \in \{D_8, C_2 \times C_2, \mathrm{Alt}(4), \mathrm{Sym}(4)\}$, in particular $\sigma(H) \leq \sigma(G) \leq \sigma(K) \leq 5$, and the result follows for example by Corollary 2.16. $\square$

We will also apply Theorem 2.32 and prove the following bounds.

THEOREM 2.50. *Let G be a primitive monolithic group with non-abelian socle S^m, and let us use Notations 2.2. Suppose that $S = \mathrm{Alt}(n)$ for some integer $n \geq 5$ and that $G/\mathrm{soc}(G)$ is cyclic. The following facts hold.*

- *Suppose $n \geq 11$ is odd and $X = \mathrm{Sym}(n)$. Then*
$$\sigma(G) = \omega(2m) + \sum_{i=1}^{(n-1)/2} \binom{n}{i}^m.$$
- *Suppose $n \geq 8$ is even and $X = \mathrm{Sym}(n)$. Then*
$$\left(\frac{1}{2}\binom{n}{n/2}\right)^m \leq \sigma(G) \leq \omega(2m) + \left(\frac{1}{2}\binom{n}{n/2}\right)^m + \sum_{i=1}^{[n/3]} \binom{n}{i}^m.$$
In particular, for fixed m, $\sigma(G) \sim \left(\frac{1}{2}\binom{n}{n/2}\right)^m$ as $n \to \infty$.
- *Suppose $n \geq 27$ is odd with a prime divisor at most $\sqrt[4]{n}$ and $X = \mathrm{Alt}(n)$. Then*
$$\left(\frac{n!}{(n/p)!^p p!}\right)^m \leq \sigma(G) \leq \omega(m) + \sum_{i=1}^{[n/3]} \binom{n}{i}^m + \left(\frac{n!}{(n/p)!^p p!}\right)^m.$$
- *Suppose $n > 12$ is divisible by 4 and $X = \mathrm{Alt}(n)$. Then*
$$\frac{1}{2}\sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i}^m \leq \sigma(G) \leq \omega(m) + \frac{1}{2}\sum_{\substack{i=1 \\ i \text{ odd}}}^{n} \binom{n}{i}^m + \left(\frac{1}{2}\binom{n}{n/2}\right)^m.$$

- *Suppose $n > 12$ is congruent to 2 modulo 4 and $X = \mathrm{Alt}(n)$. Then*

$$\sigma(G) = \alpha(m) + \sum_{\substack{i=1 \\ i \text{ odd}}}^{(n/2)-2} \binom{n}{i}^m + \frac{1}{2^m}\binom{n}{n/2}^m.$$

Theorem 2.50 summarizes the results proved in [**GM**] (dealing with the case $X = \mathrm{Alt}(n)$) by Attila Maróti and myself and in [**Gar2**] (dealing with the case $X = \mathrm{Sym}(n)$) by myself.
The remaining of this section is devoted to the proof of Theorems 2.48 and 2.50. We will prove Theorem 2.48 by applying Theorem 2.42, and we will prove Theorem 2.50 by applying Theorem 2.32. Throughout the proof we will use the following fact, proved in [**MarP**]: the order of a primitive maximal subgroup of $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ not containing $\mathrm{Alt}(n)$ is at most 2.6^n.
Condition (0) of Theorem 2.42 for $S = \mathrm{Alt}(n)$ is implied by the following fact if $n \neq 6$.

Proposition 2.51. *Let $n \geq 5$, $n \neq 6$ be an integer, and if $n \geq 8$ let ℓ be a prime such that $n/2 < \ell < n-2$ (such a prime exists by the Bertrand-Chebyshev theorem), if $n = 5$ let $\ell = 3$ and if $n = 7$ let $\ell = 5$. Let $a, b \in \mathrm{Sym}(n)$ have cyclic structures according to the following table.*

	Case 1 $[-,-]$	*Case 2* $[+,-]$	*Case 3* $[+,+]$
$n \geq 5$ *odd*	$(2, n-2), (n-1)$	(n), $(\ell, n-\ell)$	$(\ell), (n)$
$n \geq 8$ *even*	$(\ell, 2, n-\ell-2), (n)$	$(\ell), (n)$	$(2, n-2), (\ell, n-\ell)$

Then $\langle a, b\rangle \supseteq \mathrm{Alt}(n)$.

Proof. It is easy to see that $\langle a, b\rangle$ is a primitive subgroup of $\mathrm{Sym}(n)$ containing either a 2-cycle or a ℓ-cycle. By the Jordan theory (cfr. for example [**Cam**, Theorem 6.15, Exercise 6.6]), if $n \geq 8$ then $\langle a, b\rangle \supseteq \mathrm{Alt}(n)$. If $n \in \{5, 7\}$ the result follows from the fact that the transitive subgroups of $\mathrm{Sym}(n)$ not containing $\mathrm{Alt}(n)$ have order coprime to ℓ. □

Let G be a primitive monolithic group with non-abelian socle, and let us use Notations 2.2. Let $S = \mathrm{Alt}(n)$ for some $n \geq 5$, and let E_{nc} be as in the statement of Theorem 2.42. Using Observation 2.44 and Proposition 2.51 it is easy to show that $E_{nc} \geq n!/2$ whenever $n \geq 5$ and $n \neq 6$. Therefore for $S = \mathrm{Alt}(n)$, $n \geq 5$, $n \neq 6$, condition (5) of Theorem 2.42 can be substituted with the following:

$$(5') \qquad \sum_{M \in \mathcal{M} \cup \mathcal{J}} |S : M|^{m-1} \leq |S|^{m-m/r-1}$$

We will deal with each case separately. Let us first prove some useful inequalities.

6.1. Inequalities. Recall the famous

Proposition 2.52 (Stirling's formula). *For all positive integers n we have*

$$\sqrt{2\pi n}(n/e)^n e^{1/(12n+1)} < n! < \sqrt{2\pi n}(n/e)^n e^{1/(12n)}.$$

In the following we let n, m be positive integers.

Lemma 2.53. *Let a, b be positive integers, with $a > b$.*

(1) *Suppose n is odd. Let K be an intransitive maximal subgroup of* $\mathrm{Alt}(n)$. *If* $(n^2-1)^a \geq 4^a e^{2(a-b)} n^{2b}$, *then* $|K|^{a/b} \geq |\,\mathrm{Alt}(n)|$.
(2) *Suppose n is even. Let K be a maximal imprimitive subgroup of* $\mathrm{Alt}(n)$ *of the form* $(\mathrm{Sym}(n/2) \wr \mathrm{Sym}(2)) \cap \mathrm{Alt}(n)$. *If* $n^a \geq 2^a e^{a-b} n^b$, *then* $|K|^{a/b} \geq |\,\mathrm{Alt}(n)|$.

PROOF. We prove only (1), since the proof of (2) is similar. Suppose n is odd. Since the smallest intransitive maximal subgroups of $\mathrm{Alt}(n)$ are the ones of type $((n-1)/2, (n+1)/2)$, what we have to prove is the following inequality:

$$(1/2)^{a/b}((n-1)/2)!^{a/b}((n+1)/2)!^{a/b} \geq n!/2.$$

Since $e^{\frac{a/b}{6(n-1)+1}+\frac{a/b}{6(n+1)+1}} \geq e^{1/12n}$ for every positive integer n, using Stirling's formula we see that it is sufficient to show that

$$(1/2)^{a/b}((n-1)/2e)^{a(n-1)/2b}\sqrt{(\pi(n-1))^{a/b}}((n+1)/2e)^{a(n+1)/2b}\sqrt{(\pi(n+1))^{a/b}} \geq$$
$$\geq (1/2)(n/e)^n\sqrt{2\pi n}.$$

Re-write this as follows:

$$((n^2-1)/4e^2)^{a(n-1)/2b}(\pi/2)^{a/b}(n^2-1)^{a/2b}((n+1)/2e)^{a/b} \geq$$
$$\geq (1/2)(n/e)^n\sqrt{2\pi n}.$$

In other words:

$$((n^2-1)/4e^2)^{an/2b}(\pi(n+1)/2)^{a/b} \geq (1/2)\sqrt{2\pi n}(n/e)^n.$$

Since $\pi(n+1)/2 \geq (1/2)\sqrt{2\pi n}$ we are reduced to prove that

$$((n^2-1)/4e^2)^{an/2b} \geq (n/e)^n,$$

i.e. $(n^2-1)^a \geq (n/e)^{2b}(4e^2)^a = 4^a e^{2(a-b)} n^{2b}$. ☐

The following lemma is shown in the proof of [**MarS**, Lemma 2.1].

LEMMA 2.54. *If $n \geq 8$ we have*

$$((n/a)!)^a a! \geq ((n/b)!)^b b!$$

whenever a and b are divisors of n with $a \leq b$.

LEMMA 2.55. *Let $n \neq 9, 15$ be an odd positive integer, and let $a \geq 3$ be a proper divisor of n. Then*

$$\left(\frac{n-1}{2}\right)!\left(\frac{n-3}{2}\right)! \geq (n/a)!^a \cdot a!.$$

PROOF. Proceed by inspection for $21 \leq n \leq 299$, using lemma 2.54. Assume $n \geq 300$. Let us use Stirling's formula. We are reduced to prove that

$$\sqrt{\pi(n-1)}((n-1)/2e)^{(n-1)/2}\sqrt{\pi(n-3)}((n-3)/2e)^{(n-3)/2} \geq$$
$$\geq 2\sqrt{2\pi n/a}^{\,a}(n/ae)^n\sqrt{2\pi a}(a/e)^a.$$

Using the inequalities $\pi \geq \sqrt{2\pi}$ and $n-3 \geq a$ we are reduced to prove that

$$(n-1)^{1/2}(n-1)^{(n-1)/2}(n-3)^{(n-3)/2} \geq 2/(2e)^2\sqrt{2\pi n/a}^{\,a}(2n/a)^n(a/e)^a,$$

and using $n-1 \geq n-3$ we obtain:

$$(n-1)^{1/2}(n-3)^{n-2} \geq (2/(4e^2))(2\pi n/a)^{a/2}(2n/a)^n(a/e)^a.$$

Using the inequality $3 \leq a \leq \sqrt{n}$ we obtain:

$$(n-1)^{1/2}(n-3)^{n-2} \geq (2/4e^2)(2\pi n/3)^{\sqrt{n}/2}(2n/3)^n(\sqrt{n}/e)^{\sqrt{n}}.$$

Take logarithms and divide by n, obtaining

$$(1/2n)\log(n-1) + ((n-2)/n)\log(n-3) \geq (1/n)\log(2/4e^2) + (1/2\sqrt{n})\log(2\pi/3) +$$
$$+ (1/2\sqrt{n})\log(n) + \log(2n/3) + (1/\sqrt{n})\log(\sqrt{n}/e).$$

Since $\sqrt{n-1} \geq 2/4e^2$ and $(1/2\sqrt{n})\log(2\pi/3) \leq 1/\sqrt{n}$ we are reduced to show that

$$\log(n-3) \geq (2/n)\log(n-3) + (1/\sqrt{n})\log(n) + \log(2n/3).$$

Since $n \geq 300$ we have that $(2/n)\log(n-3) + (1/\sqrt{n})\log(n) < 0.37$, hence it suffices to show that $\log(n-3) \geq 0.37 + \log(2n/3)$, i.e. $n-3 \geq (2/3)e^{0.37} \cdot n$. This is true since $(2/3)e^{0.37} < 0.97$. $\square$

Corollary 2.56. *Let $n \geq 11$ be odd. Then the order of an intransitive maximal subgroup of* $\mathrm{Sym}(n)$ *(resp.* $\mathrm{Alt}(n)$*) is bigger than the order of any transitive maximal subgroup of* $\mathrm{Sym}(n)$ *(resp.* $\mathrm{Alt}(n)$*) different from* $\mathrm{Alt}(n)$.

Proof. The imprimitive case follows from Lemma 2.55 noticing that $((n+1)/2)!((n-1)/2)! \geq ((n-1)/2)!((n-3)/2)!$, and if $n = 15$ then $((n+1)/2)!((n-1)/2)! \geq (n/a)!^a a!$ for $a \in \{3,5\}$. By [**MarS**] the order of a primitive maximal subgroup of $\mathrm{Alt}(n)$ or $\mathrm{Sym}(n)$ not containing $\mathrm{Alt}(n)$ is at most 2.6^n and $((n+1)/2)!((n-1)/2)! \geq 2.6^n$. $\square$

In what follows we will use when convenient the following argument. Suppose we want to prove an inequality of the type $\sum_{i=1}^k a_i^m \leq b^m$, where $a_1,\dots,a_k,b$ are positive integers. If this is true for a particular m then it is true for every m larger. Indeed, setting $a := \max\{a_1,\dots,a_k\}$, we have $\sum_{i=1}^k a_i^{m+1} = \sum_{i=1}^k a_i a_i^m \leq a\sum_{i=1}^k a_i^m \leq ab^m \leq b^{m+1}$.

Lemma 2.57. *Let $n \geq 14$ be odd and let $m \geq 3$, $m \neq 4$. Let r be the smallest prime divisor of m. Then*

$$\sum_{k=1}^{(n-1)/2} \binom{n}{k}^m \leq (n!/2)^{m-m/r-1}.$$

Proof. The result is true by inspection for $n \geq 14$ and $m = 3$, and for $n \geq 5$ and $m = 5$. Suppose $m \geq 6$. The result is true by inspection for $14 \leq n \leq 28$. Assume that $n \geq 29$. It is enough to prove that $\frac{n-1}{2}\binom{n}{(n-1)/2}^m \leq (n!/2)^{m/2-1}$. Since $n \geq 29$, $n!/2 \geq 2^{7n/2}$ and it is enough to show that $2^{nm+n} \leq 2^{(7n/2)(m/2-1)}$, i.e. $nm+n \leq 7nm/4 - 7n/2$, i.e. $m \geq 6$. $\square$

Lemma 2.58. *If $1 \leq k \leq n$ then* $\sum_{i=1}^k \binom{n}{i}^m \leq \frac{\binom{n}{k}^m}{1-(k/(n-k+1))^m}$.

