

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Coverings and pairwise generation of some primitive groups of wreath product type

Júlia Arêdes de Almeida

Orientador: Prof. Dr. Martino Garonzi

Brasília

15 de fevereiro de 2024

Júlia Arêdes de Almeida

Coverings and pairwise generation of some primitive groups of wreath product type

Tese apresentada ao Departamento de
Matemática da Universidade de Brasília,
como parte dos requisitos para obtenção do
grau de Doutor em Matemática.

Orientador:
Prof. Dr. Martino Garonzi

Brasília

15 de fevereiro de 2024

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

AA447c Almeida, Júlia
Coverings and pairwise generation of some primitive
groups of wreath product type / Júlia Almeida; orientador
Martino Garonzi. -- Brasília, 2024.
86 p.

Tese(Doutorado em Matemática) -- Universidade de
Brasília, 2024.

1. Permutation group. 2. Primitive group. 3. Covering. 4.
Group generation. I. Garonzi, Martino, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Coverings and pairwise generation of some primitive groups of wreath product type

por

Júlia Arêdes de Almeida*

Tese apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de


DOCTOR EM MATEMÁTICA

Brasília, 15 de fevereiro de 2024.

Comissão examinadora:




Prof. Dr. Martino Garonzi – UnB (Orientador)



Prof. Dr. Emerson Ferreira de Melo – UnB (Membro)

Documento assinado digitalmente

 CSABA SCHNEIDER
Data: 28/02/2024 11:58:37-0300
Verifique em <https://validar.it.gov.br>

Prof. Dr. Csaba Schneider – UFMG (Membro)



Prof. Dr. Francesco Fumagalli – UniFI (Membro)

*O autor foi bolsista do CNPq durante a elaboração desta tese.

Resumo

O número de cobertura de um grupo finito não cíclico G , denotado por $\sigma(G)$, é o menor inteiro positivo k tal que G é uma união de k subgrupos próprios. Se G é um grupo 2-gerado, seja $\omega(G)$ o tamanho máximo de um subconjunto S de G com a propriedade de que quaisquer dois elementos distintos de S geram G . Uma vez que qualquer subgrupo próprio de G pode conter no máximo um elemento de tal conjunto S , $\omega(G)$ é no máximo $\sigma(G)$. Para uma família de grupos primitivos G com um único subgrupo normal mínimo N isomorfo a uma potência direta do grupo alternado A_n e G/N cíclico, calculamos $\sigma(G)$ para n divisível por 6 e m pelo menos 2. Este resultado é uma generalização de um resultado de E. Swartz relativo aos grupos simétricos, que corresponde ao caso $m = 1$. Para a família de grupos primitivos G acima, também provamos um resultado relativo à geração 2-a-2: para m fixo e pelo menos 2 e n par, calculamos assintoticamente o valor de $\omega(G)$ quando n vai para o infinito e mostramos que $\omega(G)/\sigma(G)$ tende para 1 quando n tende para infinito.

Palavras-chave: Grupo de Permutação, Grupo Primitivo, Cobertura, Geração de grupo.

Título: Coberturas e Geração dois a dois de alguns grupos primitivos de tipo entrelaçado

Abstract

The covering number of a finite noncyclic group G , denoted $\sigma(G)$, is the smallest positive integer k such that G is a union of k proper subgroups. If G is 2-generated, let $\omega(G)$ be the maximal size of a subset S of G with the property that any two distinct elements of S generate G . Since any proper subgroup of G can contain at most one element of such a set S , $\omega(G)$ is at most $\sigma(G)$. For a family of primitive groups G with a unique minimal normal subgroup N isomorphic to a direct power of the alternating group A_n and G/N cyclic, we calculate $\sigma(G)$ for n divisible by 6 and m at least 2. This is a generalization of a result of E. Swartz concerning the symmetric groups, which corresponds to the case $m = 1$. For the above family of primitive groups G , we also prove a result concerning pairwise generation: for fixed m at least 2 and n even, we calculate asymptotically the value of $\omega(G)$ when n goes to infinity and show that $\omega(G)/\sigma(G)$ tends to 1 as n tends to infinity.

Keywords: Permutation group, Primitive group, Covering, Group generation.

Contents

Introduction	9
1 Preliminaries	21
1.1 Primitive groups	21
1.2 Maximal subgroups of the Symmetric Group	33
2 Minimal coverings	48
2.1 The function $\sigma(G)$	48
2.1.1 $\sigma(G)$ for some groups	51
2.2 A sufficient condition for a covering to be minimal	52
2.3 Proof of Theorem 1	54
2.3.1 The group $G_{n,m}$	54
2.3.2 The set Π	58
2.3.3 The covering \mathcal{C}	64
2.3.4 Maximal subgroups of $G_{n,m}$	66
2.3.5 Proof of Theorem 1	69
3 Pairwise generation	79
3.1 The function $\omega(G)$	79

3.2	$\omega(S \times S)$	81
3.3	$\omega(G_S)$	84
3.4	The Lovász Local Lemma	85
3.5	Proof of Theorem 2	88
Appendix		96
A	$\omega(G)$ for small groups G	97
A.1	Computing a clique for A_5 with Gurobi	97
A.2	The symmetric group S_5	98
A.3	The symmetric group S_6	99
A.4	The symmetric group S_8	99
A.5	The symmetric group S_9	100
A.6	The symmetric group S_{10}	101
Bibliography		103

Introduction

In this work, all groups are assumed to be finite. A covering of a group G is a family of proper subgroups of G whose union is G and the covering number of G , denoted $\sigma(G)$, is the smallest size of a covering of G . This interesting invariant was introduced by J. H. E. Cohn in [9] and it was later studied by many authors. Note that there always exist minimal coverings consisting of maximal subgroups. 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 .

A simple graph Γ is a pair (V, E) where V is a set, whose elements are called vertices, and E is a set of subsets of V of size 2, whose elements are called edges. If $\{x, y\} \in E$, we say that x and y are connected by an edge. The graph Γ is called complete if $\{x, y\} \in E$ for every two distinct elements x, y of V . A subgraph of the simple graph $\Gamma = (V, E)$ is a graph $\Delta = (W, F)$ where W is a subset of V and F is a subset of E , and such that whenever x, y are two distinct elements of W , we have $\{x, y\} \in F$ if and only if $\{x, y\} \in E$ (in other words, for us all subgraphs are induced subgraph). A clique of a simple graph Γ is a complete subgraph of Γ , and the clique number of Γ is the maximal size of a clique of Γ , where by “size” of a graph we mean the size of its vertex set.

If G is a group, denote by $d(G)$ the minimal size of a subset S of G which generates G , i.e. $\langle S \rangle = G$. For example, G is cyclic if and only if $d(G) \leq 1$. The group G is called d -generated if $d(G) \leq d$. If G is a 2-generated group, the generating graph of G is the simple graph whose vertices are the elements of G and two vertices x, y are connected by an edge if and only if $\langle x, y \rangle = G$. We denote by $\omega(G)$ the clique number of

the generating graph of G . In other words $\omega(G)$ is the maximal size of a subset S of G with the property that $\langle x, y \rangle = G$ whenever $x, y \in S$ and $x \neq y$. Since any proper subgroup of G can contain at most one element of such a set S , we have

$$\omega(G) \leq \sigma(G).$$

It is very natural to ask whether equality occurs for some families of groups. In general, equality doesn't hold, for example $\omega(A_5) = 8$ and $\sigma(A_5) = 10$. A clique of the generating graph of A_5 of maximal size is

$$C = \{(145), (235), (12354), (15342), (12453), (15423), (14235), (12345)\}.$$

A covering of A_5 of size 10 is given by (any) four point stabilizers and the six Sylow 5-subgroup normalizers.

The following approach is due to Eric Swartz. Using GAP (a system for computational discrete algebra [16]) and GUROBI (a linear programming solver [22]), it is possible to calculate $\omega(G)$ for groups G of small orders. The approach of calculating the function σ for groups of (relatively) small order was followed in [25], where the covering number of S_9 was calculated (among other things, see below for more information).

- GAP formulates the problem,
- GUROBI solves it.

The general idea is the following.

$$\begin{aligned} G &= \{g_1, \dots, g_n\}, & n &= |G|, \\ \mathcal{M} &:= \{\text{maximal subgroups of } G\}, \\ I_M &:= \{i \in \{1, \dots, n\} : g_i \in M\} & \forall M \in \mathcal{M}. \end{aligned}$$

The linear optimization problem is the following. The variables are $x_i \in \{0, 1\}$.

Maximize $\sum_{i=1}^n x_i$ **subject to** $\sum_{i \in I_M} x_i \leq 1$ **for all** $M \in \mathcal{M}$.

The interpretation is the following: we are looking for a clique C of maximal size in the generating graph of G . Let us interpret the variables

x_i as follows.

$$x_i = \begin{cases} 1 & \text{if } g_i \in C, \\ 0 & \text{if } g_i \notin C. \end{cases}$$

The condition $\sum_{i \in I_M} x_i \leq 1$ means exactly that no two distinct elements of C can belong to M , and this must hold for every $M \in \mathcal{M}$. Of course, this is the definition of C being a clique, and we have

$$|C| = \sum_{i=1}^n x_i.$$

The GAP and GUROBI code used in [25] and the GAP code used in [36] (to compute the value $\sigma(S_{14})$) can be found in the Reference. Furthermore, in [19, Section 5.2] can be found a pseudocode that provide both upper and lower bounds for the covering number.

Let us now recall some results about $\sigma(S_n)$, $\sigma(A_n)$, $\omega(S_n)$ and $\omega(A_n)$.

In [34] A. Maróti obtained an exact formula for $\sigma(S_n)$ for odd $n \neq 9$ and $\sigma(A_n)$ for $n \equiv 2 \pmod{4}$.