PROOF. Note that

$$\frac{\binom{n}{k}^m + \binom{n}{k-1}^m + \binom{n}{k-2}^m + \cdots}{\binom{n}{k}^m} = 1 + \left(\frac{k}{n-k+1}\right)^m + \left(\frac{k(k-1)}{(n-k+1)(n-k+2)}\right)^m + \cdots$$

and we can bound the right-hand side from above by the geometric series

$$1 + \left(\frac{k}{n-k+1}\right)^m + \left(\frac{k}{n-k+1}\right)^{2m} + \cdots = \frac{1}{1 - \left(\frac{k}{n-k+1}\right)^m}.$$

The result follows. □

LEMMA 2.59. *If $m \geq 2$ and either $n \in \{8, 11, 13, 14\}$ or $n \geq 16$ then*

$$2^{m-1} + \sum_{i=1}^{[n/3]} \binom{n}{i}^m < \left(\frac{1}{2}\binom{n}{[n/2]}\right)^m.$$

PROOF. The lemma is easily seen to be true for $n \leq 23$. Suppose $n \geq 24$. Using Lemma 2.58 we see that it is enough to show that

$$2 + \binom{n}{[n/3]}^2 \frac{1}{1 - \left(\frac{[n/3]}{[2n/3]+1}\right)^2} < \left(\frac{1}{2}\binom{n}{[n/2]}\right)^2, \tag{3}$$

and this is true if $2 + (4/3)\binom{n}{[n/3]}^2 < \left(\frac{1}{2}\binom{n}{n/2}\right)^2$. It is clearly enough to show that $8\binom{n}{[n/3]}^2 \leq \binom{n}{[n/2]}^2$. It is easy to see that if $n \geq 9$ then $\binom{n}{[n/3]+1} \geq (3/2)\binom{n}{[n/3]}$, so that if $0 \leq i \leq [n/2] - [n/3]$ then $\binom{n}{[n/3]+i} \geq (3/2)^i \binom{n}{[n/3]}$. Since $n \geq 24$ we have $8(2/3)^6 \leq 1$ and $[n/3] + 3 \leq [n/2]$. Therefore

$$8\binom{n}{[n/3]}^2 \leq 8(2/3)^6 \binom{n}{[n/3]+i}^2 \leq \binom{n}{[n/2]}^2.$$

□

LEMMA 2.60. *Let p be a prime divisor of n such that $3 \leq p \leq \sqrt[4]{n}$, and let r be the smallest prime divisor of m. If $m \geq 3$ and $m \neq 4$ then $\left(\frac{1}{2}(n/p)!^p p!\right)^m \geq (m/2)(n!/2)^{m/r+1}$ for every $n \geq 5$.*

PROOF. Since $p \geq 3$, $(p!/2)^m \geq m/2$ so it is enough to show that

$$1 \leq \frac{((n/p)!)^{pm}}{(n!/2)^{1+m/r}}.$$

Substituting Stirling's formula on the right-hand side, we see that it is sufficient to show that

$$1 \leq \frac{(2\pi(n/p))^{pm/2}(n/pe)^{mn}}{\sqrt{2\pi n}^{1+m/r}(n/e)^{n(1+m/r)} e^{(1+m/r)/(12n)} 2^{-1-m/r}}.$$

Since $n \geq 5$, $(2/e^{1/12n}) \geq 1.9$ and it is enough to show that

$$1 \le \frac{(2\pi(n/p))^{pm/2}(n/pe)^{mn}}{(2\pi n/(1.9)^2)^{(1/2)(1+m/r)}(n/e)^{n(1+m/r)}}. \tag{4}$$

Suppose first $m \ge 6$. Since $3 \le p \le \sqrt[4]{n}$ and $r \ge 2$, $m \ge 6$, raising to the power $1/m$ we see that it is sufficient to prove

$$1 \le \frac{(2\pi n^{3/4})^{3/2}(n^{3/4}/e)^n}{(2\pi n/(1.9)^2)^{(1/2)(1/6+1/2)}(n/e)^{n(1/6+1/2)}}.$$

Re-arranging terms we obtain

$$\frac{(2\pi/(1.9)^2)^{(1/2)(1/2+1/6)}}{(2\pi)^{3/2}} \le \frac{n^{n/4+9/8-(1/2)(1/6+1/2)}(e/n)^{n/6}}{e^{n/2}}.$$

This is true for every $n \ge 1$.
Suppose now $r \ge 3$. Starting from inequality (4), using $3 \le p \le \sqrt[4]{n}$ and $r \ge 3$, $m \ge 3$ we are reduced to prove that

$$1 \le \frac{(2\pi n^{3/4})^{3/2}(n^{3/4}/e)^n}{(2\pi n/(1.9)^2)^{(1/2)(1/3+1/3)}(n/e)^{n(1/3+1/3)}}.$$

Re-arranging terms we obtain

$$\frac{(2\pi/(1.9)^2)^{1/3}}{(2\pi)^{3/2}} \le n^{n/12+9/8-1/3}e^{-n/3}.$$

This is true for every $n \ge 1$. □

LEMMA 2.61. *If $n \ge 19$ is odd and p is an odd prime divisor of n then* $3\binom{n}{[n/3]}^m \le \left(\frac{n!}{(n/p)!^p p!}\right)^m$.

PROOF. The lemma is true for $19 \le n \le 23$ by inspection. Suppose $n \ge 24$. By Corollary 2.56 we are reduced to show that $3\binom{n}{[n/3]} \le \binom{n}{[n/2]}$. It is easy to see that if $n \ge 9$ then $\binom{n}{[n/3]+1} \ge (3/2)\binom{n}{[n/3]}$, so that if $0 \le i \le [n/2]-[n/3]$ then $\binom{n}{[n/3]+i} \ge (3/2)^i\binom{n}{[n/3]}$. Since $n \ge 24$ we have $[n/3]+3 \le [n/2]$. Therefore

$$3\binom{n}{[n/3]} \le 3(2/3)^3\binom{n}{[n/3]+3} \le \binom{n}{[n/2]}.$$

□

LEMMA 2.62. *Let n be even and let a be the smallest divisor of n larger than 2. If $n > 10$, then*

$$n((n/a)!)^a a! \le 2((n/2)!)^2.$$

PROOF. If $n = 2a$, then we must consider the inequality $2^a \le (a-1)!$. This is clearly true if a satisfies $a > 5$, hence if $n > 10$. This means that we may assume that $3 \le a \le n/4$.
The lemma is true for $10 < n \le 28$ by inspection. From now on we assume that $n \ge 30$.
Applying Stirling's formula we see that it is sufficient to verify the inequality

$$n(\sqrt{2\pi(n/a)})^a(n/ae)^n e^{a^2/(12n)}\sqrt{2\pi a}(a/e)^a e^{1/(12a)} \le 2\pi n(n/2e)^n e^{2/(6n+1)}.$$

After rearranging factors we obtain

$$2^n (2\pi(n/a))^{a/2} e^{a^2/(12n)} \sqrt{2\pi a}(a/e)^a e^{1/(12a)} \leq a^n 2\pi e^{2/(6n+1)}.$$

After taking natural logarithms and rearranging terms we obtain

$$a\Big(\frac{\ln(2\pi)}{2} + \frac{\ln n}{2} + \frac{\ln a}{2} + \frac{a}{12n} - 1\Big) + \Big(\frac{\ln a}{2} + \frac{1}{12a} - \frac{\ln(2\pi)}{2} - \frac{2}{6n+1}\Big) \leq n(\ln a - \ln 2).$$

By the assumption $3 \leq a \leq n/4$ and by dividing both sides of the previous inequality by $\ln n$ we see that it is sufficient to prove

$$a\Big(1 + \frac{\ln(2\pi)}{2\ln n} + \frac{1}{48\ln n} - \frac{1}{\ln n}\Big) + \Big(\frac{1}{2} + \frac{1}{36\ln n} - \frac{\ln(2\pi)}{2\ln n} - \frac{2}{(6n+1)\ln n}\Big) \leq \frac{n}{\ln n}(\ln a - \ln 2).$$

Since

$$\frac{\ln(2\pi)}{2\ln n} + \frac{1}{48\ln n} - \frac{1}{\ln n} < 0$$

and

$$\frac{1}{36\ln n} - \frac{\ln(2\pi)}{2\ln n} - \frac{2}{(6n+1)\ln n} < 0,$$

it is sufficient to prove

$$\frac{a+0.5}{\ln a - \ln 2} \leq \frac{n}{\ln n}. \tag{5}$$

This is true for $a = 3$, 4, and 5 (provided that $n \geq 30$). Hence assume that $7 \leq a \leq n/4$. The function $\frac{x+0.5}{\ln x - \ln 2}$ increases when $x > 6$, hence it is sufficient to show inequality (5) in case of the substitution $a = n/4$. But that holds for $n \geq 30$. The proof of the lemma is now complete. $\square$

LEMMA 2.63. *Let n be even and let a be the smallest divisor of n larger than 2. Let $m \geq 2$. Then for $n > 10$ we have the following.*

(1) *If n is divisible by 4, then*

$$\Big(\frac{((n/a)!)^a a!}{2}\Big)^m \leq (((n/2)-2)!)((n/2)!)\Big(\frac{(((n/2)-1)!)(((n/2)+1)!)}{2}\Big)^{m-1}.$$

(2) *If n is congruent to 2 modulo 4, then*

$$\Big(\frac{((n/a)!)^a a!}{2}\Big)^m \leq (1/2^{m-1})(((n/2)-1)!)^2((n/2)!)^{2m-2}.$$

PROOF. By Lemma 2.62 it is sufficient to show that both displayed inequalities follow from the inequality

$$n((n/a)!)^a a! \leq 2((n/2)!)^2.$$

Indeed, the first displayed inequality becomes

$$\Big(\frac{((n/a)!)^a a!}{2}\Big)^m \leq \frac{8}{n^2-4}\Big(\frac{(((n/2)-1)!)(((n/2)+1)!)}{2}\Big)^m.$$

Since $2/n \leq (8/(n^2-4))^{1/2} \leq (8/(n^2-4))^{1/m}$, it is sufficient to see that

$$(n/2)((n/a)!)^a a! \leq ((n/2)-1)!((n/2)+1)!.$$

But this proves the first part of the lemma since

$$((n/2)!)^2 < ((n/2)-1)!((n/2)+1)!.$$

After rearranging the factors in the second displayed inequality of the statement of the lemma, we obtain

$$\Big(((n/a)!)^a a!\Big)^m \leq (8/n^2)(n/2)!^{2m}.$$

By similar considerations as in the previous paragraph, we see that this latter inequality follows from the inequality $n((n/a)!)^a a! \leq 2((n/2)!)^2$. □

The following lemma is easy to prove.

Lemma 2.64. *For $n > 12$ and $m \geq 2$ we have the following.*

(1) *If n is divisible by 4, then*

$$2.6^{nm} \leq (((n/2)-2)!)((n/2)!)\Big(\frac{(((n/2)-1)!)(((n/2)+1)!)}{2}\Big)^{m-1}.$$

(2) *If n is congruent to 2 modulo 4, then*

$$2.6^{nm} \leq (1/2^{m-1})(((n/2)-1)!)^2((n/2)!)^{2m-2}.$$

Lemma 2.65. *$(n/2)!^4 \geq n!^{3/2}$ for every $n \geq 32$ even.*

Proof. The result is true by inspection for $32 \leq n \leq 42$. Suppose $n \geq 44$. Applying Stirling formula we see that it is enough to show that $(n/2e)^{2n}(\pi n)^2 \geq 2^{3/2}(n/e)^{3n/2}(2\pi n)^{3/4}$. Since $n \geq 2$ we have $(\pi n)^2 \geq 2^{3/2}(2\pi n)^{3/4}$, so we are reduced to show that $(n/2e)^{n/2} \geq 2^{3n/2} = 8^{n/2}$, i.e. $n/2e \geq 8$, i.e. $n \geq 44$. □

Lemma 2.66. *Let $m \geq 2$. The following hold.*

(1) *Let n be divisible by 4 and larger than 8. Then*

$$m(n!/2)^{m/2} \leq (((n/2)-2)!)((n/2)!)\Big(\frac{(((n/2)-1)!)(((n/2)+1)!)}{2}\Big)^{m-1}.$$

(2) *Let n be congruent to 2 modulo 4 and larger than 10. Then*

$$m(n!/2)^{m/2} \leq (1/2^{m-1})(((n/2)-1)!)^2((n/2)!)^{2m-2}.$$

Proof. (1) After rearranging the inequality and taking roots we obtain

$$m^{2/m}(n!/2) \leq \Big(\frac{8}{n^2-4}\Big)^{2/m}\Big(\frac{((n/2)-1)!((n/2)+1)!}{2}\Big)^2.$$

Since $m^{2/m} \leq 4$ and $8/(n^2-4) \leq (8/(n^2-4))^{2/m}$, it is sufficient to see that

$$(n^2-4)n! \leq (((n/2)-1)!((n/2)+1)!)^2.$$

Since $\binom{n}{(n/2)-1} \leq 2^{n-1}$, it is sufficient to prove

$$(n^2-4)2^{n-1} \leq ((n/2)-1)!((n/2)+1)!.$$

But this is true for $n \geq 12$.
(2) After rearranging the inequality and taking roots we see that it is sufficient to show

$$4m^{2/m}(n/2)^{4/m}(n!/2) \leq ((n/2)!)^4.$$

Since $(m/2)^{2/m} \leq 2$ and $(n/2)^{4/m} \leq (n/2)^2$, it is sufficient to see that

$$n^2 n! \leq ((n/2)!)^4.$$

Using Lemma 2.65 we see that this is true if $n \geq 10$. □

Lemma 2.67. *Let r be the smallest prime divisor of m. If $n \geq 20$ is even and $m \geq 3$, $m \neq 4$ then $(n/4+1)\binom{n}{n/2}^m \leq (n!/2)^{m-m/r-1}$.*

Proof. Suppose first that $m \neq 3$. Since $r \geq 2$ it is enough to show that $(n/4+1)\binom{n}{n/2}^m \leq (n!/2)^{m/2-1}$. Re-arranging terms we obtain $(n/4+1)(n!/2) \leq ((n/2)!^4/(2n!))^{m/2}$. By Lemma 2.65 if $n \geq 32$ it is enough to show that $(n!/4)^{m/4-1} \geq 2(n/4+1)$, which is true as $m/4-1>0$. The case $20 \leq n \leq 30$ is easily dealt with.
Suppose now $m=3$. We obtain $(n/4+1)\binom{n}{n/2}^3 \leq (n!/2)$. This is true by inspection for $18 \leq n \leq 30$. If $n \geq 32$ then using Lemma 2.65 as above we are reduced to prove that $n/2+2 \leq n!^{1/4}$. This is true for $n \geq 6$. □

6.2. Case I: n odd, $X = \mathrm{Sym}(n)$. Suppose that n is odd and $X = \mathrm{Sym}(n)$.
Let Π be the set consisting of the $(k, n-k)$-cycles of $\mathrm{Sym}(n)$ where $1 \leq k \leq n-1$, let $\mathcal{M}$ be the family of the maximal intransitive subgroups of $\mathrm{Alt}(n)$ and let $\mathcal{J} = \emptyset$. Let A be the set of the $(2, n-2)$-cycles of $\mathrm{Sym}(n)$, let B be the set of the $(n-1)$-cycles of $\mathrm{Sym}(n)$, and for m odd let C be the set of n-cycles of $\mathrm{Alt}(n)$, for m even let $C = \emptyset$. It is easy to show that conditions (1), (2), (3) of Theorem 2.32 and conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled.
Condition (6) of Theorem 2.32 follows from Proposition 2.51.
By Lemma 2.57, condition (5) of Theorem 2.42 is fulfilled if $m \geq 3$, $m \neq 4$ and $n \geq 15$ is odd.