Theorem (A. Maróti, 2005). *Let $n > 3$, and let S_n and A_n be the symmetric and the alternating group, respectively, on n letters.*

- (1) *We have $\sigma(S_n) = 2^{n-1}$ if n is odd unless $n = 9$, and $\sigma(S_n) \leq 2^{n-2}$ if n is even.*
- (2) *If $n \neq 7, 9$, then $\sigma(A_n) \geq 2^{n-2}$ with equality if and only if $n \equiv 2 \pmod{4}$.*

In [25] L.-C. Kappe, D. Nikolova-Popova, and E. Swartz proved the following.

Theorem (L.-C. Kappe, D. Nikolova-Popova, E. Swartz, 2016). *$\sigma(S_9) = 2^{9-1}$. In particular, Maróti's formula $\sigma(S_n) = 2^{n-1}$ holds for all odd integers $n \geq 3$. Moreover $\sigma(S_8) = 64$, $\sigma(S_{10}) = 221$, $\sigma(S_{12}) = 761$, $\sigma(M_{12}) = 208$, and $5316 \leq \sigma(J_1) \leq 5413$.*

In [6] S. R. Blackburn proved that $\sigma(S_n) = \omega(S_n)$ if n is odd and sufficiently large.

Theorem (S. R. Blackburn, 2006). *For all sufficiently large odd integers n , $\omega(S_n) = 2^{n-1}$.*

Later in [39] L. Stringer proved the following.

Theorem (L. Stringer, 2008). *Let n be a positive integer larger than 2.*

- (1) *If n is odd and different from 5, 9 or 15, then $\omega(S_n) = 2^{n-1}$.*
- (2) *$\omega(S_5) = 13 < 16 = 2^{5-1} = \sigma(S_5)$, and $235 \leq \omega(S_9) \leq 244 < 256 = 2^{9-1} = \sigma(S_9)$.*
- (3) *If $n \equiv 2 \pmod{4}$ and n is different from 6, 10, 14 or 18, then $\omega(A_n) = 2^{n-2}$.*
- (4) *$\omega(A_6) = 11 < 16 = 2^{6-2}$.*

It is not known wheter $\omega(S_{15})$ equals $\sigma(S_{15})$ or not. In an unpublished paper, E. Swartz proved the following.

Theorem (E. Swartz, unpublished). *We have $\omega(A_{10}) = 256 = 2^8$, $\omega(A_{11}) = 2734$, $\omega(M_{12}) = 144$, $\omega(M_{22}) = 771$, $\omega(J_1) = 5121$, $\omega(J_2) = 907$ and $\omega(S_9) \in \{240, 241\}$.*

In the next tables we show some values of these invariants calculated for symmetric and alternating groups G of small order.

G	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
$\sigma(G)$	4	4	16	13	64	64	256	221
$\omega(G)$	4	4	13	11	64	64		191

Table 1: Comparing $\sigma(G)$ and $\omega(G)$ for some symmetric groups.

with

$$240 \leq \omega(S_9) \leq 241.$$

G	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}
$\sigma(G)$	5	10	16	31	71	157	256	2751
$\omega(G)$	5	8	11	27	71	125	256	2734

Table 2: Comparing $\sigma(G)$ and $\omega(G)$ for some alternating groups.

We also want to mention that $\omega(G)$ was calculated in [29] when $G = \text{PSL}(2, q)$ with q odd and when G is a Suzuki group $\text{Suz}(q)$.

About $\omega(S_n)$ for even n , F. Fumagalli, M. Garonzi and A. Maróti [15] proved the following result.

Theorem (F. Fumagalli, M. Garonzi, A. Maróti, 2022). *If n is even then $\sigma(S_n)$ and $\omega(S_n)$ are asymptotically equal to $\frac{1}{2}\binom{n}{n/2}$.*

This, together with S. R. Blackburn's result mentioned above, implies that the quotient $\omega(S_n)/\sigma(S_n)$ tends to 1 as n tends to infinity, without restrictions on the parity of n .

The alternating and symmetric groups are examples of a broad family of groups called primitive groups. Let $H \leq G$, the normal core of H in G is defined by

$$H_G = \bigcap_{g \in G} H^g = \bigcap_{g \in G} g^{-1}Hg.$$

A group G is called primitive if it admits a maximal subgroup with trivial normal core. If M is a maximal subgroup of G then G/M_G is a primitive group, since its subgroup M/M_G is maximal and it has trivial normal core. A normal subgroup N of G is called a minimal normal subgroup of G if $N \neq \{1\}$ and N does not properly contain any nontrivial normal subgroup of G . Recall that any minimal normal subgroup of G is isomorphic to a direct power of a simple group. The socle $\text{soc}(G)$ of a group G is the subgroup of G generated by the minimal normal subgroups of G . A group with a unique minimal normal subgroup is called monolithic. If G is primitive, then either G is monolithic or it contains precisely two minimal normal subgroups (See Theorem 4).

Recall that the Frattini subgroup of G , denoted $\Phi(G)$, is the intersection of all the maximal subgroups of G . For a general G , we have $\sigma(G) = \sigma(G/\Phi(G))$ and, if G is 2-generated, $\omega(G) = \omega(G/\Phi(G))$. Indeed, generation can be determined modulo $\Phi(G)$ and we can lift a covering consisting of maximal subgroups.

A subdirect product of a family of groups $\{X_1, \dots, X_n\}$ is a subgroup H of $X_1 \times \dots \times X_n$ such that the restrictions to H of the projections

$\pi_i|_H : H \rightarrow X_i$ are surjective. Observe that $G/\Phi(G)$ is a subdirect product of primitive groups, each of which is a quotient of G , since denoting with \mathcal{M} the family of all maximal subgroups of G , the natural map

$$G \rightarrow \prod_{M \in \mathcal{M}} G/M_G$$

has kernel equal to $\Phi(G)$. Therefore the study of $\sigma(G)$ and of $\omega(G)$ when G is a primitive group is crucial for the understanding of the general behaviour of these invariants.

Note that if N is a normal subgroup of a group G then $\sigma(G) \leq \sigma(G/N)$. Indeed, every covering of G/N can be lifted to a covering of 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 to the following definition.

Definition. *A finite noncyclic group G is called σ -elementary if $\sigma(G) < \sigma(G/N)$ for every non-trivial normal subgroup N of G .*

This definition was given in [11] but there such groups were called “ σ -primitive”. The terminology “ σ -elementary” was used in [19]. For example, any finite nonabelian simple group is σ -elementary (for obvious reasons) and the symmetric group S_n is σ -elementary for all $n \geq 3$, $n \neq 4$. More generally, if G is a noncyclic finite group such that every proper quotient of G is cyclic, then G is σ -elementary. This is an interesting notion for the following reason: if G is any finite non-cyclic group, there exists $N \trianglelefteq G$ such that $\sigma(G) = \sigma(G/N)$ and G/N is σ -elementary. To see this, consider the family \mathcal{F} consisting of the normal subgroups N of G with the property that $\sigma(G) = \sigma(G/N)$ and let N be a member of \mathcal{F} of maximal order. Then $\sigma(G) = \sigma(G/N)$ and of course $\sigma(G/N)$ is σ -elementary. An immediate consequence of this is the following observation: if we denote by \mathcal{G} the class of all finite noncyclic groups and by \mathcal{S} the class of all σ -elementary groups, then

$$\{\sigma(G) : G \in \mathcal{G}\} = \{\sigma(G) : G \in \mathcal{S}\}.$$

An interesting open question is the following: are there infinitely many natural numbers not belonging to the above set?

The σ -elementary groups were studied by E. Detomi and A. Lucchini in [11]. They conjectured that:

Conjecture (E. Detomi, A. Lucchini, 2008). *Every non-abelian σ -elementary group is primitive and monolithic.*

This was confirmed in [19, Theorem 4.5] for σ -elementary groups G with $\sigma(G) \leq 129$.

This conjecture suggests that it makes sense to consider primitive monolithic groups that are σ -elementary and to compute $\sigma(G)$ for such groups G . Note that deciding whether a primitive monolithic group G is σ -elementary is hard in general, but it is certainly true if $G/\text{soc}(G)$ is cyclic. In other words, every primitive monolithic group G with $G/\text{soc}(G)$ cyclic is σ -elementary. So, this is the first case to consider.

Let us consider a primitive monolithic group G , with $N = \text{soc}(G) \cong T_1 \times \dots \times T_m \cong T^m$, where $T_i \cong T$ for $i = 1, \dots, m$, T a non-abelian simple group, and G/N is cyclic. Since every proper quotient of G is cyclic, G is a σ -elementary group. Let now n, m be positive integers with $n \geq 5$ and suppose that $T = A_n$, i. e., $\text{soc}(G) = A_n^m$. Define $X = N_G(T_1)/C_G(T_1)$. This is a group isomorphic to a subgroup of $\text{Aut}(T)$ containing an isomorphic copy of T as a normal subgroup. If $n \neq 6$, then $\text{Aut}(A_n) \cong S_n$, therefore either $X \cong A_n$ (“even case”) or $X \cong S_n$ (“odd case”). In the even case $G \cong A_n \wr C_m$, and these groups have been studied in [20] by M. Garonzi and A. Maróti obtaining lower and upper bounds for $\sigma(G)$ and its exact value in the case $n \equiv 2 \pmod{4}$. The odd case is the group $G_{n,m}$ and will be defined below.

Let $G = G_{n,m}$ be the semidirect product $A_n^m \rtimes \langle \gamma \rangle$ where $\gamma = (1, \dots, 1, \tau)\delta \in S_n \wr S_m$, with $\tau = (1\ 2)$ and $\delta = (1 \dots m)$. If $x_1, \dots, x_m \in A_n$, we have

$$(x_1, \dots, x_m)^\gamma = (x_m^\tau, x_1, \dots, x_{m-1}).$$

The group $G_{n,m}$ is a generalization of the Symmetric Group S_n , if $m = 1$ then $G = A_n \rtimes \langle (1\ 2) \rangle \cong S_n$.

In [17] M. Garonzi obtained an exact formula for $\sigma(G)$ when n is odd with some exceptions, and an asymptotic formula when n is even.

Theorem (M. Garonzi, 2013). *Let m, n be positive integers, and let $G = G_{m,n}$. Let $\alpha(x)$ denote the number of prime factors of the positive integer*

x. The following holds:

(1) Suppose that $n \geq 7$ is odd and $m \neq 1$ if $n = 9$. Then

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

(2) If $n = 5$, then

$$10^m \leq \sigma(G) \leq \alpha(2m) + 5^m + 10^m.$$

(3) Suppose that $n \geq 8$ is even. Then

$$\left(\frac{1}{2} \binom{n}{n/2}\right)^m \leq \sigma(G) \leq \alpha(2m) + \left(\frac{1}{2} \binom{n}{n/2}\right)^m + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}^m.$$

In particular, $\sigma(G) \sim \left(\frac{1}{2} \binom{n}{n/2}\right)^m$ as $n \rightarrow \infty$.

(4) If $n = 6$, then

$$\sigma(G) = \alpha(2m) + 2 \cdot 6^m.$$

In 2016, E. Swartz calculated $\sigma(S_n)$ when n is divisible by 6 (see [40]), which corresponds to the group $G_{n,m}$ when $m = 1$.

Theorem (E. Swartz, 2016). *Let $n \equiv 0 \pmod{6}$, $n \geq 24$. If $\sigma(S_n)$ denotes the covering number of S_n , then*

$$\sigma(S_n) = \frac{1}{2} \binom{n}{n/2} + \sum_{i=0}^{n/3-1} \binom{n}{i}.$$

Moreover,

$$\sigma(S_{18}) = \frac{1}{2} \binom{18}{9} + \sum_{i=0, i \neq 2}^5 \binom{18}{i} = 36773.$$

In each of these cases, the minimal covering using only maximal subgroups is unique.

Inspired by this result, we investigated the value of $\sigma(G)$ where $G = G_{n,m}$, n is divisible by 6 and $m > 1$. The first main results of this thesis concern this covering number, and it was published in [2]. We obtained an exact formula for $\sigma(G)$ when $n \geq 30$ and divisible by 6 and $m \geq 2$.

Theorem 1 (J. Almeida, M. Garonzi, 2023). *Let $G = G_{n,m}$, for $n \geq 30$ divisible by 6 and $m \geq 2$. Denote by $\alpha(x)$ the number of distinct prime factors of the positive integer x . Then*

$$\sigma(G) = \alpha(2m) + \left(\frac{1}{2} \binom{n}{n/2}\right)^m + \sum_{i=1}^{n/3-1} \binom{n}{i}^m.$$

Moreover, G has a unique minimal covering consisting of maximal subgroups.

We now consider the problem of determining the clique number of the generating graph of such groups. The fact that $G_{n,m}$ is 2-generated can be proved directly or with the help of the following theorem of A. Lucchini and F. Menegazzo [31].

Theorem (A. Lucchini, F. Menegazzo, 1997). *If G is noncyclic finite group with a unique minimal normal subgroup N , then $d(G) = \max\{2, d(G/N)\}$.*

This result implies that, if G is a primitive monolithic group and $G/\text{soc}(G)$ is cyclic, then $d(G) = 2$. So, in this case too, the first case to consider is the one in which G/N is cyclic, and we have seen that, if N is a direct power of an alternating group, then G must be one of the two types of groups discussed above (the even type and the odd type). As in Theorem 1, we concentrate on the odd type. Let $G := G_{n,m}$ and assume n is even. Two explicit generators of $G_{n,m}$ are $\alpha_i = (x_i, 1, \dots, 1)\gamma$ for $i = 1, 2$, where $x_1, x_2 \in A_n$ and $\langle x_1\tau, x_2\tau \rangle = S_n$ (see Section 2.3.4 for more details).

The second main result of this thesis, published in [2], is the following. It gives an asymptotic formula for $\omega(G)$ when n is even and tends to infinity.

Theorem 2 (J. Almeida, M. Garonzi, 2023). *Set $G := G_{n,m}$. For fixed $m \geq 1$, $\omega(G)$ is asymptotically equal to*

$$\left(\frac{1}{2} \binom{n}{n/2}\right)^m$$

for $n \rightarrow \infty$, n even. Moreover $\omega(G)/\sigma(G)$ tends to 1 as $n \rightarrow \infty$, n even.

This is a generalization of [15, Theorem 1], which deals with $m = 1$. Note that the second statement of the theorem follows from the first one using item (3) from M. Garonzi's theorem above. Specifically, we achieve the above asymptotic formula by proving that, if n is sufficiently large, then

$$\left(\frac{1}{2}\binom{n}{n/2}\right)^m \leq \omega(G) \leq \sigma(G) \leq \alpha(2m) + \left(\frac{1}{2}\binom{n}{n/2}\right)^m + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}^m.$$

It would be interesting to investigate exactly how large n should be for the lower bound to hold for all $m \geq 1$ (the upper bound always holds). This would settle the question of whether $\omega(G)/\sigma(G)$ tends to 1 as $|G| \rightarrow \infty$.

A coclique of a graph Γ is an empty subgraph of Γ , i.e. a full subgraph without edges.

Definition. *The chromatic number of the generating graph of G , denoted by $\chi(G)$, is the least number of colors needed to color the vertices of the graph in such a way that the endpoints of each edge receive different colors.*

Observe that a coloring as above corresponds to writing the vertex set as a union of cocliques. This means that $\chi(G)$ is the ‘‘coclique covering number’’ of G , i.e. the smallest number of cocliques (of the generating graph) whose union is G . We have

$$\omega(G) \leq \chi(G) \leq \sigma(G),$$

where the first inequality follows from the fact that the intersection between a clique and a coclique has size at most 1 and the second inequality follows from the fact that the proper subgroups of G are cocliques of the generating graph. It is very natural to ask whether equalities among $\omega(G)$, $\chi(G)$, $\sigma(G)$ occur for some families of groups, at least asymptotically.

In [30] A. Lucchini and A. Maróti proved:

Theorem (A. Lucchini, A. Maróti, 2009). *Let G be a 2-generated finite group with Fitting height at most 2, in other words there exists a nilpotent normal subgroup N of G such that G/N is nilpotent. Then $\omega(G) = \chi(G)$. Moreover, if G is noncyclic, then $\omega(G) = \sigma(G)$.*

In the case of Suzuki groups $\text{Suz}(q)$ where $q = 2^{2m+1}$, M. S. Lucido [32] calculated $\sigma(\text{Suz}(q))$, and A. Lucchini and A. Maróti [29] calculated $\omega(\text{Suz}(q))$ and $\chi(\text{Suz}(q))$.

$$\omega(\text{Suz}(q)) = q^4/2, \quad \chi(\text{Suz}(q)) = q^2(q^2+1)/2-1, \quad \sigma(\text{Suz}(q)) = q^2(q^2+1)/2.$$

Note that $\chi(\text{Suz}(q)) = \sigma(\text{Suz}(q)) - 1$.

About linear groups, A. Lucchini and A. Maróti [29] the following result:

Theorem (A. Lucchini, A. Maróti, 2009). *Let $q > 9$ be an odd prime power. Let G be any of the groups $\text{PSL}(2, q)$, $\text{SL}(2, q)$. Then $\omega(G) = \chi(G) = \sigma(G) = (q(q+1)/2) + 1$.*

And in [7], J. R. Britnell et al. proved the following:

Theorem (J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, A. Maróti, 2008). *Let G be any of the groups $(P)GL(n, q)$, $(P)SL(n, q)$. Let b be the smallest prime factor of n , and let $N(b)$ be the number of proper subspaces of $V = \mathbb{F}_q^n$ of dimensions not divisible by b . If $n \geq 12$, then*

$$\omega(G) = \frac{1}{b} \prod_{\substack{i=1, \\ b \nmid i}}^{n-1} (q^n - q^i) + \lfloor N(b)/2 \rfloor.$$

We have seen that, in general, $\sigma(G)$ and $\omega(G)$ are not equal, however it is still interesting to ask whether the quotient $\omega(G)/\sigma(G)$ tends to 1 when $|G|$ tends to infinity. In general, this is false: in [30] A. Lucchini and A. Maróti show an interesting example of a family of groups G for which $\omega(G)/\sigma(G)$ tends to 0. However, it is reasonable to expect that $\omega(G)/\sigma(G)$ tends to 1 when G varies in the family of nonabelian simple groups. This was conjectured by S. R. Blackburn in [6]:

Conjecture (S. R. Blackburn, 2006). *Let G vary in the family of nonabelian simple groups. Then $\omega(G)/\sigma(G)$ tends to 1 when $|G| \rightarrow \infty$.*

Of course, in order to attack this conjecture, it makes sense to prove it for G varying in specific families \mathcal{F} of simple groups. In [7] the authors

show that Blackburn's conjecture holds for projective special linear groups. In [14], F. Fumagalli, M. Garonzi and P. Gheri proved the conjecture for the family of alternating groups of composite degree.