Claim 2.68. *Condition (4)(i) of Theorem 2.32 and condition (6) of Theorem 2.42 are fulfilled if $n \geq 11$ is odd and $m \geq 1$.*

Suppose $n \geq 11$, and take $M \in \mathcal{M}$, K a subgroup of $\mathrm{Alt}(n)$ outside $\mathcal{M}$ such that $N_{\mathrm{Sym}(n)}(K)$ is a maximal subgroup of $\mathrm{Sym}(n)$ supplementing $\mathrm{Alt}(n)$. Then $|M| \geq |K|$ by Corollary 2.56, and the inequality $|N_{\mathrm{Sym}(n)}(M) \cap \Pi| \geq |N_{\mathrm{Sym}(n)}(K) \cap (\Pi \cup C)|$ is proved in [**MarS**, Claim 3.2].

Claim 2.69. *Condition (4)(ii) of Theorem 2.32 and condition (7) of Theorem 2.42 are fulfilled if $n \geq 11$ is odd and $m \geq 2$.*

If $M \in \mathcal{M}$ is the stabilizer of a subset of $\{1, \ldots, m\}$ of size k then $|N_X(M) \cap \Pi| = (k-1)!(n-k-1)!$, so we have to prove that

$$(\frac{1}{2}(\frac{n-1}{2})!(\frac{n+1}{2})!)^{m-1}(\frac{n-1}{2}-1)!(\frac{n+1}{2}-1)! \geq 2m(n!/2)^{m/r}.$$

In other words

$$\frac{8}{n^2-1}\left(\frac{1}{2}\left(\frac{n-1}{2}\right)!\left(\frac{n+1}{2}\right)!\right)^m \geq 2m \cdot (n!/2)^{m/r}. \tag{6}$$

Suppose that $n \geq 15$. Let $M < \mathrm{Alt}(n)$ be the stabilizer of a proper non-empty subset of $\{1, \ldots, m\}$. Then $|M|^{3/2} \geq |\mathrm{Alt}(n)|$ for every $M \in \mathcal{M}$ by Lemma 2.53, so we are reduced to prove that $(8/(n^2-1))|\mathrm{Alt}(n)|^{\frac{2}{3}m} \geq 2m \cdot |\mathrm{Alt}(n)|^{m/2}$, i.e. $|\mathrm{Alt}(n)|^{m/6} \geq (m/4)(n^2-1)$. This is clearly true for every $m \geq 2$ since $n \geq 15$. If $n = 11$ then $|M| \geq \frac{1}{2}5!6! = 43200$ and (6) is true for $m \geq 2$. If $n = 13$ then $|M| \geq \frac{1}{2}6!7! = 1814400$ and (6) is true for $m \geq 2$.
Let us deal with condition (8) of Theorem 2.32.

Claim 2.70. *Condition (8) of Theorem 2.32 is fulfilled if $n \geq 7$ is odd and $m \geq 2$.*

Let V be a maximal subgroup of $\mathrm{Sym}(n)$ supplementing $\mathrm{Alt}(n)$ and such that $V \cap \mathrm{Alt}(n) \notin \mathcal{M}$. Condition (8) of Theorem 2.32 translates as follows:

$$\frac{2|\mathrm{Alt}(n)|^m}{(n-1)(n-2)} \geq \max\{|V \cap \mathrm{Alt}(n)|^{m-1} \cdot (|V \cap \Pi| + |V \cap C|), 2m \cdot |\mathrm{Alt}(n)|^{m/r}\}.$$

The inequality $\frac{2|\mathrm{Alt}(n)|^m}{(n-1)(n-2)} \geq 2m \cdot |\mathrm{Alt}(n)|^{m/r}$ is clearly true for $m \geq 2$ and $n \geq 5$. The inequality

$$\frac{2|\mathrm{Alt}(n)|^m}{(n-1)(n-2)} \geq |V \cap \mathrm{Alt}(n)|^{m-1} \cdot (|V \cap \Pi| + |V \cap C|)$$

is easily seen to be true if $n \in \{7, 9\}$. Suppose $n \geq 11$. It suffices to show that $\frac{2}{(n-1)(n-2)}|\mathrm{Alt}(n)|^m \geq 2|R|^m$ for any maximal transitive subgroup R of $\mathrm{Sym}(n)$ different from $\mathrm{Alt}(n)$, i.e. $(|\mathrm{Sym}(n) : R|/2)^m \geq (n-1)(n-2)$, and this is true by Corollary 2.56, being true for $m = 1$: $|\mathrm{Sym}(n) : R|/2 \geq \binom{n}{5}/2 > (n-1)(n-2)$ since $n > 8$.

6.3. Case II: n even, $X = \mathrm{Sym}(n)$. Suppose that $n \geq 32$ is even and $X = \mathrm{Sym}(n)$. Let Π be the set of the n-cycles in $\mathrm{Sym}(n)$, let $\mathcal{M}$ be the family of the maximal imprimitive subgroups of $\mathrm{Alt}(n)$ corresponding to the partitions given by two subsets of $\{1, \ldots, n\}$ of size $n/2$. Set $C = \emptyset$. Let $\mathcal{J}$ be the family of the maximal intransitive subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(i) \times \mathrm{Sym}(n-i)) \cap \mathrm{Alt}(n)$ where $i \in \{1, \ldots, [n/3]\}$. It is easy to see that conditions (1), (2), (3) of Theorem 2.32 and conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled.
In [**MarP**] it is shown that the order of a primitive subgroup of $\mathrm{Sym}(n)$ not containing $\mathrm{Alt}(n)$ is at most 2.6^n. This together with Lemma 2.54 implies that if $n \geq 8$ then the order of any member of $\mathcal{M}$ is larger than the order of any subgroup of $\mathrm{Alt}(n)$ of the form $K \cap \mathrm{Alt}(n)$ where K is a maximal subgroup of $\mathrm{Sym}(n)$ whose intersection with Π is non-empty. Indeed $(n/2)!^2 \geq 2.6^n$ if $n \geq 10$, and all the maximal subgroups of $\mathrm{Alt}(8)$ whose normalizer in $\mathrm{Sym}(8)$ intersects Π non-trivially belong to $\mathcal{M}$. In [**MarS**, Claims 3.3, 3.4] it is proved that $|N_{\mathrm{Sym}(n)}(M) \cap \Pi| \geq |K \cap \Pi|$ for every $M \in \mathcal{M}$ and every maximal subgroup K of $\mathrm{Sym}(n)$ such that $K \cap \mathrm{Alt}(n) \notin \mathcal{M}$. This implies that condition (4)(i) of Theorem 2.32 and condition (6) of Theorem 2.42 are fulfilled for $n \geq 8$ and $m \geq 1$.

Let us deal with condition (4)(ii) of Theorem 2.32 and condition (7) of Theorem 2.42. It is easy to see that they are fulfilled if $n \in \{8, 10\}$. Suppose $n \geq 12$. By Lemma 2.53 $|M|^{3/2} \geq |\mathrm{Alt}(n)|$ for every $M \in \mathcal{M}$. Therefore it suffices to prove that

$$|\mathrm{Alt}(n)|^{(2/3)(m-1)} \cdot |N_{\mathrm{Sym}(n)}(M) \cap \Pi| \geq 2m \cdot |\mathrm{Alt}(n)|^{m/2}.$$

This is true for $m = 3$ and every $m \geq 5$ (being true for $m = 5$, since $|N_{\mathrm{Sym}(n)}(M) \cap \Pi| \geq 10$). Observe that if $m \in \{2, 4\}$ then condition (4)(iii) of Theorem 2.32 is trivially fulfilled (since n is even, the n-cycles are odd permutations, so they do not admit square roots in $\mathrm{Sym}(n)$). Lemma 2.59 implies that if $n \geq 14$ and $m \geq 2$ then condition (8) of Theorem 2.42 is fulfilled. Condition (5) of Theorem 2.42 is then implied by the following inequality if $n \geq 14$ and $m \geq 2$:

$$2\left(\frac{1}{2}\binom{n}{n/2}\right)^m \leq (n!/2)^{m-m/r-1}. \tag{7}$$

Using $r \geq 2$ we are reduced to

$$2(n!/2) \leq \left(\frac{n!/2}{\frac{1}{4}\binom{n}{n/2}^2}\right)^{m/2} = (2(n/2)!^4/n!)^{m/2}.$$

If $n = 30$ then this is true for every $m \geq 4$. If $n \geq 32$ then by Lemma 2.65 it suffices that $m/2 \geq 2$, i.e. $m \geq 4$. If $m = 3$ then inequality (7) becomes

$$2\left(\frac{1}{2}\binom{n}{n/2}\right)^3 \leq n!/2,$$

in other words $n!^2 \leq 2(n/2)!^6$. This is true by inspection for $12 \leq n \leq 30$. If $n \geq 32$ then using Lemma 2.65 we are reduced to $n!^2 \leq 2n!^{9/4}$, which is true.

6.4. Case III: n odd, $p \leq \sqrt[4]{n}$, $X = \mathrm{Alt}(n)$. Suppose that $n \geq 5$ is odd, with smallest prime divisor p at most $\sqrt[4]{n}$ and $X = \mathrm{Alt}(n)$.

Let Π be the set of n-cycles in $\mathrm{Alt}(n)$, and let $\mathcal{M}$ be the set consisting of the intransitive maximal subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(n/p) \wr \mathrm{Sym}(p)) \cap \mathrm{Alt}(n)$. Let $C = \emptyset$. Let $\mathcal{J}$ be the family of intransitive maximal subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(i) \times \mathrm{Sym}(n-i)) \cap \mathrm{Alt}(n)$ for $i \in \{1, \ldots, [n/3]\}$. It is easy to see that conditions (1), (2), (3) of Theorem 2.32 and conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled.

Condition (4)(i) of Theorem 2.32 and condition (6) of Theorem 2.42 translate as follows:

$$\frac{2}{n}\left(\frac{1}{2}(n/p)!^p p!\right)^m \geq \max\{2.6^{nm}, \frac{2}{n}\left(\frac{1}{2}(n/r)!^r r!\right)^m\},$$

where r is a prime divisor of n different from p. This follows from Lemma 2.54 if $n \geq 8$.

Condition (4)(ii) of Theorem 2.32 and condition (7) of Theorem 2.42 translate as follows:

$$\frac{2}{n}\left(\frac{1}{2}(n/p)!^p p!\right)^m \geq m(n!/2)^{m/2}.$$

This is implied by Lemma 2.60 if $n \geq 5$, $m \geq 3$ and $m \neq 4$.
Condition (8) of Theorem 2.42 translates as follows:

$$2^{m-1} + \sum_{i=1}^{[n/3]} \binom{n}{i}^m < \left(\frac{n!}{(n/p)!^p p!}\right)^m.$$

By Lemma 2.58 and Lemma 2.61 this is true if $m \geq 1$ and $n \geq 19$.
Condition (5) of Theorem 2.42 translates as follows:

$$\sum_{i=1}^{[n/3]} \binom{n}{i}^m + \left(\frac{n!}{(n/p)!^p p!}\right)^m \leq (n!/2)^{m/2-1}.$$

Given condition (8), this is implied by

$$2\left(\frac{n!}{(n/p)!^p p!}\right)^m \leq (n!/2)^{m/2-1}.$$

This is implied by Lemma 2.60 if $n \geq 5$ and $m \geq 3$, $m \neq 4$.

6.5. Case IV: n even, $X = \mathrm{Alt}(n)$. Suppose that n is even and $X = \mathrm{Alt}(n)$. Let $C = \emptyset$. Suppose n is divisible by 4. Let Π be the set of all $(i, n-i)$-cycles of $\mathrm{Alt}(n)$ for all odd i with $i < n/2$ and let $\mathcal{M}$ be the set of all maximal subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(i) \times \mathrm{Sym}(n-i)) \cap \mathrm{Alt}(n)$ for all odd i with $i < n/2$. Let $\mathcal{J}$ be the family of maximal imprimitive subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(n/2) \wr \mathrm{Sym}(2)) \cap \mathrm{Alt}(n)$. It is easy to see that conditions (1), (2), (3) of Theorem 2.32 and conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled.
Lemmas 2.63 and 2.64 imply that if $n > 12$ is divisible by 4 and $m \geq 2$ then condition (4)(i) of Theorem 2.32 and condition (6) of Theorem 2.42 are fulfilled.
Lemma 2.66 implies that if $n > 8$ is divisible by 4 and $m \geq 2$ then condition (4)(ii) of Theorem 2.32 and condition (7) of Theorem 2.42 are fulfilled.
Let us deal with condition (8) of Theorem 2.42. It translates as follows:

$$2^{m-1} + \left(\frac{1}{2}\binom{n}{n/2}\right)^m < \sum_{i=1 \ odd}^{n/2-1} \binom{n}{i}^m.$$

It is implied by the inequality $\frac{1}{2}\binom{n}{n/2} < \binom{n}{n/2-1}$, true for $n \geq 4$.
Condition (5) of Theorem 2.42 translates as follows:

$$\left(\frac{1}{2}\binom{n}{n/2}\right)^m + \sum_{i=1 \ odd}^{n/2-1} \binom{n}{i}^m \leq (n!/2)^{m-m/r-1}.$$

It is therefore implied by Lemma 2.67 if $n \geq 20$ and $m \geq 3$, $m \neq 4$.
Suppose $6 < n \equiv 2 \mod (4)$. Let ℓ be a prime not dividing n such that $\ell \leq n-3$ (cfr. Proposition 2.51). Let Π be the set of all $(i, n-i)$-cycles of $\mathrm{Alt}(n)$ for all odd i with $i \leq n/2$, let A be the set of all $(n-1)$-cycles of $\mathrm{Alt}(n)$, let B be the set of all $(\ell, n-\ell)$-cycles of $\mathrm{Alt}(n)$, let $C = \emptyset$ and let $\mathcal{M}$ be

the set of all maximal subgroups of $\mathrm{Alt}(n)$ conjugate to $(\mathrm{Sym}(i) \times \mathrm{Sym}(n-i)) \cap \mathrm{Alt}(n)$ for some i odd with $i < n/2$ or conjugate to $(\mathrm{Sym}(n/2) \wr \mathrm{Sym}(2)) \cap \mathrm{Alt}(n)$. Let $\mathcal{J} = \emptyset$. It is easy to see that conditions (1), (2), (3), (5), (6), (7) of Theorem 2.32 and conditions (1), (2), (3), (4) of Theorem 2.42 are fulfilled. Note that the quantity

$$(1/2^{m-1})(((n/2)-1)!)^2((n/2)!)^{2m-2}$$

is a lower bound of the left-hand sides of condition (4) of Theorem 2.32. Thus Lemmas 2.63, 2.64 and 2.66 imply that condition (4) of Theorem 2.32 and conditions (6) and (7) of Theorem 2.42 are fulfilled if $m \geq 2$ and $n \geq 14$ is congruent to 2 modulo 4.
Condition (8) of Theorem 2.32 translates as follows:

$$\frac{4}{\ell(n-\ell)(n-1)}|\mathrm{Alt}(n)|^m \geq \max\{2.6^{nm}, (\frac{1}{2}(n/a)!^a a!)^m, m|\mathrm{Alt}(n)|^{m/r}\},$$

where a is the smallest odd divisor of n. Observe that $\ell(n-\ell) \leq (n/2)^2$. Therefore Lemmas 2.63, 2.64 and 2.66 imply that Condition (8) of Theorem 2.32 is implied by the following inequality if $m \geq 2$ and $n \geq 14$ is congruent to 2 modulo 4.

$$(1/2^{m-1})(((n/2)-1)!)^2((n/2)!)^{2m-2} \leq \frac{4}{(n/2)^2(n-1)}|\mathrm{Alt}(n)|^m.$$

It re-writes as follows:

$$(n/2)!^{2m} \leq \frac{2n!^m}{n-1}.$$

This is implied by $\binom{n}{n/2}^m \geq (n-1)/2$, true for $m \geq 1$ and $n \geq 2$.
Condition (5) of Theorem 2.42 translates as follows:

$$\sum_{\substack{i=1 \\ i \text{ odd}}}^{(n/2)-2} \binom{n}{i}^m + \left(\frac{1}{2}\binom{n}{n/2}\right)^m \leq (n!/2)^{m-m/r-1}.$$

This is implied by Lemma 2.67 if $n \geq 20$ and $m \geq 3$, $m \neq 4$.