Combining [15] and [6] we see that $\omega(S_n)/\sigma(S_n) \rightarrow 1$ if $n \rightarrow \infty$. It is natural to expect that S. R. Blackburn's conjecture should hold for more general families of groups, for example the monolithic primitive groups. For instance, it is natural to expect that $\omega(G_{n,m})/\sigma(G_{n,m})$ tends to 1 for fixed m and for $n \rightarrow \infty$. We did this for n even. In the case n odd, this is very probably true.

Chapter 1

Preliminaries

In this chapter we present definitions and results that are important throughout the text.

1.1 Primitive groups

Let G be a finite group acting on the set X , and denote the action by $(x, g) \mapsto x^g$. Such action is said to be transitive if for every $x, y \in X$ there exists $g \in G$ such that $x^g = y$. For $x \in X$, we define

$$\text{Stab}_G(x) = \{g \in G : x^g = x\} \leq G$$

the stabilizer of x and

$$O_G(x) = \{x^g : g \in G\} \subseteq X$$

the G -orbit of x . Equivalently, the action is transitive if X is the unique orbit.

Giving an action of G on X is equivalent to giving a group homomorphism

$$\begin{aligned} \gamma : G &\longrightarrow \text{Sym}(X) \\ g &\longmapsto \gamma_g : X \longrightarrow X \\ &\quad x \longmapsto x^g. \end{aligned}$$

The kernel of this homomorphism is

$$\begin{aligned} \text{Ker}(\gamma) &= \{g \in G : \gamma_g = id_X\} = \{g \in G : \gamma_g(x) = x, \forall x \in X\} \\ &= \{g \in G : x^g = x, \forall x \in X\} = \bigcap_{x \in X} G_x. \end{aligned}$$

The kernel of the action is by definition equals to the kernel of the correspondent homomorphism $G \rightarrow \text{Sym}(X)$. An action is said to be faithful if it has trivial kernel.

A partition of X is a family $\mathcal{P} = \{B_1, \dots, B_k\}$ of non-empty proper subsets of X such that $B_1 \cup \dots \cup B_k = X$ and $B_i \cap B_j = \emptyset$ whenever $i \neq j$. The trivial partitions of X are $\{X\}$ and $\{\{x\} : x \in X\}$. We say that G stabilizes the partition \mathcal{P} if $B_i^g \in \mathcal{P}$ for every $g \in G$ and for every $i \in \{1, \dots, k\}$. An example of stabilized partition is given by the G -orbits, and such partition is not $\{X\}$ if the action of G is intransitive. Assume now that the action of G on X is transitive and that it stabilizes a partition $\mathcal{P} = \{B_1, \dots, B_k\}$. Then G acts on \mathcal{P} by $(B_i, g) \mapsto B_i^g$, and this action is transitive. In fact, if $B_i, B_j \in \mathcal{P}$ and $x \in B_i, y \in B_j$ then there exists $g \in G$ such that $x^g = y$, so $y \in B_i^g \cap B_j$. But B_i^g and B_j are members of the partition \mathcal{P} , so the fact that $B_i^g \cap B_j \neq \emptyset$ implies that $B_i^g = B_j$.

The action of G on X is said to be primitive if it is transitive and no nontrivial partition of X is stabilized by G , in other words for every partition \mathcal{P} of X that is not trivial and for every $g \in G$ we have

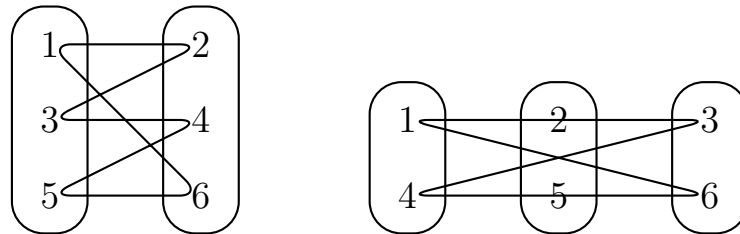
$$\{B^g : B \in \mathcal{P}\} \neq \mathcal{P}.$$

Since the partition consisting of the orbits is always stabilized, in the definition of primitive action the assumption that the action is transitive is superfluous unless $|X| = 2$, and in this case the trivial action $(x, g) \mapsto x^g = x$ does not stabilize nontrivial partitions since all partitions are trivial. If the action of G on X is not primitive and P is a G -invariant partition of X , then the parts of P are called blocks of imprimitivity.

Lemma 1. *Let the group G act transitively on the set X , and assume $|X| > 2$. Such action is not primitive if and only if there exists a subset A of X such that $|A| \geq 2$ and whenever $g \in G$, either $A^g = A$ or $A^g \cap A = \emptyset$. Such an A is called imprimitivity block for the action of G on X .*

Proof. Let us assume that the action is not primitive, and let \mathcal{P} be a nontrivial G -invariant partition. Since this partition is not trivial, there exists $A \in \mathcal{P}$ such that $|A| \geq 2$ and $A \neq X$. Since the partition is stabilized, the claim follows. Conversely, let us assume that there exists A as in the statement. Then the family $\{A^g : g \in G\}$ is a partition of X stabilized by G . \square

Example. Consider $X = \{1, 2, 3, 4, 5, 6\}$, $\sigma = (123456) \in S_6$ and $G = \langle \sigma \rangle < S_6$, as a permutation group of degree 6. Since $\sigma^2 = (135)(246)$ and $\sigma^3 = (14)(25)(36)$, X has precisely two G -invariant partitions, namely $\{\{1, 3, 5\}, \{2, 4, 6\}\}$ and $\{\{1, 4\}, \{2, 5\}, \{3, 6\}\}$. As the following picture shows, the cycle (123456) acts as a 2-cycle on the first partition and as a 3-cycle on the second.



A group G acting on X is called faithfully primitive on X if its action on X is faithful and primitive. In this case, the cardinality of X is called a primitivity degree of G .

Proposition 1. [5, Proposition 1.1.2] *Let G be a group acting on a set X and $x \in X$. If the action is transitive, then there is a bijection between*

$$\{ \text{block } B \text{ of } X : x \in B \} \rightarrow \{ H \leq G : \text{Stab}_G(x) \leq H \}$$

which preserves containments.

Proof. Given a block B in X such that $x \in B$, then $G_B = \{g \in G : B^g = B\}$ is a subgroup of G and the stabiliser $\text{Stab}_G(x)$ is a subgroup of G_B . Conversely, if H is a subgroup of G containing $\text{Stab}_G(x)$ then the set $B = \{x^h : h \in H\}$ is a block and $x \in B$. These are the mutually inverse bijections required. \square

Let $H \leq G$, the normal core of H in G is defined by

$$H_G = \bigcap_{g \in G} H^g.$$

Theorem 3. [5, Theorem 1.1.5] *Let G be a group. The following conditions are equivalent:*

1. G possesses a faithful transitive permutation representation with no nontrivial blocks;
2. there exists a core-free maximal subgroup of G .

Proof. 1 implies 2: Suppose that there exists a transitive G -set X with no non-trivial blocks and consider any $x \in X$. The action of G on X is equivalent to the action of G on the set of right cosets of $Stab_G(x)$ in G (see [24, Theorem 1.10]). The kernel of this action is the normal core $(Stab_G(x))_G$ and, by hypothesis, is trivial. By Proposition 1 if H is a subgroup of G containing $Stab_G(x)$, there exists a block $B = \{x^h : h \in H\}$ of X such that $x \in B$ and $H = G_B = \{g \in G : B^g = B\}$. Since G has no non-trivial blocks, either $B = \{x\}$ or $B = X$. If $B = \{x\}$, then $Stab_G(x) = H$ and if $B = X$, then $H = G$. Hence the stabiliser $Stab_G(x)$ is a core-free maximal subgroup of G .

2 implies 1: If U is a core-free maximal subgroup of G , then the action of G on the set of right cosets of U in G is faithful and transitive. By maximality of U , this action has no non-trivial blocks by Proposition 1. \square

The primitivity degrees of an abstract group G are the indices of the maximal subgroups of G with trivial normal core.

Definition 1. *We say that a group is primitive if it admits a faithful primitive action. Equivalently, G is primitive if and only if there exists a maximal subgroup M of G with $M_G = \{1\}$.*

Lemma 2. *Let G be a group.*

1. Let $N \trianglelefteq G$. If $N \leq H \leq G$, then $(H/N)_{G/N} = H_G/N$.

2. If M is a maximal subgroup of G , then G/M_G is primitive.

Proof. 1.

$$(H/N)_{G/N} = \bigcap_{gN \in G/N} (H/N)^{gN} = \bigcap_{g \in G} H^g/N = (\bigcap_{g \in G} H^g)/N = H_G/N.$$

2. Since M is maximal in G , M/M_G is maximal in G/M_G . By the previous item, $(M/M_G)_{G/M_G} = M_G/M_G$, that is, M/M_G has trivial core in G/M_G .

□

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

A nontrivial subgroup N of a group G is called a minimal normal subgroup if it is normal and for any normal subgroup K of G such that $K \leq N$, either $K = N$ or K is trivial.

The socle of a group G , denoted by $\text{soc}(G)$, is the subgroup generated by the minimal normal subgroups of G . If $\text{soc}(G)$ is a minimal normal subgroup of G , then it is the unique minimal normal subgroup of G . A group admitting a unique minimal normal subgroup is usually called monolithic. The next theorem was proved by R. Baer and in this result the primitive groups are classified in terms of their socle.

Theorem 4. [5, Theorem 1.1.7] *Let G be a finite group.*

1. G is primitive if and only if there exists a proper subgroup U of G such that $UN = G$ whenever N is a nontrivial normal subgroup of G .
2. Let G be a primitive group. Assume that M is a core-free maximal subgroup of G and that N is a nontrivial normal subgroup of G . Then $C_G(N) \cap M = \{1\}$, moreover either $C_G(N) = \{1\}$ or $C_G(N)$ is a minimal normal subgroup of G .

3. If G is a primitive group and M is a core-free maximal subgroup of G , then exactly one of the following statements holds:
- (a) $\text{soc}(G)$ is an abelian minimal normal subgroup of G complemented by M . In this case G is called affine or primitive of type I.
 - (b) $\text{soc}(G)$ is a nonabelian minimal normal subgroup of G supplemented by M . In this case G is called primitive of type II.
 - (c) G admits precisely two minimal normal subgroups A, B and $\text{soc}(G) = A \times B$. Moreover A and B are nonabelian, $A = C_G(B)$, $B = C_G(A)$, M complements both A and B in G and $A \cong AB \cap M \cong B$. In this case G is called primitive of type III.

Proof. 1. If G is primitive and M is a core-free maximal subgroup of G then M does not contain any nontrivial normal subgroup of G and $M < MN \leq G$ for all $N \trianglelefteq G$, therefore $MN = G$ for all $\{1\} \neq N \trianglelefteq G$. Conversely if G is a finite group and the proper subgroup U of G satisfies $UN = G$ whenever N is a nontrivial normal subgroup of G then let M be a maximal subgroup of G containing U . We have $M_G = \{1\}$, because otherwise, since $M_G \trianglelefteq G$, we would have $G = UM_G \leq M$, a contradiction. So G is primitive.

2. Let G be primitive and let M be a core-free maximal subgroup of G . If N is a nontrivial normal subgroup of G then $C_G(N)$ is the kernel of the conjugation action $G \rightarrow \text{Aut}(N)$, hence $C_G(N) \trianglelefteq G$, therefore $M \cap C_G(N) \trianglelefteq M$, so M is contained in the normalizer $N_G(M \cap C_G(N))$. But N is also contained in such normalizer, hence $G = MN \leq N_G(M \cap C_G(N))$ which implies that $M \cap C_G(N) \trianglelefteq G$. Since $M_G = \{1\}$, we deduce that $M \cap C_G(N) = \{1\}$. If $C_G(N) \neq \{1\}$ then, since G is finite, there exists a minimal normal subgroup X of G contained in $C_G(N)$. Since $M_G = \{1\}$ we have $XM = G$. By Dedekind's law

$$C_G(N) = C_G(N) \cap G = C_G(N) \cap XM = X(C_G(N) \cap M) = X.$$

This implies that $C_G(N)$ is a minimal normal subgroup of G .

3. Let G be primitive and let M be a core-free maximal subgroup of G . If G admits three distinct minimal normal subgroups A, B, C then

B, C are contained in $C_G(A)$ being $A \cap B = \{1\}$ and $A \cap C = \{1\}$ and this contradicts the fact that $C_G(A)$, if nontrivial, is a minimal normal subgroup of G . This proves that G admits at most two minimal normal subgroups.

Assume first that G contains only one minimal normal subgroup, call it N . Since M is a core-free maximal subgroup, $MN = G$. If N is nonabelian then G is a primitive group of type II and $C_G(N) = \{1\}$. Assume now that N is abelian. Then $N \leq C_G(N)$ and, since $C_G(N)$ is a minimal normal subgroup of G , we deduce that $C_G(N) = N$. This implies that $M \cap N = M \cap C_G(N) = \{1\}$, in other words M is a complement for N in G hence G is a primitive group of type I.

Finally assume that G contains precisely two minimal normal subgroups, A and B . Clearly $\text{soc}(G) = A \times B$. The fact that $A \cap B = \{1\}$ implies that $A \leq C_G(B)$ and $B \leq C_G(A)$, so since $C_G(A)$ and $C_G(B)$ are minimal normal subgroups of G , we deduce that $A = C_G(B)$ and $B = C_G(A)$. In particular A and B are nonabelian. Moreover $M \cap A = M \cap C_G(B) = \{1\}$ and $M \cap B = M \cap C_G(A) = \{1\}$, so M complements both A and B in G . By Dedekind's law,

$$A(AB \cap M) = AB \cap AM = AB \cap G = AB,$$

$$B(AB \cap M) = AB \cap BM = AB \cap G = AB,$$

therefore

$$A \cong A/A \cap B \cong AB/B = B(AB \cap M)/B \cong AB \cap M,$$

$$B \cong B/A \cap B \cong AB/A = A(AB \cap M)/A \cong AB \cap M.$$

It follows that $A \cong AB \cap M \cong B$.

□

Since we focus on monolithic primitive groups with non-abelian socle, we are interested in primitive groups of type II. According to Baer's Theorem, the socle of a primitive group of type II is a non-abelian minimal normal subgroup. A non-abelian minimal normal subgroup N of a finite group G is a direct product of copies of a non-abelian simple group S , i. e., there is a positive integer m with $N = S^m$ [23, Chapter I, Theorem 9.12].

Proposition 2. *Let G be a finite group. The following are equivalent.*

1. G is primitive of type II.
2. There exists a minimal normal subgroup N of G such that $C_G(N) = \{1\}$.
3. There exists a nonabelian minimal normal subgroup N of G such that, up to isomorphism, $N \leq G \leq \text{Aut}(N)$, where N is embedded in $\text{Aut}(N)$ via the natural conjugation action $G \rightarrow \text{Aut}(N)$.

Proof. By Baer's theorem, (1) implies (2). If (2) holds then the conjugation action $G \rightarrow \text{Aut}(N)$ has kernel $C_G(N) = \{1\}$, so (3) follows. If (3) holds then any element of the centralizer $C_G(N)$ is an automorphism of N fixing N pointwise, hence $C_G(N) = \{1\}$ and (2) follows.

We are left to prove that (2) implies (1). The Frattini subgroup of G is nilpotent, however N is not nilpotent being a direct product of nonabelian simple groups. Since every subgroup of a nilpotent group is nilpotent, this implies that there exists a maximal subgroup M of G not containing N . In particular N is not contained in the normal core M_G of M in G . The intersection $N \cap M_G$ is normal in G and contained in N , so since N is a minimal normal subgroup, $N \cap M_G = \{1\}$. This implies that $M_G \leq C_G(N) = \{1\}$, hence $M_G = \{1\}$. Moreover, N is the unique minimal normal subgroup of G since any other minimal normal subgroup would be contained in $C_G(N) = \{1\}$. This proves that G is primitive of type II. \square

Definition 2. *A group G is said to be almost-simple if it admits a nonabelian simple normal subgroup S such that $C_G(S) = \{1\}$. In this case, S coincides with the socle of G .*

For $n \geq 5$, S_n is an almost simple group. In fact, for $n \geq 5$, A_n is a nonabelian simple normal subgroup of S_n such that $C_{S_n}(A_n) = \{1\}$.

If G is an almost-simple group with socle S , then the canonical map $G \rightarrow \text{Aut}(S)$ is injective, therefore G can be thought of as a subgroup of $\text{Aut}(S)$ containing the isomorphic copy of S which is the image of the canonical map $S \rightarrow \text{Aut}(S)$. In other words, we may assume that $S \trianglelefteq G \leq \text{Aut}(S)$.

$\text{Aut}(S)$. This shows that the group G is almost-simple if and only if there exists a nonabelian simple group S such that G is isomorphic to a subgroup of $\text{Aut}(S)$ containing S (where we identify S with a subgroup of $\text{Aut}(S)$ via the canonical map $S \rightarrow \text{Aut}(S)$). In particular, if S is a nonabelian simple group, then $\text{Aut}(S)$ is almost-simple.

By Proposition 2, an almost simple group is a primitive group of type II.

Definition 3. Let H and K be two groups and $K \leq S_n$. The wreath product $H \wr K$ is the semidirect product $H^n \rtimes K$, where H^n is the direct product of n copies of H , and K acts on H^n by permuting the coordinates. More specifically, $\pi \in K$ acts on H^n by

$$(h_1, \dots, h_n)^\pi = (h_{1\pi^{-1}}, \dots, h_{n\pi^{-1}})$$

for each $h_i \in H$, $i = 1, \dots, n$.

Let's show that this action is a group action. If $\pi, \tau \in K$, defining $t_i = h_{i\pi^{-1}}$ we have

$$t_{i\tau^{-1}} = h_{i\tau^{-1}\pi^{-1}} = h_{i(\pi\tau)^{-1}},$$

then

$$((h_1, \dots, h_n)^\pi)^\tau = (h_{1\pi^{-1}}, \dots, h_{n\pi^{-1}})^\tau = (h_{1(\pi\tau)^{-1}}, \dots, h_{n(\pi\tau)^{-1}}) = (h_1, \dots, h_n)^{\pi\tau}.$$

The subgroup H^n is said to be the base of the group $H \wr K$. Note that $|H \wr K| = |H|^n |K|$.

The following result is due to Frobenius.

Theorem 5 (Embedding Argument). Let H be a subgroup of the finite group G , let x_1, \dots, x_n be a right transversal for H in G , and let ξ be any homomorphism with domain H , say $\xi : H \rightarrow X$. Then the map

$$f : G \rightarrow \xi(H) \wr S_n,$$

$$x \mapsto (\xi(x_1 x x_{1\pi}^{-1}), \dots, \xi(x_n x x_{n\pi}^{-1}))\pi,$$

where $\pi \in S_n$ is the unique permutation that satisfies $x_i x \in H x_{i\pi}$ for all $i = 1, \dots, n$, is a well-defined homomorphism with kernel equal to the normal core of $\ker \xi$ in G , in other words $\ker f = (\ker \xi)_G$.