7. $\sigma(\mathrm{Alt}(5) \wr C_2) = 57$

We conclude this chapter with a computation which appears to need arguments which are essentially different from those we have used so far. We prove that

Theorem 2.71. *$\sigma(\mathrm{Alt}(5) \wr C_2) = 1 + 6 \cdot 6 + 4 \cdot 5 = 57$.*

The meaning of the displayed sum is the following: $\sigma(\mathrm{Alt}(5) \wr C_2)$ is realized by the upper bound of Proposition 2.29 obtained considering the covering of $\mathrm{Alt}(5)$ consisting of the six normalizers of the Sylow 5-subgroups and four point stabilizers.
Let $G := \mathrm{Alt}(5) \wr C_2$, the semidirect product $(\mathrm{Alt}(5) \times \mathrm{Alt}(5)) \rtimes \langle \varepsilon \rangle$ where ε, of order 2, acts on $\mathrm{Alt}(5) \times \mathrm{Alt}(5)$ by exchanging the two variables. Recall that the maximal subgroups of G are of the following five types:

- The socle $N = \mathrm{Alt}(5) \times \mathrm{Alt}(5)$.

- Type 'r': $N_G(M \times M^l)$ where $l \in \mathrm{Alt}(5)$ and M is a point stabilizer.
- Type 's': $N_G(M \times M^l)$ where $l \in \mathrm{Alt}(5)$ and M is the normalizer of a Sylow 5-subgroup.
- Type 't': $N_G(M \times M^l)$ where $l \in \mathrm{Alt}(5)$ and M is an intransitive subgroup of type $(3, 2)$.
- Type 'd': $N_G(\Delta_\alpha)$ where $\alpha \in \mathrm{Sym}(5)$ and $\Delta_\alpha := \{(x, x^\alpha) \mid x \in \mathrm{Alt}(5)\}$.

Recall that:

- $N \cap N_G(H) = H$ for every H of the type $M \times M^l$ or Δ_α with M a maximal subgroup of $\mathrm{Alt}(5)$.
- The element $(x, y)\varepsilon$ belongs to $N_G(M \times M^l)$ if and only if $xl^{-1}, ly \in M$. In particular $xy \in M$.
- The element $(x, y)\varepsilon$ belongs to $N_G(\Delta_\alpha)$ if and only if $(\alpha y)^2 = xy$.

Let $\mathcal{M}$ be a family of proper subgroups of G which cover G.

Observation 2.72. *$N \in \mathcal{M}$*

Proof. Let $x \in \mathrm{Alt}(5)$ be a 5-cycle, and let $y \in \mathrm{Alt}(5)$ be a 3-cycle. Then the element (x, y) does not belong to any $N_G(M \times M^l)$ or $N_G(\Delta_\alpha)$ by the remarks above (no maximal subgroup of $\mathrm{Alt}(5)$ has order divisible by 3 and 5). $\square$

Call i the number of subgroups of type i in $\mathcal{M}$ for $i = r, s, t, d$.
The 'type' of an element $(x, y)\varepsilon \in G - N$ will be the cyclic structure of the element $xy \in \mathrm{Alt}(5)$.
The four possible cyclic structures will be denoted by 1, (3), (5), (2, 2).
The only maximal subgroups of G containing elements of type (3) are the ones of type r or t or d.
A subgroup of type r contains 96 elements of type (3). A subgroup of type t contains 12 elements of type (3). A subgroup of type d contains 20 elements of type (3). G contains 1200 elements of type (3). In particular $96r + 12t + 20d \geq 1200$, in other words

$$24r + 3t + 5d \geq 300. \tag{8}$$

The only maximal subgroups of G containing elements of type (5) are the ones of type s or d. A subgroup of type s contains 40 elements of type (5). A subgroup of type d contains 24 elements of type (5) if α is even, 0 if α is odd. G contains 1440 elements of type (5). In particular $40s + 24d \geq 1440$, in other words

$$5s + 3d \geq 180. \tag{9}$$

We know that G admits a cover which consists of 57 proper subgroups, with $s = 36$, $r = 20$, $t = d = 0$ (the 20 subgroups of type r are $N_G(M \times M^l)$ where $l \in \mathrm{Alt}(5)$ and $M = \mathrm{Stab}(i)$ for some $i \in \{1, 2, 3, 4\}$).
Suppose by contradiction that $\sigma(G) < 57$, and let $\mathcal{M}$ be a cover with 56 proper subgroups. In particular $r + s + t + d + 1 = 56$, i.e. $r + s + t + d = 55$.

Observation 2.73. *$d \leq 33$, $s \geq 17$ and $r \geq 6$.*

Proof. Inequality 9 re-writes as $s \geq 36 - \frac{3}{5}d$. Since $r + s + t + d = 55$, $r + t = 55 - s - d \leq 55 - 36 + \frac{3}{5}d - d = 19 - \frac{2}{5}d$. Combining this with inequality 8 we obtain $24(19 - \frac{2}{5}d) + 5d \geq 300$, i.e. $d \leq 156 \cdot 5/23$, i.e. $d \leq 33$. Therefore $s \geq 36 - \frac{3}{5}d = 36 - \frac{99}{5} > 16$.

Inequality 8 re-writes as $21r + 2d - 3s + 3(r + t + d + s) \geq 300$, i.e. $21r + 2d - 3s \geq 135$. Since $d \leq 33$ and $s \geq 17$, $21r \geq 135 + 3 \cdot 17 - 2 \cdot 33 = 120$, i.e. $r \geq 6$. $\square$

OBSERVATION 2.74. *$r + t + d \geq 20$ and $s < 36$.*

PROOF. Consider the following elements of $\mathrm{Alt}(5)$: $a_1 := (243) \in \mathrm{Stab}(1)$, $a_2 := (143) \in \mathrm{Stab}(2)$, $a_3 := (142) \in \mathrm{Stab}(3)$, $a_4 := (132) \in \mathrm{Stab}(4)$. Let $\mathcal{X}$ be the set of elements of G of the form $(x, y)\varepsilon$ with $xy = a_i$ for an $i \in \{1, 2, 3, 4\}$ and $x \in J_i$, where J_i is a fixed set of representatives of the right cosets of $\mathrm{Stab}(i)$, which will be specified later. Let $\mathcal{H}$ be the set of the 20 subgroups $N_G(M \times M^l)$ of G of type r with M the stabilizer of i for $i \in \{1, 2, 3, 4\}$. Notice that every element of $\mathcal{X}$ lies in exactly one element of $\mathcal{H}$. Now observe that if a subgroup $N_G(K \times K^l)$ of type t contains an element $(x, y)\varepsilon \in \mathcal{X}$ then K is determined by $a_i = xy$ - use this to label the K's as K_i for $i \in \{1, 2, 3, 4\}$ -, so that the only freedom is in the choice of the coset $K_i l$. We will choose the sets J_i in such a way that any two elements of J_i lie in different right cosets of K_i. This implies that for every subgroup $N_G(K \times K^l)$ of G of type t we have $|\mathcal{X} \cap N_G(K \times K^l)| \leq 1$. Let us choose the J_i's in such a way that for every subgroup $N_G(\Delta_\alpha)$ of type d we have $|\mathcal{X} \cap N_G(\Delta_\alpha)| \leq 1$. Choose:

$$\begin{aligned} J_1 &= \{(452), (12534), (13425), (14)(35), (23)(15)\}, \\ J_2 &= \{(134), (245), (123), (152), (125)\}, \\ J_3 &= \{(142), (132), (134), (153), (135)\}, \\ J_4 &= \{(132), (142), (243), (154), (145)\}. \end{aligned}$$

We have that for any $i = 1, 2, 3, 4$ any two elements of J_i lie in different right cosets of K_i. We have to check that every subgroup of the form $N_G(\Delta_\alpha)$ contains at most one element of $\mathcal{X}$. In other words we have to check that if $(x, y)\varepsilon \in \mathcal{X} \cap N_G(\Delta_\alpha)$ then $(x, y)\varepsilon$ is determined. We have $(\alpha y)^2 = xy$, so that if α is even then $\alpha = xyx$, if α is odd then $\alpha = \tau_{xy} xyx$, where τ_{xy} is the transposition whose support is pointwise fixed by xy. Let

$$P_i := \{xyx \mid xy = a_i,\ (x, y)\varepsilon \in \mathcal{X}\} \cup \{\tau_{xy} xyx \mid xy = a_i,\ (x, y)\varepsilon \in \mathcal{X}\} \subset \mathrm{Sym}(5)$$

for $i = 1, 2, 3, 4$. Clearly $|P_i| = 10$ for $i = 1, 2, 3, 4$. All we have to show is that the P_i's are pairwise disjoint. This follows from the computation:

$$\begin{aligned} P_1 = \{&(25)(34), (12)(35), (135), (14532), (15)(24), \\ &(125)(34), (1352), (35), (132)(45), (24)\}, \\ P_2 = \{&1, (15243), (14)(23), (14352), (14325), \\ &(25), (1543), (14)(253), (1435), (1432)\}, \\ P_3 = \{&(124), (14)(23), (234), (14253), (14235), \\ &(124)(35), (14)(235), (2354), (1425), (1423)\}, \\ P_4 = \{&(123), (13)(24), (12)(34), (13254), (13245), \\ &(123)(45), (13)(245), (12)(345), (1325), (1324)\}. \end{aligned}$$

Clearly, the subgroups of G of type s do not contain any element of $\mathcal{X}$.

All this implies that $\mathcal{H}$ is definitely unbeatable on $\mathcal{X}$, hence $r+t+d \geq |\mathcal{H}| = 20$. It follows that $56 = |\mathcal{M}| = 1+r+s+t+d > s+20$, i.e. $s < 36$. □

Observation 2.75. *Let M be the normalizer of a Sylow 5-subgroup of $\mathrm{Alt}(5)$, let $l \in \mathrm{Alt}(5)$ and suppose that $N_G(M \times M^l) \notin \mathcal{M}$. Then $N_G(\Delta_\alpha) \in \mathcal{M}$ for every $\alpha \in Ml$. In particular, letting $\mathcal{L}$ be the family of the cosets Ml where $M < \mathrm{Alt}(5)$ is the normalizer of a Sylow 5-subgroup and $N_G(M \times M^l) \notin \mathcal{M}$, the number of subgroups of type d in $\mathcal{M}$ is at least the size of the union of $\mathcal{L}$.*

Proof. The number of elements of type (5) in $N_G(M \times M^l)$ is 40. Moreover the only maximal subgroup of G of type r, s, t which contains one of these 40 elements is the one we are considering: $xy \in M$ determines M and $x \in Ml$ determines Ml. Let $c \in M$ be a 5-cycle. The element $(x, x^{-1}c)\varepsilon$ belongs to $N_G(\Delta_\alpha)$ if and only if $(\alpha x^{-1}c)^2 = c$, i.e. $\alpha x^{-1} c = c^3$, i.e. $\alpha = c^2 x$. The result follows. □

Lemma 2.76. *We have the following facts:*

1. *Let k be a positive integer, and let $\mathcal{L}$ be the family of the cosets of the normalizers of the Sylow 5-subgroups of $\mathrm{Alt}(5)$. Then any subfamily of $\mathcal{L}$ consisting of exactly k cosets covers at least $10k - 2\binom{k}{2}$ elements of $\mathrm{Alt}(5)$.*
2. *Let $H \neq K$ be two normalizers of Sylow 5-subgroups of $\mathrm{Alt}(5)$. Then for any a_1, a_2, a_3, b_1, b_2, $b_3 \in \mathrm{Alt}(5)$ such that Ha_1, Ha_2, Ha_3, Kb_1, Kb_2, Kb_3 are pairwise distinct, the union*
$$Ha_1 \cup Ha_2 \cup Ha_3 \cup Kb_1 \cup Kb_2 \cup Kb_3$$
has size at least 42.

Proof. Let $Ha, Kb \in \mathcal{L}$. If the intersection $Ha \cap Kb$ is non-empty then it contains an element x, so that $Ha = Hx$, $Kb = Kx$, and $Ha \cap Kb = Hx \cap Kx = (H \cap K)x$. It follows that the maximum size of the intersection of two elements of $\mathcal{L}$ equals the maximum size of the intersection of two normalizers of Sylow 5-subgroups, i.e. 2. Maximizing the sizes of the intersections we find that k cosets cover at least $10k - 2\binom{k}{2}$ elements.
We now prove the second statement. Clearly $|Ha_1 \cup Ha_2 \cup Ha_3| = 30$. Since $|Ha_i \cap Kb_j| \leq 2$ for every $i, j = 1, 2, 3$,
$$|Ha_1 \cup Ha_2 \cup Ha_3 \cup Kb_1 \cup Kb_2 \cup Kb_3| \geq 30 + 3 \cdot (10 - 3 \cdot 2) = 42,$$
as we wanted. □

Corollary 2.77. *$s \leq 31$ and $d \geq 30$.*

Proof. Recall that the subgroups of G of type s are 36. In the following we use Lemma 2.76 and Observation 2.75. If $s = 32$ then $d \geq 28$, impossible; if $s = 33$ then $d \geq 24$, impossible; if $s = 34$ then $d \geq 18$, impossible since $r \geq 6$. Assume now $s = 35$, so that $d \geq 10$. Since $r \geq 6$, $6 + 35 + t + d \leq r + s + t + d = 55$, i.e. $t + d \leq 14$. Thus inequality 8 implies that $5 \cdot 14 \geq 300 - 24r$, i.e. $r \geq 10$. Hence $d = r = 10$ and $t = 0$. This contradicts inequality 8. Since $s < 36$, we deduce that $s \leq 31$ and consequently $d \geq 30$. □

Since $d \geq 30$, $r + s + t + 30 \leq r + s + t + d = 55$, i.e. $r + s + t \leq 25$. Since $s \geq 17$ we obtain that $r + t \leq 8$. In particular $r \in \{6, 7, 8\}$.