Proof. Since $x_i \in Hx_i$ the permutation corresponding to the identity is 1 hence $f(1) = 1$. Now let $x, y \in G$ and assume $x_i x x_{i\pi}^{-1} \in H$, $x_i y x_{i\tau}^{-1} \in H$ for all $i \in I = \{1, \dots, n\}$, then applying the second to $i\pi$ we find $x_{i\pi} y x_{i\pi\tau}^{-1} \in H$ for all $i \in I$, so $x_i x y x_{i\pi\tau}^{-1} = (x_i x x_{i\pi}^{-1})(x_{i\pi}^{-1} y x_{i\pi\tau}^{-1}) \in H$. It follows that the permutation corresponding to xy is $\pi\tau$ and

$$\begin{aligned} f(xy) &= (\xi(x_i x y x_{i\pi\tau}^{-1}))_{i \in I\pi\tau} = (\xi(x_i x x_{i\pi}^{-1}) \xi(x_{i\pi}^{-1} y x_{i\pi\tau}^{-1}))_{i \in I\pi\tau} \\ &= f(x) \cdot \pi^{-1}(\xi(x_{i\pi} y x_{i\pi\tau}^{-1}))_{i \in I\pi\tau} = f(x) \cdot (\xi(x_i y x_{i\tau}^{-1}))_{i \in I\tau} = f(x)f(y). \end{aligned}$$

$f(x) = 1$ if and only if the permutation π corresponding to x is the identity and $x_i x x_i^{-1} \in \ker \xi$ for all $i \in I$, in other words $x \in x_i^{-1}(\ker \xi)x_i$ for all $i \in I$. Since $\ker \xi \trianglelefteq H$, the conjugates of $\ker \xi$ in G are precisely the groups $x_i^{-1}(\ker \xi)x_i$ for $i \in I$. This proves that $\ker f = (\ker \xi)_G$. \square

Proposition 3. *Let G be a finite group. Then the following are equivalent.*

1. G is primitive of type II.
2. There exists an almost-simple group X with socle S and a transitive group $K \leq S_m$ such that G is isomorphic to a subgroup of $X \wr K$ containing S^m and the restriction of the natural projection $G \rightarrow K$ is surjective.

Proof. Assume (2) holds. Let $S = \text{soc}(X)$, a nonabelian simple group. Then $N = S^m$ is a minimal normal subgroup of G since S is simple and K acts transitively on the components. We are left to check that $C_G(N) = \{1\}$. If $g \in C_G(N)$ then of course the permutational part of g is trivial since g must fix all the direct factors of N . So g has type (x_1, \dots, x_m) and x_i is an element of X centralizing S , so since $C_X(S) = \{1\}$ we deduce that $x_i = 1$ for all i .

Assume (1) holds. Let $N = T_1 \times \dots \times T_m$ be the socle of G , where the T_i 's are pairwise isomorphic nonabelian simple groups. Denote by R the first factor, $R := T_1 \times \{1\} \times \dots \times \{1\}$. Let $H := N_G(R)$ and $C := C_G(R) \trianglelefteq H$. Note that since $R \cong T_1$ is a nonabelian simple group, $R \cap C = \{1\}$. We claim that $X := H/C$ is an almost-simple group with socle RC/C . Clearly RC/C is a normal subgroup of H/C and $RC/C \cong R/R \cap C \cong R$

is nonabelian simple. We are left to show that $C_{H/C}(RC/C)$ is trivial. Assume that $h \in H$ is such that hC centralizes RC/C , in other words $hCrC = rChC$ for all $r \in R$, then $h^{-1}r^{-1}hr \in R \cap C = \{1\}$ for all $r \in R$ and this implies that $h \in C$, in other words $hC = C$.

We now apply the embedding argument to the natural homomorphism

$$\xi : H \rightarrow \text{Aut}(R).$$

Note that $\ker(\xi) = C$, $\xi(H) \cong H/C = X$ and the conjugates of C in G are precisely the centralizers of the direct factors of N , therefore an element belongs to the normal core $\ker(\xi)_G$ if and only if it centralizes all of the factors, in other words $\ker(\xi)_G = C_G(N) = \{1\}$. The group K is the image of the homomorphism $G \rightarrow S_m$ given by the conjugation action of G on the direct factors of N , which is transitive being N a minimal normal subgroup of G . \square

Proposition 4. *Let S a non-abelian simple group and write $S^n = S \times \dots \times S$, the direct product of n copies of S , for some positive integer n . Then the minimal normal subgroups of S^n are the $N_i = \{1\} \times \dots \times \{1\} \times S \times \{1\} \times \dots \times \{1\}$, where only the i -th coordinate is equal to S , for each $i = 1, \dots, n$.*

Proof. For each $i = 1, \dots, n$, the subgroups N_i are normal in S^n . Indeed, given $s = (s_1, \dots, s_n) \in S^n$ and $x = (1, \dots, x_i, \dots, 1) \in N_i$, we have

$$x^s = (1, \dots, x_i^{s_i}, \dots, 1) \in N_i.$$

Furthermore, the subgroups N_i are minimal normal in S^n . If there is $K_i \leq N_i$ with $K_i \triangleleft S^n$, the subgroup $K \leq S$ formed by the elements of the i -th coordinate of K_i is such that K is normal in the simple group S . Then either $K = \{1\}$ or $K = S$ and then either $K_i = \{1\} \times \dots \times \{1\}$ or $K_i = N_i$.

Let N be a minimal normal subgroup of S^n different from the N_i . Then $N \cap N_i = \{1\}$ for all $i = 1, \dots, n$. Since N and N_i are normal in S^n , we have $[N, N_i] \leq N \cap N_i = \{1\}$, and then N centralizes all the N_i and $N \leq Z(S^n) = \{1\} \times \dots \times \{1\}$, a contradiction. Therefore, the only minimal normal subgroups of S^n are the N_i , $i = 1, \dots, n$. \square

Proposition 5. [5, Proposition 1.1.20] *Let S be a non-abelian simple group and write $S^n = S_1 \times \dots \times S_n$ for the direct product of n copies S_1, \dots, S_n of S , for some positive integer n . Then $\text{Aut}(S^n) \cong \text{Aut}(S) \wr \text{Sym}(n)$, where $\text{Sym}(n)$ is the symmetric group of degree n .*

We are interested in the maximal subgroups of a primitive group of type II.

Definition 4. *Let $G = \prod_{i=1}^n S_i$ be a direct product of groups. A subgroup H of G is said to be diagonal if each projection $\pi_i : H \rightarrow S_i$ $i = 1, \dots, n$, is injective. If each projection $\pi_i : H \rightarrow S_i$ is an isomorphism, then the subgroup H is said to be a full diagonal subgroup.*

A reference for the following discussion is [5, Remark 1.1.40].

Let G be a primitive monolithic group with non-abelian socle $N = S^m$, and S a non-abelian simple group. For $i \in \{1, \dots, m\}$, let S_i be the subgroup of N equal to $\prod_{j=1}^m U_j$ where $U_i = S$ and $U_j = \{1\}$ for all $j \neq i$ (coordinate subgroup), so that $S_i \cong S$ for all i . Let H be a maximal subgroup of G such that $N \not\subseteq H$, then $HN = G$. Suppose that $N \cap H \neq \emptyset$. 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 $X := N_G(S_1)/C_G(S_1)$. X is an almost simple group with socle $S_1 C_G(S_1)/C_G(S_1) \cong S_1$. There are two possibilities for the intersection $N \cap H$:

1. Product type. Suppose the projections $H \rightarrow S_i$ are not surjective. Then there exists a subgroup M of S such that $N_X(M)$ supplements S in X and there exists elements $a_2, \dots, a_m \in S$ such that

$$H \cap N = M \times M^{a_2} \times \dots \times M^{a_m}.$$

2. Diagonal type. Suppose the projections $H \rightarrow S_i$ 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

$$H \cap N = \prod_{D \in \Delta} (H \cap N)^{\pi_D},$$

and for each $D \in \Delta$ the projection $(H \cap N)^{\pi_D}$ is a full diagonal subgroup of $\prod_{i \in D} S_i$.

1.2 Maximal subgroups of the Symmetric Group

A subgroup G of S_n is typically classified according to its action on $X = \{1, \dots, n\}$. If P is a property of a group action, for example transitive, a subgroup G of S_n is called P if its natural action on $X = \{1, \dots, n\}$ is P . We will use the word intransitive to mean not transitive.

Observe that if $G \leq S_n$ is intransitive then it has more than one orbit on X , and letting O be one of them, G is contained in

$$\text{Stab}_{S_n}(O) = \{g \in S_n : O^g = O\} \cong \text{Sym}(O) \times \text{Sym}(X \setminus O).$$

This is called a maximal intransitive subgroup of S_n . We will see such a subgroup is maximal in S_n unless $|O| = |X \setminus O|$. For this we use a reformulation of Jordan's Theorem [42, Theorem 13.9].

Proposition 6. *Let $G \leq S_n$ act primitively on $X = \{1, \dots, n\}$. If G contains a transposition then $G = S_n$. If G contains a 3-cycle then $G = A_n$ or $G = S_n$.*

Proposition 7. *Let O be a nonempty proper subset of $X = \{1, \dots, n\}$ and let $G := \text{Stab}_{S_n}(O)$. Then G is a maximal subgroup of S_n unless n is even and $|O| = n/2$.*

Proof. We study the maximality of G inside S_n . If G is not maximal then it is properly contained in $K \leq S_n$ which therefore is transitive on X . If K is primitive then it contains a 2-cycle, moving 2 elements of O or of $\bar{O} := X \setminus O$, and Jordan's Theorem implies that $K = S_n$.