- $r = 6$. Then by inequality 8 we have $144 + 5(t + d) \geq 24r + 3t + 5d = 24r + 3t + 5d \geq 300$, and we deduce that $t + d \geq 32$. Therefore $55 = r + s + t + d \geq 6 + s + 32$, i.e. $s \leq 17$. Since $s \geq 17$ we obtain that $s = 17$. Inequality 9 says that $5 \cdot 17 + 3d \geq 180$, i.e. $d \geq 32$, so that $d = 32$ and $t = 0$.
- $r = 7$. Since $d \geq 30$, $7 + s + 30 \leq r + s + t + d = 55$, i.e. $s \leq 18$.
  - $s = 18$. Then $7 + 18 + t + d = r + s + t + d = 55$, i.e. $t + d = 30$. Since $d \geq 30$ we obtain $d = 30$ and $t = 0$.
  - $s = 17$. Inequality 9 says that $5 \cdot 17 + 3d \geq 180$, i.e. $d \geq 32$, so that $55 = r + s + t + d \geq 7 + 17 + 32 = 56$, contradiction.
- $r = 8$. Then since $r + s + t \leq 25$ we obtain $s + t \leq 17$, and since $s \geq 17$ we have $s = 17$, $t = 0$ and $d = 30$. This contradicts inequality 9.

We deduce that either $(r, s, t, d) = (7, 18, 0, 30)$ or $(r, s, t, d) = (6, 17, 0, 32)$.
In both these cases there are at least 18 subgroups of type s outside $\mathcal{M}$. Therefore Observation 2.75 and Lemma 2.76(2) imply that $d \geq 42$, a contradiction.

CHAPTER 3

Normal covers

Given a non-cyclic group G and a family $\mathcal{H}$ of subgroups of G, we say that $\mathcal{H}$ is a "normal cover" of G if:

- every $g \in G$ belongs to some $H \in \mathcal{H}$, in other words $\bigcup_{H \in \mathcal{H}} H = G$;
- for every $g \in G$ and $H \in \mathcal{H}$, $H^g \in \mathcal{H}$, in other words $\mathcal{H}$ is stable under G-conjugation.

For a normal cover $\mathcal{H}$ of G, we denote by $\mathcal{H}^*$ the set of the orbits of the conjugation action of G on $\mathcal{H}$. We define $\gamma(G)$ to be $\min_{\mathcal{H}} |\mathcal{H}^*|$ where $\mathcal{H}$ varies in the family of the normal covers of G. Call "γ-minimal (normal) cover" of G a normal cover $\mathcal{H}$ of G such that $|\mathcal{H}^*| = \gamma(G)$. If G is cyclic we put $\gamma(G) := \infty$. We call $\gamma(G)$ the "normal covering number" of G.

3.1. $\gamma(G) > 1$ *for every finite group* G*. Indeed, if* $\{M_1, \ldots, M_n\}$ *is the conjugacy class of a maximal non-normal subgroup* $M = M_1$ *of* G *then since* $1 \in M_1 \cap \ldots \cap M_n$*,*

$$|M_1 \cup \ldots \cup M_n| < |M_1| + \ldots + |M_n| = |M| \cdot |G : M| = |G|.$$

Therefore $M_1 \cup \ldots \cup M_n \neq G$*.*

Note that this is false for infinite groups: for instance, since any complex matrix can be taken to upper-triangular form, and the invertible upper-triangular matrices form a group, we have

$$\gamma(GL(n, \mathbb{C})) = 1$$

for every integer $n \geq 2$.

Dealing with the covering number we had evidence of the following fact: given an integer $n \geq 3$, it is hard to decide whether there exists a group G with $\sigma(G) = n$, indeed there exists some n for which $\sigma(G) \neq n$ for every group G (cf. the introduction). We have a completely different behaviour for the normal covering number: A. Lucchini and E. Crestani [**LCg**] proved that for every integer $n \geq 2$ there exists a finite solvable group G with $\gamma(G) = n$.

It is clear that if N is a normal subgroup of G then $\gamma(G) \leq \gamma(G/N)$, since every normal cover of G/N lifts to a normal cover of G.

Definition 3.2. *We say that the non-cyclic group* G *is* γ*-elementary if* $\gamma(G) < \gamma(G/N)$ *for every non-trivial normal subgroup* N *of* G*.*

We now prove the analogous of Lemma 1.8:

Lemma 3.3. *Let* G *be a non-cyclic group. If* $\mathcal{M}$ *is a minimal normal cover of* G *and* g *is a central element of prime order* p *which does not belong to every* $M \in \mathcal{M}$ *then* $N := \bigcap_{K \in \mathcal{M}} K \trianglelefteq G$*,* $G/N \cong C_p \times C_p$ *and* $\gamma(G) = \gamma(G/N) = p + 1$*.*

Proof. Let $M_1, \dots, M_n$ be maximal subgroups of G with $n = \gamma(G)$ and $\mathcal{M} = M_1^G \cup \ldots \cup M_n^G$. The subgroups M_i not containing g are normal of index p and by Lemma 1.2 their number is at least p, so if M_i, M_j are two of them then $\gamma(G) \leq \gamma(G/M_i \cap M_j) = \gamma(C_p \times C_p) = p+1$, in particular since there is at least one M_i containing g we have $p < \gamma(G) \leq p+1$. The result follows. $\square$

We easily deduce the analogous of Proposition 1.9:

Proposition 3.4. *If G is a γ-elementary group then $\Phi(G) = \{1\}$, and either G is abelian or $Z(G) = \{1\}$. In particular, any nilpotent γ-elementary group is abelian.*

1. Coverings with normal subgroups

Coverings consisting of normal subgroups have been studied in [**BCK**].
Recall that if $G = \prod_{\alpha \in A} T_\alpha$ is a direct product of simple groups - and $\pi_\alpha : G \to T_\alpha$ denotes the α-th projection - then any maximal normal subgroup H of G is of one of the following forms:

- **Standard**: there exists $\alpha \in A$ such that
$$H = \prod_{A \ni \beta \neq \alpha} T_\beta.$$
- **Diagonal**: there exists a subset $B \subseteq A$ such that $\{T_\beta\}_{\beta \in B}$ consists of isomorphic abelian simple groups and H contains $\prod_{\alpha \in A-B} T_\alpha$ and projects surjectively onto T_β for each $\beta \in B$.

Proposition 3.5. *Let G be a group. The following statements are equivalent:*

1. *G is covered by its proper normal subgroups;*
2. *G is covered by its proper normal subgroups N such that G/N is abelian;*
3. *G/G' is non-cyclic.*

Proof. Clearly (3) $\Rightarrow$ (2) $\Rightarrow$ (1), so we are left to prove that (1) $\Rightarrow$ (3). Suppose G is covered by its proper normal subgroups, and let I be the intersection of the maximal normal subgroups of G. Then clearly G/I is covered by its proper normal subgroups. G/I is a subdirect product of simple groups, and it is well known that a subdirect product of simple groups is isomorphic to a direct product of simple groups. Say $I \cong T_1 \times \cdots \times T_r$. We need to prove that there exist $i \neq j$ in $\{1, \dots, r\}$ and a prime p such that $T_i \cong T_j \cong C_p$, i.e. that G admits a maximal normal subgroup of diagonal type. This is implied by the fact that the elements of $T_1 \times \cdots \times T_r$ with no non-trivial entries do not belong to any maximal normal subgroup of standard type. $\square$

2. Normal covers of a direct product

We now employ the ideas of Lemma 2.24 to prove a result analogous to Theorem 2.22 for the normal covering number.

Theorem 3.6. *Let H_1, H_2 be two groups such that $|H_1/H_1'|$ and $|H_2/H_2'|$ are coprime. Then*
$$\gamma(H_1 \times H_2) = \min(\gamma(H_1), \gamma(H_2)).$$

PROOF. Let $G := H_1 \times H_2$, and call $\pi_i : G \to H_i$ the i-th projection, for $i \in \{1,2\}$. Let K_i be the smallest normal subgroup of H_i such that H_i/K_i is a direct product of simple groups. Write

$$H_1/K_1 = S_1 \times \cdots \times S_\alpha, \qquad H_2/K_2 = T_1 \times \cdots \times T_\beta.$$

For $a \in \{1,\dots,\alpha\}$ and $b \in \{1,\dots,\beta\}$ let $\pi_{1,a} : H_1 \to S_a$ and $\pi_{2,b} : H_2 \to T_b$ be the canonical projections. Fix a minimal normal cover $\mathcal{M}$ of G consisting of maximal subgroups. Write $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2 \cup \mathcal{M}_3$ where $\mathcal{M}_i$ for $i \in \{1,2\}$ is the set of the maximal subgroups of G of the form $\pi_i^{-1}(L)$ where L is a maximal subgroup of H_i. Notice that $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$ are stable under conjugation, therefore

$$|\mathcal{M}^*| = |\mathcal{M}_1^*| + |\mathcal{M}_2^*| + |\mathcal{M}_3^*|.$$

By Lemma 2.23 every maximal subgroup M in $\mathcal{M}_3$ has the following form: there exist $a \in \{1,\dots,\alpha\}$, $b \in \{1,\dots,\beta\}$ and an isomorphism $\varphi : S_a \to T_b$ such that

$$M = \Delta(a,b,\varphi) := \{(h_1,h_2) \in G \mid \varphi(\pi_{1,a}(h_1)) = \pi_{2,b}(h_2)\}.$$

By the hypothesis if $\Delta(a,b,\varphi) \in \mathcal{M}_3$ then S_a and T_b are non-abelian simple groups. Now for $i \in \{1,2\}$ let

$$\Omega_i := \{h \in H_i \mid h \notin \pi_i(M)\ \forall M \in \mathcal{M}_i\}.$$

We now prove that $\Omega_1 \times \Omega_2 = \emptyset$, so that either $\mathcal{M} = \mathcal{M}_1$ or $\mathcal{M} = \mathcal{M}_2$.
By contradiction, assume that $\Omega_1 \times \Omega_2 \neq \emptyset$, and take $\omega \in \Omega_1$. For $\Delta(a,b,\varphi) \in \mathcal{M}_3$ define

$$U(a,b,\varphi) := \{h \in H_2 \mid \pi_{2,b}(h) \in \langle \varphi(\pi_{1,a}(\omega)) \rangle\}.$$

Since $\langle \varphi(\pi_{1,a}(\omega)) \rangle$ is a proper subgroup of T_b (because T_b is a non-abelian simple group, by hypothesis!), $U(a,b,\varphi)$ is a proper subgroup of H_2.
We claim that the family $\{U(a,b,\varphi) \mid \Delta(a,b,\varphi) \in \mathcal{M}_3\}$ is a normal family of subgroups of H_2 (stable under conjugation). Note that if $(x,y) \in G$ then being $\mathcal{M}_3$ a normal family,

$$\mathcal{M}_3 \ni \Delta(a,b,\varphi)^{(x,y)} = \Delta(a,b,\pi_{1,a}(x)^{-1} \circ \varphi \circ \pi_{2,b}(y)),$$

where $\pi_{1,a}(x)^{-1}$ and $\pi_{2,b}(y)$ are identified with the corresponding inner automorphisms of S_a, T_b respectively. Since $U(a,b,\varphi)^{h_2} = U(a,b,\varphi \circ \pi_{2,b}(h_2))$ for $h_2 \in H_2$, the subgroup $U(a,b,\varphi)^{h_2}$ comes from the diagonal subgroup $\Delta(a,b,\varphi)^{(1,h_2)}$. Thus $\{U(a,b,\varphi) \mid \Delta(a,b,\varphi) \in \mathcal{M}_3\}$ is a normal family. The claim is proved.
We claim that the family

$$\{M < H_2 \mid H_1 \times M \in \mathcal{M}_2\} \cup \{U(a,b,\varphi) \mid \Delta(a,b,\varphi) \in \mathcal{M}_3\}$$

covers H_2. Let $h \in \Omega_2$. The element (ω,h) belongs to $\Omega_1 \times \Omega_2$, and this set is covered by $\mathcal{M}_3$ (having empty intersection with each element of $\mathcal{M}_1 \cup \mathcal{M}_2$), therefore there exists $\Delta(a,b,\varphi) \in \mathcal{M}_3$ such that $(\omega,h) \in \Delta(a,b,\varphi)$, in other words $\varphi(\pi_{1,a}(\omega)) = \pi_{2,b}(h)$, in particular $h \in U(a,b,\varphi)$. The claim is proved.
Let $\mathcal{H} := \{U(a,b,\varphi) \mid \Delta(a,b,\varphi) \in \mathcal{M}_3\}$. We claim that $|\mathcal{H}^*| \leq |\mathcal{M}_3^*|$. For this it suffices to show that the function

$$\mathcal{M}_3^* \to \mathcal{H}^*, \qquad \Delta(a,b,\varphi)^G \mapsto U(a,b,\varphi)^{H_2}$$

is well defined and surjective. The surjectivity is clear. Let us show that it is well defined. Let $\Delta(a,b,\varphi) \in \mathcal{M}_3$ and $(x,y) \in G$. Since $\Delta(a,b,\varphi)^{(x,y)} = \Delta(a,b,\pi_{1,a}(x)^{-1} \cdot \varphi \cdot \pi_{2,b}(y))$, it suffices to show that $U(a,b,\pi_{1,a}(x)^{-1} \cdot \varphi \cdot \pi_{2,b}(y))$ and $U(a,b,\varphi)$ are conjugated by an element of H_2. Since $T_b \trianglelefteq \mathrm{Aut}(T_b)$, $\varphi^{-1} \cdot \pi_{1,a}(x)^{-1} \cdot \varphi$ is an inner automorphism of T_b, call it $t \in T_b$ and let $h \in H_2$ be such that $\pi_{2,b}(h) = t$. Note that

$$\pi_{1,a}(x)^{-1} \cdot \varphi \cdot \pi_{2,b}(y) = \varphi \cdot t \cdot \pi_{2,b}(y) = \varphi \cdot \pi_{2,b}(hy).$$

Therefore

$$U(a,b,\varphi)^{hy} = U(a,b,\varphi \cdot \pi_{2,b}(hy)) = U(a,b,\pi_{1,a}(x)^{-1} \cdot \varphi \cdot \pi_{2,b}(y)).$$

The claim is proved.
We obtain that

$$|\mathcal{M}_1^*| + |\mathcal{M}_2^*| + |\mathcal{M}_3^*| = \gamma(H_1 \times H_2) \leq \gamma(H_2) \leq |\mathcal{M}_2^*| + |\mathcal{H}^*| \leq |\mathcal{M}_2^*| + |\mathcal{M}_3^*|,$$

and this implies that $\mathcal{M}_1 = \emptyset$. Similarly we obtain $\mathcal{M}_2 = \emptyset$, thus $\mathcal{M} = \mathcal{M}_3$.
By Proposition 3.5 there exists $h \in H_2$ which does not belong to any proper normal subgroup N of H_2 with the property that H_2/N is non-abelian. In particular $\pi_{2,b}(h) \neq 1$ for every $b \in \{1,\dots,\beta\}$ such that T_b is non-abelian. It follows that the element $(1,h)$ does not belong to any subgroup in $\mathcal{M}_3$, contradiction. □

3. Upper bounds

In this section we give some upper bounds for $\gamma(G)$ for G a group. The content of this section is a joint work with Attila Maróti.

Proposition 3.7. *Let G be a non-cyclic solvable group. Then:*
1. *if G is σ-elementary and non-abelian then $\gamma(G) = 2$;*
2. *if $\gamma(G) > 2$ then there exist a prime p and a normal subgroup N of G such that $G/N \cong C_p \times C_p$ and $\sigma(G) = \sigma(G/G') = \sigma(G/N) = p+1$;*
3. *if G/G' is cyclic then $\gamma(G) = 2$.*

Proof. The first assertion follows from Theorem 1.24. Now suppose that $\gamma(G) > 2$, and let G/N be a σ-elementary quotient of G with the property that $\sigma(G) = \sigma(G/N)$. Since $\gamma(G) \leq \gamma(G/N)$, the first assertion implies that G/N is abelian hence $G/N \cong C_p \times C_p$ for some prime p, and (2) follows. (3) follows from (2). □

Proposition 3.8. *Let G be a non-cyclic group, and write $|G| = p_1^{a_1} \cdots p_k^{a_k}$ with the primes $p_1,\dots,p_k$ pairwise distinct. Then $\gamma(G) \leq \sum_{i=1}^k \frac{p_i^{a_i}-1}{p_i-1}$.*

Proof. We may assume that G is non-abelian and γ-elementary, in particular $Z(G) = \{1\}$ by Proposition 3.4. For every $i = 1,\dots,k$ choose a Sylow p_i-subgroup P_i of G. Then G is covered by the conjugates of the subgroups of the form $C_G(\langle x \rangle)$ where x belongs to $P_1 \cup \ldots \cup P_k$. □

Theorem 3.9. *Let G be a non-cyclic group. Then $\gamma(G) \leq \sqrt{|G|} + 1$.*

PROOF. Let G be a smallest counterexample to the statement of the theorem. Then G is non-solvable by proposition 3.7, and by minimality every proper quotient of G is cyclic, in particular G, being non-solvable, is monolithic and its Fitting subgroup is trivial. By [**GRp**, Theorem 10] it follows that the number of conjugacy classes of G is at most $\sqrt{|G|}$. Since G is covered by its cyclic subgroups, it follows that $\gamma(G) \leq \sqrt{|G|}$, contradiction. □

Proposition 3.7 implies that if G is a solvable group and p is the largest prime divisor of $|G|$ then $\gamma(G) \leq p+1$. What can we say about the general case?

CONJECTURE 3.10 (A. Maróti, M. Garonzi). *Let G be a non-cyclic group, and let p be the largest prime divisor of $|G|$. Then $\gamma(G) \leq p+1$.*

In the following we will prove the following partial result.

THEOREM 3.11. *Let G be a non-cyclic group, and suppose that whenever X is an almost simple section of G and $X/\operatorname{soc}(X)$ is cyclic, one of the following holds:*

- $\operatorname{soc}(X)$ *is either alternating or sporadic,*
- $X = PSL(n,q)$ *or* $X = PGL(n,q)$ *for some integer n and some prime-power q.*

Then $\gamma(G) \leq p+1$, where p is the largest prime divisor of $|G|$.

3.1. Reduction to the almost simple case. We now deal with Conjecture 3.10. In this section we reduce the problem to almost-simple groups. Let G be a smallest counterexample to the conjecture. By Proposition 3.7, we know that G is non-solvable. If N is a non-trivial normal subgroup of G such that G/N is non-cyclic then the conjecture holds for G/N hence it holds for G, contradiction. It follows that every proper quotient of G is cyclic, in particular G, being non-solvable, is monolithic with non-abelian socle. Let us use Notations 2.2. By Lemma 2.7 X/S is cyclic, let $x \in X$ be such that $X/S = \langle xS \rangle$. By Proposition 2.29

$$\gamma(G) \leq \omega(|G/\operatorname{soc}(G)|) + \gamma_X(xS) \leq \omega(|G/\operatorname{soc}(G)|) + \gamma(X),$$

where $\gamma_X(xS)$ denotes the smallest number of conjugacy classes of a family of subgroups of X which covers xS. For a positive real number r let $\pi(r)$ be the number of primes at most r. Let p be the largest prime dividing $|G|$. Since $\omega(|G/\operatorname{soc}(G)|) \leq \omega(|G|) \leq \pi(p)$, it is sufficient to prove that $\gamma(X) \leq p+1-\pi(p)$. Let q be the largest prime divisor of $|X|$. Then since $q \leq p$ and the function $x \mapsto x+1-\pi(x)$ is monotone non-decreasing, $q+1-\pi(q) \leq p+1-\pi(p)$, hence it is sufficient to prove that $\gamma(X) \leq q+1-\pi(q)$.
More in general, the following holds:

LEMMA 3.12. *For a group G denote by p_G the largest prime dividing $|G|$. If G is a group such that $\gamma(X) \leq {p_X}^k - \pi(p_X)$ for every almost simple section X of G such that $X/\operatorname{soc}(X)$ is cyclic then $\gamma(G) \leq {p_G}^k$. In particular if $\gamma(X) \leq {p_X}^k$ for every almost simple group X with $X/\operatorname{soc}(X)$ cyclic then $\gamma(G) \leq {p_G}^{k+1}$ for every group G.*

3.2. The almost simple case. Let X be an almost simple group with $\mathrm{soc}(X) = S$ and suppose that X/S is cyclic. Let p be the largest prime divisor of $|X|$. We want to prove that

$$\gamma(X) \leq p + 1 - \pi(p). \tag{10}$$

3.3. The alternating groups.

THEOREM 3.13 (Bubboloni, Praeger, [**BP**]). *Let $n \geq 4$ be an integer, and let G be* $\mathrm{Sym}(n)$ *or* $\mathrm{Alt}(n)$. *Then $\gamma(G)$ is at most:*

- $[\frac{n+4}{4}]$ *if $G = \mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$ and n is even;*
- $\frac{n-1}{2}$ *if $G = \mathrm{Sym}(n)$ and n is odd;*
- $[\frac{n+3}{3}]$ *if $G = \mathrm{Alt}(n)$ and n is odd.*

In particular $\gamma(G) \leq \frac{n-1}{2}$ for every $n \geq 5$.

THEOREM 3.14 (P. L. Chebyshev, [**Chb**]). *Let $x \geq 5$ be a real number. Then*

$$0.92 < \pi(x)\frac{\ln(x)}{x} < 1.11.$$

By Theorem 3.13, we see that bound (10) holds for $5 \leq n \leq 179$. Suppose now that $n \geq 180$. By Theorem 3.13, to prove bound (10) it is enough to prove $\frac{n-1}{2} + \pi(n) \leq p + 1$, and by Theorem 3.14 it suffices to prove that $\frac{n}{2} + 1.11 \cdot \frac{n}{\ln(n)} \leq p$. Since p is the largest prime at most n, it is enough to show that $\pi(n) > \pi(\frac{n}{2} + 1.11 \cdot \frac{n}{\ln(n)})$. By Theorem 3.14 it is enough to show that

$$0.92 \cdot \frac{1}{\ln(n)} > 1.11 \cdot \frac{\frac{1}{2} + 1.11 \cdot \frac{1}{\ln(n)}}{\ln(n(\frac{1}{2} + \frac{1.11}{\ln(n)}))}.$$

After multiplying by $2\ln(n)/1.11$ it is enough to see that

$$1.65 > \frac{\ln(n) + 2.22}{\ln(n) + \ln(\frac{1}{2} + \frac{1.11}{\ln(n)})}.$$

Since $\ln(\frac{1}{2} + \frac{1.11}{\ln(n)}) \geq -0.7$, it is enough to consider

$$0.65 > \frac{2.92}{\ln(n) - 0.7}.$$

Rearranging terms we obtain $\ln(n) > 5.2$, i.e. $n \geq 180$.
We are left with the case $X \in \{M_{10}, PGL_2(9)\}$. In this case $\mathrm{soc}(X) \cong \mathrm{Alt}(6)$, $p = 5$, and bound (10) follows from the following fact: X has exactly three conjugacy classes of maximal non-normal subgroups, and they cover X.
Recall the following result.

THEOREM 3.15 (Zsigmondi). *Let $a > b > 0$ be two coprime integers. For every integer $n > 1$ there exists a prime number p (called "primitive prime divisor") that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any positive integer $k < n$, with the following exceptions:*

- *$a = 2$, $b = 1$ and $n = 6$;*
- *$a + b$ is a power of 2 and $n = 2$.*

With what we have proved so far we can deduce the following:

THEOREM 3.16. *There exists a constant C such that for any non-cyclic group G, $\gamma(G) \leq Cp\log(p)$, where p is the largest prime divisor of $|G|$.*

PROOF. By the results above we are reduced to show that if G is almost-simple of Lie type, $G/\operatorname{soc}(G)$ is cyclic and $g \in G$ generates G modulo $\operatorname{soc}(G)$ then in order to cover $g\operatorname{soc}(G)$ with subgroups of G we need at most $Cp\log(p)$ conjugacy classes of subgroups of G, where C is some absolute constant. Assume first that $\operatorname{soc}(G)$ is of classical type. Aschbacher's theorem about the maximal subgroups of the classical groups [**AsCl**] implies that any cyclic subgroup generated by an element of $g\operatorname{soc}(G)$ is contained in a member of one of eight natural families of maximal subgroups. This implies that the natural families provide a (normal) cover of $g\operatorname{soc}(G)$, and by [**GKS**, Lemma 2.1] and [**LPS**, Lemmas 2.1(ii) and 2.4] the number of conjugacy classes of maximal subgroups in the natural families is at most $8r\log(r) + r\log(\log(q))$, where r is the rank and q is the order of the underlying field. It follows that in order to conclude the classical case it is enough to show that $q \leq p^p$ and $r \leq p$.

- Write $q = \ell^f$ where ℓ is a prime. If $(\ell, f) = (2, 6)$ or $f \leq 2$ then $q \leq 2^6p^2$. Otherwise, noticing that $q - 1$ divides $|G|$, we see that a primitive prime divisor (cf. Theorem 3.15) of $\ell^f - 1$ divides $|G|$ and this is at least $f + 1$. So $f + 1 \leq p$. Hence $q = \ell^f \leq p^p$.
- Now we bound r in terms of a function of p. Notice that a primitive prime divisor of $q^k - 1$ divides $|G|$ for some $k \geq r$, and it is at least $k + 1$. Therefore $r \leq p$.

If $\operatorname{soc}(G)$ is of exceptional type then since the rank of X is bounded the result is implied by [**LMS**, Theorem 1.3].

$\square$

The bound $\gamma(G) \leq Cp\log(p)$ of the above theorem does not seem to be easily improvable. The number of conjugacy classes of maximal subgroups in the natural families is at most $8r\log(r) + r\log(\log(q))$, and here the term $r\log(\log(q))$ comes from the subfield subgroups (class $\mathcal{C}_5$). Moreover if X is an almost simple group with $\operatorname{soc}(X)$ of exceptional type then [**LMS**, Theorem 1.2, Lemma 3.1] imply that the number of conjugacy classes of maximal subgroups of X is at most $C\log(r)$ for some absolute constant C. In particular, if one could show that every almost-simple group X with $X/\operatorname{soc}(X)$ cyclic and $\operatorname{soc}(X)$ of classical type is covered by the classes $\mathcal{C}_i$, $i \neq 5, 6, 7$ then the proof of Lemma 2.4 in [**LPS**] would improve the bound of Theorem 3.16 to $C\sqrt{p}\log(p) \leq Cp$.
In particular, we obtain the following result.

THEOREM 3.17. *Let G be a non-cyclic group without composition factors of classical Lie type. Then $\gamma(G) \leq Cp/\log(p)$, where p is the largest prime divisor of $|G|$ and C is an absolute constant.*

The term $p/\log(p)$ comes from $\omega(|G/\operatorname{soc}(G)|) \leq \pi(p)$.

3.4. The linear groups. Since the groups $GL(n,q)$ can be covered by all stabilizers of all k-dimensional subspaces, where $1 \leq k \leq [n/2]$, together with the cyclic subgroups of order $q^n - 1$, which are all conjugate, we see that $\gamma(GL(n,q)) \leq [n/2]+1$. Let L be a subgroup of $GL(n,q)$ containing $SL(n,q)$. The set of subgroups in the previous covering with each element intersected with L provides a covering for L, and these subgroups split into $[n/2]+1$ conjugacy classes of subgroups. Since all the considered subgroups contain the center of L, we obtain the following bound: $\gamma(L/Z(L)) \leq [n/2]+1$. Hence if $PSL(n,q) \leq X \leq PGL(n,q)$ then $\gamma(X) \leq [n/2]+1$.
Suppose $n \neq 2$ and q is not a Mersenne prime, or $(n,q) \neq (6,2)$. Then by Theorem 3.15 $q^n - 1$ admits a prime factor q_n which divides $|X|$ and such that $q_n \geq n+1$. It is sufficient to prove that $[n/2]+1 \leq n+2-\pi(n+1)$, i.e. $\pi(n+1) \leq n-[n/2]+1$, which is true for every $n \geq 2$.
Suppose $(n,q) = (6,2)$. Then 7 divides $|X|$ and $7 = n+1$, so the previous argument works.
Suppose $n = 2$. Then the largest prime divisor of $|X|$ is at least 3, so the previous argument works.
Note that if X is any cyclic extension of $PSL(n,q)$ then by these arguments it is sufficient to prove that $\gamma(X) \leq [n/2]+1$.

3.5. The sporadic groups. If X is a sporadic simple group then bound (10) follows from the table found in [**HMsp**].
Suppose that X is the automorphism group of a simple sporadic group with $\mathrm{soc}(X) \neq X$. Let p be the largest prime divisor of X. We see by inspection that X has at most $p - \pi(p)$ conjugacy classes of involutions, and since every element of odd order belongs to $\mathrm{soc}(X)$ and every element of even order centralizes an involution, to conclude it is enough to consider the family

$$\{\mathrm{soc}(X)\} \cup \{C_X(x) \mid x \in X,\ |x| = 2\}^G.$$

This concludes the proof of Theorem 3.11.