Suppose now that K is imprimitive, let B be a nontrivial block for K . Then B is a nontrivial block for G , therefore $B \cap O$ is either empty or a block for G^O and $B \cap \bar{O}$ is either empty or a block for $G^{\bar{O}}$. Since $G^O \cong \text{Sym}(O)$ is primitive on O and $G^{\bar{O}} \cong \text{Sym}(\bar{O})$ is primitive on \bar{O} , we deduce that either $|B \cap O| \leq 1$ or $B \cap O = O$, furthermore either $|B \cap \bar{O}| \leq 1$ or $B \cap \bar{O} = \bar{O}$.

Assume $B \cap O = \{\alpha\}$, $B \cap \bar{O} = \{\beta\}$, then $B = \{\alpha, \beta\}$. If there exists $\gamma \in O - B$ then $g = (\alpha\gamma) \in G$ and $B^g = \{\beta, \gamma\}$, a contradiction, and similarly $\bar{O} - B = \emptyset$, so $X = B$ and $n = 2$, this contradicts the fact that B is nontrivial.

Assume $B \cap O = \{\alpha\}$, $B \supseteq \bar{O}$. Then $B = \{\alpha\} \cup \bar{O}$, however this is a contradiction because, since B is a nontrivial block, there exists $\beta \in O - B$, hence there exists $g \in G$ such that $\alpha g = \beta$ (being $G^O = \text{Sym}(O)$) so $B^g = \{\beta\} \cup \bar{O}$ is not disjoint from B and not equal to B .

We are left with the case in which one of $B \cap O$ and $B \cap \bar{O}$ is empty, say $B \cap O = \emptyset$. Then $B = \bar{O}$. Since K is transitive, there exists $k \in K$ that takes an element of \bar{O} to an element of O , hence $B^k \subseteq O$. But then $B^k = B^k \cap O$ is a block for $G^O = \text{Sym}(O)$, of size at least 2, hence $B^k = O$.

This proves that if O is a proper subset of X and $G = \text{Stab}(O) < \text{Sym}(X)$ is not a maximal subgroup then $|X| > 2$ and $|O| = |\bar{O}|$. In other words G has type $S_a \times S_a$ with $2a = n$. \square

Indeed, such subgroup is not maximal if $n > 2$: it is contained in an imprimitive wreath product $S_{n/2} \wr S_2$, the stabilizer of a partition with two parts of size $n/2$, which, as we will see, is a maximal subgroup of S_n .

If $a, b > 1$ and $ab = n$, then the full wreath product $S_a \wr S_b$ embeds into S_n as an imprimitive subgroup. To see this, it is enough to check that $S_a \wr S_b$ acts faithfully and imprimitively on the set $\{1, \dots, a\} \times \{1, \dots, b\}$, which is a set of size $ab = n$, by the rule

$$(i, j)^{(x_1, \dots, x_b)\sigma} := (ix_j, j\sigma).$$

This is an action since

$$(i, j)^{(x_1, \dots, x_b)\sigma \cdot (y_1, \dots, y_b)\tau} = (i, j)^{(x_1 y_{1\sigma}, \dots, x_b y_{b\sigma})\sigma\tau} = (ix_j y_{j\sigma}, j\sigma\tau),$$

is equals to

$$\left((i, j)^{(x_1, \dots, x_b)\sigma} \right)^{(y_1, \dots, y_b)\tau} = (ix_j, j\sigma)^{(y_1, \dots, y_b)\tau} = (ix_j y_{j\sigma}, j\sigma\tau).$$

This action is imprimitive admitting $B_j = \{1, \dots, a\} \times \{j\}$ as a block system, $j = 1, \dots, b$. Indeed,

$$B_j^{(x_1, \dots, x_b)\sigma} = B_j^\sigma = B_{j\sigma}.$$

The block system consists of b blocks of size a . The kernel of the action consists of the elements $(x_1, \dots, x_b)\sigma \in S_a \wr S_b$ such that

$$(i, j)^{(x_1, \dots, x_b)\sigma} = (ix_j, j\sigma) = (i, j),$$

for all $(i, j) \in \{1, \dots, a\} \times \{1, \dots, b\}$. This implies that $x_1 = \dots = x_b = 1$ and $\sigma = 1$, that is, the action is faithful. Therefore $S_a \wr S_b$ embeds into S_{ab} as an imprimitive subgroup.

Proposition 8. *Actually $S_a \wr S_b$ is a maximal imprimitive subgroup, meaning that it is not properly contained in any imprimitive subgroup of S_n . Moreover, every maximal imprimitive subgroup is conjugate in the symmetric group to $S_a \wr S_b$.*

Proof. Assume $G \leq S_n$ acts transitively and imprimitively on $X = \{1, \dots, n\}$. This means that there is a nontrivial imprimitivity block B for G , let $a = |B|$. Let $H = G_B = \{g \in G : B^g = B\}$, the setwise stabilizer of B . Observe that G acts transitively on the set of blocks $\{B^g : g \in G\}$ with H as point stabilizer, so $|G : H|$ equals the number of translates of B , call it b . Since the translates of B partition X we have $ab = n$. Of course we have a homomorphism

$$\xi : H \rightarrow \text{Sym}(B) \cong S_a$$

induced by the action of H on B . By Theorem 5 we deduce a homomorphism

$$f : G \rightarrow \xi(H) \wr S_b \leq S_a \wr S_b$$

with kernel the normal core of $\ker(\xi)$ in G . Observe that if $h \in \ker(\xi)$ then h fixes B pointwise, and if $h \in \ker(\xi)^g$ then $ghg^{-1} \in \ker(\xi)$ so h fixes B^g pointwise. This implies that $(\ker(\xi))_G = \{1\}$ hence f is injective. This means that G embeds in the wreath product $S_a \wr S_b$. On the other hand such wreath product embeds in S_n as an imprimitive subgroup with blocks of size a . This proves that the stabilizers in S_n of the partitions consisting of b blocks of size a , i.e. the maximal imprimitive subgroups of S_n with blocks of size a , are isomorphic to wreath products $S_a \wr S_b$. \square

Similarly, the maximal imprimitive subgroups of A_n with b blocks of size a are isomorphic to the intersection between A_n and the maximal

imprimitive subgroups of S_n with b blocks of size a , in other words, with abuse of notation, they are of the form $A_n \cap (S_a \wr S_b)$.

Consider the wreath product $G = S_n \wr S_m$. We have seen that it admits a faithful imprimitive action of degree nm . Consider now the product action of G , that is, the action of G on $\{1, \dots, n\}^m$ given by

$$(a_1, \dots, a_m)^{(\sigma_1, \dots, \sigma_m)\pi} := (a_{1\pi^{-1}}\sigma_{1\pi^{-1}}, \dots, a_{m\pi^{-1}}\sigma_{m\pi^{-1}}).$$

We show that this action is transitive.

Given $(a_1, \dots, a_m) \in \{1, \dots, n\}^m$, if $(\sigma_1, \dots, \sigma_m) \in (S_n)^m$, we have

$$(a_1, \dots, a_m)(\sigma_1, \dots, \sigma_m)(1) = (a_1\sigma_1, \dots, a_m\sigma_m),$$

and

$$\begin{aligned} \{1, \dots, n\}^m &\subseteq \{(a_1\sigma_1, \dots, a_m\sigma_m) : \sigma_i \in S_n, \} \subseteq O_G((a_1, \dots, a_m)) \\ &= \{(a_1, \dots, a_m)^g : g \in G\} \subseteq \{1, \dots, n\}^m. \end{aligned}$$

Also this is a faithful action. Moreover the stabilizer of (i, i, \dots, i) is isomorphic to $S_{n-1} \wr S_m$. Indeed, if $(\sigma_1, \dots, \sigma_m)\pi \in \text{Stab}_G((i, \dots, i))$ then $(i_\pi\sigma_{1\pi}, \dots, i_\pi\sigma_{m\pi}) = (i, \dots, i)$, that is, $i_\pi\sigma_{k\pi} = i$, for all $k = 1, \dots, m$. Since π only permutes the coordinates, we have $i\sigma_k = i$, for all $k = 1 \dots, m$, that is, $\sigma_k \in \text{Stab}_{S_n}(i)$. Then $(\sigma_1, \dots, \sigma_m)\pi \in \text{Stab}_{S_n}(i) \wr S_m \cong S_{n-1} \wr S_m$. Using the same calculations, it is proved that $\text{Stab}_{S_n}(i) \wr S_m \subseteq \text{Stab}_G(i, \dots, i)$.

For the following observe that if A, B are subgroups of G such that AB is a subgroup of G then $|AB : A| = |B : A \cap B|$.

Lemma 3. *Assume that $n \geq 5$ and m a positive integer. Then $G = S_n \wr S_m$ is a primitive group of type II with degree n^m .*

Proof. Since $n \geq 5$, A_n is the only proper normal subgroup of S_n , then $N = (A_n)^m$ is a non-Abelian normal subgroup of G . We will show that N is a minimal normal subgroup of G . Let N_i, N_j , as in Proposition 4, minimal normal subgroups of N with $i \neq j$. The permutation $(ij) \in S_m$ is such that $N_i^{(ij)} = N_j$. Let $\{1\} \neq K \triangleleft N$ with $K \triangleleft G$. Since K is normal in N there exists i with $N_i \leq K$. Since $K \triangleleft G$, we have $K^g = K$, for all

$g \in G$. Let $g = 1(ij)$. We have $N_j \leq K$, for all j . Then $K = N$ and N is a minimal normal subgroup of G . We will now show that $C_G(N) = \{1\}$. Let $g = (\sigma_1, \dots, \sigma_m)\pi \in C_G(N)$. Since g must centralize all elements of N of the form $(1, \dots, 1, a, 1, \dots, 1)$, we must have $\pi = 1$. Then $C_G(N) \leq S_n^m$, and $C_G(N) \leq C_{S_n^m}(A_n^m) = (C_{S_n}(A_n))^m = (\{1\})^m$. Therefore A_n^m is a minimal normal subgroup of G with trivial centralizer. By proposition 2, G is a primitive group of type II.