APPENDIX A

Some almost-simple groups

THEOREM A.1 (Maróti [**MarS**]). *Let $n > 3$ be an integer.*

- $\sigma(\mathrm{Sym}(n)) = 2^{n-1}$ *if n is odd and $n \neq 9$.*
- $\sigma(\mathrm{Sym}(n)) \leq 2^{n-2}$ *if n is even.*
- $\sigma(\mathrm{Alt}(n)) = 2^{n-2}$ *if $n \equiv 2 \mod 4$.*
- $\sigma(\mathrm{Alt}(n)) > 2^{n-2}$ *if $n \neq 7, 9$.*
- $172 \leq \sigma(\mathrm{Sym}(9)) \leq 256$, $\sigma(\mathrm{Sym}(12)) \leq 761$.
- *If $n \geq 14$ then $\sigma(\mathrm{Sym}(n)) > \frac{1}{2}\binom{n}{n/2}$.*

THEOREM A.2. *We list known results about small almost-simple groups.*

- $\sigma(M_{11}) = 23$ *([**MarS**]),*
- $\sigma(\mathrm{Alt}(5)) = 10$, $\sigma(\mathrm{Sym}(5)) = 16$ *([**Cohn**]),*
- $\sigma(\mathrm{Sym}(6)) = 13$ *([**S6**]),*
- $\sigma(\mathrm{Alt}(7)) = 31$, $\sigma(\mathrm{Alt}(8)) = 71$, $127 \leq \sigma(\mathrm{Alt}(9)) \leq 157$, $\sigma(\mathrm{Alt}(10)) = 256$ *([**KR**]),*
- $\sigma(M_{10}) \geq 45$ *([**DLpr**]).*

THEOREM A.3 ([**Lgps**] Theorem 1.2). *Let G be any of the groups $(P)GL(n,q)$, $(P)SL(n,q)$. Let b be the smallest prime factor of n, let $\left[\begin{array}{c} n \\ k \end{array}\right]_q$ be the number of k-dimensional subspaces of the n-dimensional vector space V over $\mathbb{F}_q$, and let $N(b)$ be the number of proper subspaces of V of dimensions not divisible by b. Suppose that $n \geq 12$. Then if $n \not\equiv 2 \mod 4$, or if $n \equiv 2 \mod 4$, q odd and $G = (P)SL(n,q)$, then*

$$\sigma(G) = \frac{1}{b} \prod_{i=1, b \nmid i}^{n-1} (q^n - q^i) + [N(b)/2]. \tag{11}$$

Otherwise

$$\sigma(G) = \frac{1}{2} \prod_{i=1, b \nmid i}^{n-1} (q^n - q^i) + \sum_{k=1, 2 \nmid k}^{n/2-1} \left[\begin{array}{c} n \\ k \end{array}\right]_q + \frac{q^{n/2}}{q^{n/2}+1} \left[\begin{array}{c} n \\ n/2 \end{array}\right]_q + \epsilon, \tag{12}$$

where $\epsilon = 0$ if q is even and $\epsilon = 1$ if q is odd.

THEOREM A.4 (Bryce, Fedri, Serena [**BFS**]). *Let $q \geq 4$ be a prime-power. Let*

$$G \in \{GL(2,q), PGL(2,q), SL(2,q), PSL(2,q)\},$$

with $q \neq 5, 7, 9$ *if* $G \in \{SL(2,q), PSL(2,q)\}$. *Then:*

$$\sigma(G) = \frac{1}{2}q(q+1) \qquad q \text{ even};$$

$$\sigma(G) = \frac{1}{2}q(q+1)+1 \qquad q \text{ odd}.$$

Moreover $\sigma(GL(2,2)) = \sigma(PGL(2,2)) = \sigma(SL(2,2)) = \sigma(PSL(2,2)) = 4$ *(these four groups are isomorphic to* Sym(3)*), and:*

$$\sigma(GL(2,3)) = \sigma(PGL(2,3)) = 4,\ \sigma(SL(2,3)) = \sigma(PSL(2,3)) = 5,$$
$$\sigma(SL(2,5)) = \sigma(PSL(2,5)) = 10,\ \sigma(SL(2,7)) = \sigma(PSL(2,7)) = 15,$$
$$\sigma(SL(2,9)) = \sigma(PSL(2,9)) = 16.$$

THEOREM A.5 (Lucido [**Luc**]). *Let* $G = {}^2B_2(q) = Suz(q)$ *be the simple Suzuki group. Then* $\sigma(G) = q^2(q^2+1)/2$.

APPENDIX B

Inspection

We now consider some more almost-simple groups and prove bounds needed in the thesis.

- Sym(8). It admits $PGL(2,7)$ as a maximal subgroup of index 120 and covering number 29, so $\sigma(\mathrm{Sym}(8)) \geq 29$ by Lemma 1.6.
- Let $G := \mathrm{Aut}(PSL(2,8)) = P\Gamma L(2,8)$. We are going to show that $\sigma(G) = 29$ and that there exists only one minimal cover of G.

  G is an almost simple group of order $1512 = 2^3 \cdot 3^3 \cdot 7$. $PSL(2,8)$, its non-trivial proper normal subgroup, is a maximal subgroup of covering number 36, thus if $\sigma(G) < 36$ then $PSL(2,8)$ appears in every minimal cover.

  Now, since $\mathrm{soc}(G)$ together with the normalizers of the Sylow 3-subgroups of $PSL(2,8)$ form a cover of G consisting of 29 subgroups, we have $\sigma(G) \leq 29$ so $\mathrm{soc}(G)$ appears in every minimal cover of G. The only maximal subgroups of G which contain elements of order 9 are $\mathrm{soc}(G) = PSL(2,8)$ and the normalizers of the Sylow 3-subgroups of $PSL(2,8)$. It follows that if P is a Sylow 3-subgroup of $\mathrm{soc}(G) = PSL(2,8)$ then $N_G(P)$ is the only maximal subgroup of G which contains the elements of order 9 in $N_G(P) - P$. So the 28 normalizers of the Sylow 3-subgroups of $\mathrm{soc}(G)$ appear in every minimal cover. So $\sigma(G) = 29$.
- Sym(10). Its maximal subgroups are the following [**Atl**]:
  - Sym(9);
  - $\mathrm{Sym}(8) \times C_2$;
  - $\mathrm{Sym}(7) \times \mathrm{Sym}(3)$;
  - $(\mathrm{Sym}(5) \times \mathrm{Sym}(5)) : 2$;
  - $\mathrm{Sym}(6) \times \mathrm{Sym}(4)$;
  - $2^5 : \mathrm{Sym}(5)$;
  - $\mathrm{Alt}(6) : 2^2$.

  Sym(8) and Sym(9) do not have elements of order 21. Thus $\mathrm{Sym}(8) \times C_2$ has no elements of order 21, and the only maximal subgroups of Sym(10) which contain elements of order 21 are of the kind $\mathrm{Sym}(7) \times \mathrm{Sym}(3)$. Now Sym(10) has $6! \cdot \binom{10}{7} \cdot 2! = 172800$ elements of order 21, and $\mathrm{Sym}(7) \times \mathrm{Sym}(3)$ has $6! \cdot 2! = 1440$ such elements, so in order to cover the elements of order 21 we need at least $172800/1440 = 120$ proper subgroups. Therefore $\sigma(\mathrm{Sym}(10)) \geq 120$.
- M_{12}. It admits $PSL(2,11)$ as a maximal non normal subgroup of covering number 67 and index 144, so $\sigma(M_{12}) \geq 67$ by Lemma 1.6.

- Sym(12). It admits $PGL(2,11)$ as a maximal non normal subgroup of covering number 67 and index 9!, so $\sigma(\mathrm{Sym}(12)) \geq \sigma(PGL(2,11)) = 67$ by Lemma 1.6.
- $PSL(3,3)$. It has 1728 elements of order 13, and its maximal subgroups which contain elements of order 13 are of the kind $C_{13} \rtimes C_3$, and such subgroups are 144. Since the $C_{13} \rtimes C_3$ have 12 elements of order 13, in order to cover the elements of order 13 we need at least $1728/12 = 144$ proper subgroups. In particular $\sigma(G) \geq 144$.
- $G := PSL(2,16) : 2$ admits $PSL(2,16)$ as a maximal and normal subgroup. The maximal subgroups of G are:
  - 17 copies of $((2^4.5).3).2$;
  - 120 copies of 17.4;
  - 68 copies of $C_2 \times \mathrm{Alt}(5)$;
  - 1 copies of $PSL(2,16)$;
  - 136 copies of $\mathrm{Sym}(3) \times D_{10}$.

  The only maximal subgroups which contain elements of order 10 are $C_2 \times \mathrm{Alt}(5)$ (which has 24 elements of order 10) and $\mathrm{Sym}(3) \times D_{10}$ (which contains 12 elements of order 10), and since G contains 1632 elements of order 10, we need at least $1632/24 = 68$ proper subgroups to cover the elements of order 10. In particular $\sigma(G) \geq 68$.
- $G := P\Gamma L(2,16) = PSL(2,16) \rtimes C_4$. The maximal subgroups of G are:
  - 17 copies of $((2^4.5).3).4$;
  - 136 copies of $(5.4) \times \mathrm{Sym}(3)$;
  - 68 copies of $\mathrm{Alt}(5).4$;
  - 120 copies of 17.8;
  - 1 copy of $PSL(2,16) \rtimes C_2$.

  The only maximal subgroups which contain elements of order 12 are $(5.4) \times \mathrm{Sym}(3)$ (which contains 20 elements of order 12) and $\mathrm{Alt}(5).4$ (which contains 40 elements of order 12), so to cover the elements of order 12 (which are 2720) we need at least $2720/40 = 68$ proper subgroups, so that $\sigma(G) \geq 68$.
- $PSL(3,4) = M_{21}$. The only maximal subgroup of $PSL(3,4)$ which contains elements of order 7 is $PSL(2,7)$, which contains 48 elements of order 7. Since $PSL(3,4)$ has 5760 elements of order 7, the covering number of $PSL(3,4)$ is at least $5760/48 = 120$.
- $P\Sigma L(3,4) = PSL(3,4) : 2$. The only maximal subgroup of $P\Sigma L(3,4)$ which contains elements of order 14 is $PSL(2,7) \times C_2$, which contains 48 elements of order 14. Since $P\Sigma L(3,4)$ has 5760 elements of order 14, the covering number of $P\Sigma L(3,4)$ is at least 120.
- $PGL(3,4)$. The only maximal subgroup of $PGL(3,4) = PSL(3,4) : 3$ which contains elements of order 21 is $(7:3) \times 3$, which contains 12 elements of order 21. Since $PGL(3,4)$ contains 11520 elements of order 21, the covering number of $PGL(3,4)$ is at least $11520/12 = 960$.
- $\sigma(P\Gamma L(3,4)) = 3$.
- M_{22}. It contains 80640 elements of order 11, and the only maximal subgroup of M_{22} which contains elements of order 11 is $PSL(2,11)$, which contains 120 such elements. Thus the covering number of M_{22} is at least $80640/120 = 672$.

- $M_{22}:2$. It admits $PGL(2,11)$ as a maximal and non normal subgroup of index 672 and covering number 67, so $\sigma(M_{22}:2) \geq 67$ by Lemma 1.6.
- M_{23}. It admits $\mathrm{Alt}(8)$ as a maximal non normal subgroup of index 506 and covering number ≥ 64, so $\sigma(M_{23}) \geq 64$ by Lemma 1.6.
- M_{24}. It admits $PSL(2,23)$ as a maximal non normal subgroup of covering number 277 and index 40320, so $\sigma(M_{24}) \geq 277$ by Lemma 1.6.

In the following list we summarize some information we need, deduced from above, about $\sigma(G)$ where G is a primitive group of degree at most 24.

- Degree 5. $\sigma(\mathrm{Alt}(5)) = 10; \sigma(\mathrm{Sym}(5)) = 16$.
- Degree 6. $\sigma(\mathrm{Alt}(5)) = 10; \sigma(\mathrm{Sym}(6)) = 13; \sigma(\mathrm{Sym}(5)) = 16$.
- Degree 7. $\sigma(SL(3,2)) = 15; \sigma(\mathrm{Alt}(7)) = 31; \sigma(\mathrm{Sym}(7)) = 64$.
- Degree 8. $\sigma(PSL(2,7)) = \sigma(PGL(2,7)) = 29$; $\sigma(\mathrm{Alt}(8)) \geq 64$; $\sigma(\mathrm{Sym}(8)) \geq 29$.
- Degree 9. $\sigma(\mathrm{Aut}(PSL(2,8))) = 29$; $\sigma(PSL(2,8)) = 36$; $\sigma(\mathrm{Alt}(9)) \geq 80$; $\sigma(\mathrm{Sym}(9)) \geq 172$.
- Degree 10. $\sigma(\mathrm{Alt}(5)) = 10$; $\sigma(\mathrm{Sym}(6)) = 13$; $\sigma(\mathrm{Alt}(6)) = 16$; $\sigma(PGL(2,9)) = 46$; $\sigma(M_{10})$, $\sigma(\mathrm{Alt}(10))$, $\sigma(\mathrm{Sym}(10)) \geq 45$, $\sigma(P\Gamma L(2,9)) = 3$.
- Degree 11. $\sigma(M_{11}) = 23$; $\sigma(PSL(2,11)) = 67$; $\sigma(\mathrm{Alt}(11))$, $\sigma(\mathrm{Sym}(11)) \geq 512$.
- Degree 12. $\sigma(M_{11}) = 23$; $\sigma(PSL(2,11)) = \sigma(PGL(2,11)) = 67$; $\sigma(M_{12})$, $\sigma(\mathrm{Alt}(12))$, $\sigma(\mathrm{Sym}(12)) \geq 67$.
- Degree 13. $\sigma(PSL(3,3))$, $\sigma(\mathrm{Alt}(13))$, $\sigma(\mathrm{Sym}(13)) \geq 144$.
- Degree 14. $\sigma(PSL(2,13))$, $\sigma(PGL(2,13))$, $\sigma(\mathrm{Alt}(14))$, $\sigma(\mathrm{Sym}(14)) \geq 92$.
- Degree 15. $\sigma(\mathrm{Sym}(6)) = 13$; $\sigma(\mathrm{Alt}(6)) = 16$; $\sigma(\mathrm{Alt}(7)) = 31$; $\sigma(PSL(4,2))$, $\sigma(\mathrm{Alt}(15))$, $\sigma(\mathrm{Sym}(15)) \geq 64$.
- Degree 16. $\sigma(\mathrm{Alt}(16)) \geq 2^{14}$; $\sigma(\mathrm{Sym}(16)) > 6435$.
- Degree 17. $\sigma(PSL(2,16))$, $\sigma(PSL(2,16):2)$, $\sigma(P\Gamma L(2,16))$, $\sigma(\mathrm{Alt}(17))$, $\sigma(\mathrm{Sym}(17)) \geq 68$.
- Degree 18. $\sigma(PSL(2,17))$, $\sigma(PGL(2,17))$, $\sigma(\mathrm{Alt}(18))$, $\sigma(\mathrm{Sym}(18)) \geq 2^{16}$.
- Degree 19. $\sigma(\mathrm{Alt}(19))$, $\sigma(\mathrm{Sym}(19)) \geq 2^{17}$
- Degree 20. $\sigma(PSL(2,19))$, $\sigma(PGL(2,19))$, $\sigma(\mathrm{Alt}(20))$, $\sigma(\mathrm{Sym}(20)) \geq 191$.
- Degree 21. $\sigma(SL(3,2)) = 15$; $\sigma(\mathrm{Alt}(7)) = 31$; $\sigma(P\Gamma L(3,4)) = 3$; $\sigma(PGL(2,7))$, $\sigma(\mathrm{Sym}(7))$, $\sigma(PSL(3,4))$, $\sigma(P\Sigma L(3,4))$, $\sigma(PGL(3,4))$, $\sigma(\mathrm{Alt}(21))$, $\sigma(\mathrm{Sym}(21)) \geq 64$.
- Degree 22. $\sigma(M_{22})$, $\sigma(M_{22}:2)$, $\sigma(\mathrm{Alt}(22))$, $\sigma(\mathrm{Sym}(22)) \geq 67$.
- Degree 23. $\sigma(M_{23})$, $\sigma(\mathrm{Alt}(23))$, $\sigma(\mathrm{Sym}(23)) \geq 64$.
- Degree 24. $\sigma(M_{24})$, $\sigma(PSL(2,23))$, $\sigma(PGL(2,23))$, $\sigma(\mathrm{Alt}(24))$, $\sigma(\mathrm{Sym}(24)) \geq 277$.

1. Two affine groups

In this section we show that $\sigma(AGL(4,2)) \geq 31 = \sigma(\mathbb{F}_2{}^4 \rtimes \mathrm{Alt}(7))$.

- $G := AGL(4,2) = \mathbb{F}_2{}^4 \rtimes GL(4,2)$. We want to show that $\sigma(G) \geq 31$. We observe that $GL(4,2) \cong \mathrm{Alt}(8)$ and G is monolithic. Let $V := \mathbb{F}_2{}^4$ and $H := GL(4,2)$, so that $G = V \rtimes H$. Since $\sigma(\mathrm{Alt}(8)) \geq 69$, if (as we can suppose) $\sigma(G) < 69$ then every complement of V must appear in every minimal cover $\{M_1, \ldots, M_n\}$ of G, where $n = \sigma(G)$. We have $H^1(H,V) = 0$ by the result in [**JP**], so that V has exactly 16 complements in G, let them be $M_1, \ldots, M_{16}$. If $g \in GL(4,2)$ stabilizes a non-zero vector

$v \in V$ then the function ${\mathbb{F}_2}^4 \to {\mathbb{F}_2}^4$ which sends x to $x^g - x$ is not injective (having v in its kernel), so it is not surjective: there exists $w \in V$ such that $x^g - x \neq w$ for every $x \in V$. In this case $wg \in G$ does not belong to any complement of V, because the complements of V are conjugate to H, and $wg \in H^x$ means $g \in H$ and $w = x - x^g$. Thus wg must lie in at least one M_i with $i \geq 17$, so g must belong to it, because the maximal subgroups which do not complement V must contain it (V is the only minimal normal subgroup of G). It turns out that $M_{17}/V, \ldots, M_n/V$ must cover all the point stabilizers of $GL(4,2)$. If v is a non-zero vector then the point stabilizer of v in $GL(4,2)$ is isomorphic to $ASL(3,2)$, whose covering number is 15. So either every point stabilizer is one of the M_i/V with $i \geq 17$ or the M_i/V with $i \geq 17$ are at least 15. In any case the M_i/V with $i \geq 17$ are at least 15, so $\sigma(G) \geq 15 + 16 = 31$.

- $G := {\mathbb{F}_2}^4 \rtimes \mathrm{Alt}(7)$. Let $V := {\mathbb{F}_2}^4$ and $H := \mathrm{Alt}(7)$. We want to show that $\sigma(G) \geq 31$. Suppose by contradiction that $\sigma(G) \leq 30$, so that all the complements of V appear in every minimal cover of G (because $\sigma(\mathrm{Alt}(7)) = 31$). Since $\sigma(G) \leq \sigma(H) = 31$ we have $H^1(H,V) = 0$ (otherwise we would have at least 32 complements of V). Let $M_1, \ldots, M_{16}$ be the 16 complements of V in G. Since H acts faithfully on 16 elements, we have an injection $\mathrm{Alt}(7) \to \mathrm{Sym}(16)$, and a 7-cicle h of $\mathrm{Alt}(7)$ must fix a non-zero vector in this action (the image of a 7-cycle in $\mathrm{Sym}(16)$ is either a 7-cycle or a product of two disjoint 7-cycles), let v be this vector. Then $vh \in G$ does not belong to any complement of H because it has order 14, and H has no elements of order 14. Thus vh lies in a M_i with $i \geq 17$, and every such M_i contains V (because it does not complement it), so $M_{17}/V, \ldots, M_n/V$ contain together all the 7-cycles. But to cover the 7-cycles in $\mathrm{Alt}(7)$ we need at least 15 subgroups, because the 7-cycles in $\mathrm{Alt}(7)$ are 6! and the only maximal subgroups of $\mathrm{Alt}(7)$ which contain 7-cycles are the $SL(3,2)$, and they contain 48 7-cycles. We deduce that $\sigma(G) \geq 16 + 15 = 31$, contradiction. In particular since $\sigma(G) \leq \sigma(\mathrm{Alt}(7)) = 31$, G is a non-σ-elementary group with covering number 31.

APPENDIX C

Acknowledgements

I want to thank my supervisor, Andrea Lucchini, for giving me the opportunity of writing a thesis in Group Theory, and particularly for fruitful conversations which helped me asking better and better questions to myself: thanks to him I realized many things about the importance of formulating problems properly and of asking the right questions. I want to thank Federico Menegazzo and Eloisa Detomi for giving me the opportunity to actively participate to the didactic activity. I want to thank Attila Maróti for very fruitful collaborations, Tim Burness for the support and all the members of my committee. I want to thank my family, Paola (my mother), Luigi (my father), Emiliano (my brother), Angelina (my grandmother), my cousins and my uncles for supporting me and being always there. I want to thank my friends, especially I want to thank the three most amazing friends one can have: Neeraja, Sophie, Eleni. I want to thank Franzisca. And Jonna, Maura, Velibor, Priyanka, Silu, Elisa, Szabolcs, and Betty, Alessandro, Chunlei, Esen, and Tiberio, Anita, Marco, Juan, and Gian Maria, Eleonora, Alessio, Ivano, and Davide, Leonardo, and Marcus, Roberto, Zizzari. I want to thank *Chess* thanks to which I got used to fight and *Mathematics* for constantly providing me with things to think about.

Bibliography

[AGco] M. Aschbacher, R. Guralnick, Some applications of the first Cohomology Group; J. Algebra, 90(1984), 446–460.

[AGpr] M. Aschbacher, R. Guralnick, On abelian quotients of primitive groups; Proc. Amer. Math. Soc., 107 (1989) 89–95.

[Asch] M. Aschbacher, Finite group theory, Second edition; Cambridge Studies in Advanced Mathematics 10, Cambridge University Press, Cambridge, (2000).

[AsCl] M. Aschbacher, On the maximal subgroups of the finite classical groups; Invent. Math. 76 (1984), no. 3, 469-514.

[Atl] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups; Clarendon Press Oxford.

[BB] D. Berend, Y. Bilu, Polynomials with roots modulo every integer; Proc. Amer. Math. Soc. 124 (1996), no. 6, 16631671.

[BCK] M. A. Brodie, R. F. Chamberlain, L. C. Kappe, Finite coverings by normal subgroups; Proc. Amer. Math. Soc. 104 (1988), no. 3, 669-674.

[BEcl] A. Ballester-Bolinches, L. M. Ezquerro, Classes of Finite Groups; Springer, 2006.

[BFS] R.A. Bryce, V. Fedri, L. Serena, Subgroup coverings of some linear groups; Bull. Austral. Math. Soc., 60(1999), 227–238.

[Bha] M. Bhargava, Finiteness Criteria for Coverings of Groups by finitely many Subgroups or Cosets; Int. Electron. J. Algebra 2 (2007), 83-89.

[BP] D. Bubboloni, C. E. Praeger, Normal Coverings of Symmetric and Alternating Groups; Journal of Combinatorial Theory, Series A, 2011.

[Cam] P.J. Cameron, “Permutation Groups”; London Mathematical Society Student Texts 45. Cambridge University Press, 1999.

[Chb] P. L. Chebyshev, Mémoire sur les nombres premiers; J. de Math. Pures Appl. (1) 17 (1852), 366–390.

[Cohn] J.H.E. Cohn, On n-sum groups; Math. Scand., 75(1) (1994), 44–58.

[Coo] B. N. Cooperstein, Minimal degree for a permutation representation of a classical group; Israel J. Math. 30 (1978), no. 3, 213–235.

[DaLdp] E. Damian, A. Lucchini, On the Dirichlet polynomial of finite groups of Lie type; Rend. Sem. Mat. Univ. Padova Vol. 115 (2006).

[DaLpm] E. Damian, A. Lucchini, Finite Groups with p-Multiplicative Probabilistic Zeta Function; Comm. Algebra 35 (2007), no. 11, 3451-3472.

[DLcr] E. Detomi, A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group; Journal of Algebra 265 (2003) 651–668.

[Dlg] Dickson, L. E. Linear groups: With an exposition of the Galois field theory; Dover Publication Inc. New York, 1958.

[DLpr] E. Detomi, A. Lucchini, On the Structure of Primitive n-Sum Groups; CUBO A Mathematical Journal Vol.10 n. 03 (195–210), 2008.

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4; 2005, (http://www.gap-system.org).

[Gar1] M. Garonzi, Finite Groups that are the union of at most 25 proper subgroups; Journal of Algebra and Its Applications Vol. 12, No. 4 (2013) 1350002.

[Gar2] Garonzi Martino, Covering certain monolithic groups with proper subgroups; Communications in algebra, 41:2, 471–491

[Gasc] W. Gaschütz, Existenz und Konjugiertsein von Untergruppen, die in endlichen auflosbaren Gruppen durch gewisse Indexschranken definiert sind; Journal of Algebra 53 (1978), 1–20.

[GKS] R. Guralnick, W. M. Kantor, J. Saxl, The probability of generating a Classical Group; Comm. Algebra 22 (1994), no. 4, 1395-1402.

[GL] M. Garonzi, A. Lucchini, Direct products of finite groups as unions of proper subgroups; Arch. Math. (Basel) 95 (2010), no. 3, 201-206.

[GM] A. Maróti, M. Garonzi, Covering certain wreath products with proper subgroups; J. Group Theory 14 (2011), no. 1, 103-125.

[GRp] R. M. Guralnick, G. R. Robinson, On the commuting probability in finite groups; Journal of Algebra 300 (2006) 509-528.

[HMsp] P. E. Holmes, A. Maróti, Pairwise generating and covering sporadic simple groups; Journal of Algebra Vol. 324 Issue 1 (2010) 25–35.

[JP] W. Jones, B. Parshall, On the 1-cohomology of finite groups of Lie type; Proceeding of the conference on Finite Groups (Univ. Utah, Park City, Utah 1975) 313-328 Academic Press, New York 1976.

[KR] L. C. Kappe, J. L. Redden, On the Covering Number of Small Alternating Groups; Contemp. Math., 511, Amer. Math. Soc., Providence, RI, 2010.

[KL] P. Kleidman, M. Liebeck, The Subgroup Structure of the Finite Classical Groups; Cambridge University Press.

[KLS] W. M. Kantor, A. Lubotzky, A. Shalev, Invariable generation and the Chebotarev invariant of a finite group; J. Algebra 348 (2011), 302-314.

[LCg] A. Lucchini, E. Crestani, Normal Coverings of Solvable Groups; Arch. Math. 98 (2012), 13-18.

[Lgps] J.R. Britnell, A. Evseevb, R.M. Guralnick, P.E. Holmes, A. Maróti, Sets of elements that pairwise generate a linear group; J. Combin. Theory Ser. A 115 (3) (2008) 442–465.

[LMkn] A. Lucchini, A. Maróti, On non-abelian simple groups and Kneser graphs; J. Algebraic Combin. 30 (2009), no. 4, 549-566.

[LMS] M. W. Liebeck, B. M. S. Martin, A. Shalev, On conjugacy classes of maximal subgroups of finite simple groups, and a related zeta function; Duke Math. J. 128 (2005), no. 3, 541-557.

[LPS] M. Liebeck, L. Pyber, A. Shalev, On a conjecture of G. E.Wall; J. Algebra 317 (2007), 184-197.

[Luc] M. S. Lucido, On the covers of finite groups; Groups St. Andrews 2001 in Oxford. Vol. II, 395399, London Math. Soc. Lecture Note Ser., 305, Cambridge Univ. Press, Cambridge, 2003.

[MarP] A. Maróti, "On the orders of primitive groups"; J. Algebra 258 (2002), no.2, 631–640.

[MarS] A. Maróti, Covering the symmetric groups with proper subgroups; J. Combin. Theory Ser. A, 110(1) (2005), 97–111.

[Neu] B. H. Neumann, Groups covered by permutable subsets; J. London Math. Soc. 29, 236–248 (1954).

[O'N] M. W. Liebeck, C. E. Praeger, J. Saxl, On the ONan-Scott theorem for finite primitive permutation groups. J. Austral. Math. Soc. Ser. A 44(3) (1988), 389-396.

[Rob] D. J. S. Robinson, A course in the theory of groups; Second edition; Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[S6] A. Abdollahi, F. Ashraf, S. M. Shaker, The symmetric group of degree six can be covered by 13 and no fewer proper subgroups; Bull. Malays. Math. Sci. Soc. (2) 30 (2007), no. 1, 57–58.

[Sco] G. Scorza, I gruppi che possono pensarsi come somme di tre loro sottogruppi; Boll. Un Mat. Ital. (1926) 216–218.

[SerLaf] P. Jiménez-Seral and J. P. Lafuente, On complemented non-abelian chief factors of a finite group; Israel Journal of Mathematics 106 (1998), 177–188.

[Suz] M. Suzuki, Group theory. I; Grundlehren der Mathematischen Wissenschaften 247, Springer-Verlag, Berlin, (1982).

[Tom] M.J. Tomkinson, Groups as the union of proper subgroups; Math. Scand., 81(2) (1997), 191–198.

[Wfpf] Y. M. Wang, Finite groups admitting a fixed-point-free automorphism group; Northeast. Math. J., 9(4) (1993), 516–520.