We are left to show that $M := S_{n-1} \wr S_m$ is a core-free maximal subgroup of G . It is clearly core-free because A_n^m is the unique minimal normal subgroup of G and M does not contain it. We also have

$$|G : M| = \frac{(n!)^m m!}{((n-1)!)^m m!} = n^m.$$

We need to show that M is a maximal subgroup of G .

Let $K := (S_{n-1})^m \leq B := (S_n)^m$. We claim that $M = N_G(K)$. The inclusion $M \leq N_G(K)$ is clear since $K \trianglelefteq M$. Now

$$B \cap N_G(K) = N_B(K) = N_{S_n^m}(S_{n-1}^m) = (N_{S_n}(S_{n-1}))^m = S_{n-1}^m = K,$$

since S_{n-1} is maximal and not normal in S_n . It is clear that the permutational factor S_m is contained in $N_G(K)$, therefore $G = BS_m \leq B \cdot N_G(K)$ hence $G = B \cdot N_G(K)$. Therefore

$$\begin{aligned} |G : N_G(K)| &= |B \cdot N_G(K) : N_G(K)| = |B : B \cap N_G(K)| \\ &= |B : K| = |B : M \cap B| = |BM : M| = |G : M|. \end{aligned}$$

Since $M \leq N_G(K)$, it follows that $M = N_G(K)$.

Let H be a maximal subgroup of G containing M . We claim that $H = M$. This follows if we can show that $H \cap B = K$. Indeed, assuming $H \cap B = K$, since $H \cap B \trianglelefteq H$ we have that $H \leq N_G(H \cap B) = N_G(K)$ and $N_G(K) \neq G$ being K not normal in G . Since H is maximal in G , we deduce that $H = N_G(H \cap B) = N_G(K) = M$. Therefore it is enough to show that $H \cap B = K$. The inclusion $K \subseteq H \cap B$ is clear.

We are left to prove that $H \cap B \subseteq K$. Write $B = B_1 \times \dots \times B_m$ and

$$R_i = \{1\} \times \dots \times \{1\} \times B_i \times \{1\} \times \dots \times \{1\}$$

for $i \in \{1, \dots, m\}$. G acts transitively on $\Gamma = \{R_1, \dots, R_m\}$ by conjugation with kernel equal to B . Since $H \geq M$ and $G = BM$, we have $G = BH$, hence H acts transitively on Γ . Let $\pi_i : B \rightarrow R_i$ be the canonical projections, $i \in \{1, \dots, m\}$. Fix $i, j \in \{1, \dots, m\}$ and let $h \in H$ be such that $R_i^h = R_j$. Composing the conjugation by h , $\gamma_h : H \cap B \rightarrow H \cap B$, with the canonical projection we find a surjective homomorphism

$$H \cap B \xrightarrow{\gamma_h} H \cap B \xrightarrow{\pi_j|_{H \cap B}} \pi_j(H \cap B)$$

whose kernel is $\ker(\pi_i|_{H \cap B})$. The isomorphism theorem implies that

$$\pi_i(H \cap B) \cong \pi_j(H \cap B).$$

Since $\pi_i(K) \cong S_{n-1}$ is a maximal subgroup of $B_i \cong S_n$ and $K \leq H \cap B$, we have $\pi_i(K) \leq \pi_i(H \cap B) \leq B_i$ therefore either $\pi_i(H \cap B) = \pi_i(K)$ or $\pi_i(H \cap B) = B_i$. In the first case

$$|H \cap B| \leq \prod_{i=1}^m |\pi_i(H \cap B)| = \prod_{i=1}^m |\pi_i(K)| = ((n-1)!)^m = |K|$$

hence $H \cap B = K$ being $H \cap B \geq K$.

Now assume that $\pi_i(H \cap B) = B_i$ for all $i \in \{1, \dots, m\}$.

Let $i \in \{1, \dots, m\}$. We claim that $H \cap R_i \leq R_i$. If $y \in H \cap R_i$ then $\pi_j(y) = 1$ for every $j \neq i$. If $r \in R_i$ then, being $\pi_i(H \cap B) = B_i$, there exists $x \in H \cap B$ such that $\pi_i(x) = \pi_i(r)$. Since x, y, r are m -tuples and $y \in R_i$, the fact that $\pi_i(x) = r$ implies that $r^{-1}yr = x^{-1}yx \in H$. This proves the claim.

But since $H \cap R_i$ contains $K \cap R_i \cong S_{n-1}$, $H \cap R_i$ is nontrivial and it is not the alternating group A_n , hence $H \cap R_i = R_i$, in other words $R_i \leq H$. This holds for every $i \in \{1, \dots, m\}$, hence $B \leq H$. This contradicts the fact that $H \neq HB = G$. The proof is completed. \square

We now state the O'Nan-Scott Theorem.

Theorem 6 (O'Nan-Scott Theorem). *If G is any proper subgroup of S_n , other than A_n , then G is a subgroup of one or more of the following subgroups.*

1. An intransitive group $S_k \times S_m$ where $n = k + m$.
2. An imprimitive group $S_k \wr S_m$ where $n = km$.
3. A primitive wreath product $S_k \wr S_m$ where $n = k^m$.
4. An affine group $AGL_d(p) = \mathbb{F}_p^d \rtimes GL_d(\mathbb{F}_p)$ where $n = p^d$.
5. A group of shape $T^m \cdot (\text{Out}(T) \times S_m)$ where T is a non-abelian simple group, acting on the cosets of a subgroup $\text{Aut}(T) \times S_m$, where $n = |T|^{m-1}$.
6. An almost-simple group acting on the cosets of a core-free maximal subgroup of index n .

Note that this theorem does not say that the groups listed are maximal in S_n . But certainly every maximal subgroup of S_n is of one of the types listed.

Now we will prove O’Nan-Scott Theorem.

Proof. This proof follows the line of [44], [5] and [28].

Set $\Omega := \{1, \dots, n\}$, let $\alpha \in \Omega$ and let U be the stabilizer of α in G . We know that U is a core-free maximal subgroup of G .

Let $G \leq \text{Sym}(\Omega)$ be a primitive group with socle N . Set $K := U \cap N$. Then

$$|G : U| = |UN : U| = |N : K|.$$

Moreover $K \trianglelefteq U$, so U is contained in the normalizer $N_G(K)$. Since $K \trianglelefteq U$, we have $U \leq N_G(K)$, and since U is maximal in G , either $U = N_G(K)$ or $N_G(K) = G$. In the latter case $K \trianglelefteq G$, hence the fact that $U_G = \{1\}$ forces $K = \{1\}$. This implies that either $K = \{1\}$ or $U = N_G(K)$. We know that $K = \{1\}$ if G is primitive of type I or III, so we will discuss these cases first.

If G is primitive of type I then the socle N of G is abelian and it is the unique minimal normal subgroup of G , moreover N is complemented by U , in other words $G \cong N \rtimes U$. The action of U on $N = \mathbb{F}_p^d$ is \mathbb{F}_p -linear,

faithful and irreducible, hence U is an irreducible subgroup of $\mathrm{GL}_d(\mathbb{F}_p)$. This is the affine case. In this case, G can be embedded in $\mathrm{AGL}(\mathbb{F}_p^d)$ which is a primitive subgroup of S_{p^d} with point stabilizer $\mathrm{GL}_d(\mathbb{F}_p)$.

If G is primitive of type III then the socle of G is $N = A \times B$ where A, B are the two minimal normal subgroups of G , both nonabelian and $A \cong AB \cap U \cong B$. We know that U is a complement of both A and B , hence A and B act regularly on Ω . The isomorphism $A \cong AB \cap U \cong B$ is explicated as follows. For every $a \in A$, since G is a semidirect product $B \rtimes U$, there is a unique $b_a \in B$ such that $ab_a \in U$. The map

$$f : A \rightarrow B, a \mapsto b_a$$

is a group isomorphism since $a_1 a_2 b_{a_1} b_{a_2} = a_1 b_{a_1} a_2 b_{a_2} \in U$ for every $a_1, a_2 \in A$ and the inverse $f^{-1} : B \rightarrow A$ sends $b \in B$ to the unique $a_b \in A$ such that $a_b b \in U$. We can define an element $\sigma \in \mathrm{Sym}(\Omega)$ as follows. Fix $\omega \in \Omega$. Every element of Ω can be uniquely written as ωa where $a \in A$. Define $(\omega a)\sigma := \omega(af)$. We claim that $af = \sigma^{-1}a\sigma$ for all $a \in A$, proving that $B = \sigma^{-1}A\sigma$. Indeed, if $x \in \Omega$, then we can write $x = \omega(a^*f)$ for a unique $a^* \in A$ and, if $a \in A$,

$$\begin{aligned} x\sigma^{-1}a\sigma &= (\omega(a^*f))\sigma^{-1}a\sigma = (\omega a^*)\sigma\sigma^{-1}a\sigma = (\omega a^*a)\sigma \\ &= \omega((a^*a)f) = \omega(a^*f)(af) = x(af). \end{aligned}$$

Therefore A and B are conjugate in $\mathrm{Sym}(\Omega)$ via σ , hence G is properly contained in $\langle G, \sigma \rangle \leq \mathrm{Sym}(\Omega)$ since A is normal in G but it is not normalized by σ . Moreover

$$B^\sigma = C_G(A)^\sigma = C_G(A^\sigma) = C_G(B) = A,$$

hence σ normalizes $A \times B$, in other words $A \times B$ is normal in $\langle G, \sigma \rangle$. This implies that $\langle G, \sigma \rangle$ is not equal to $\mathrm{Sym}(\Omega)$, since the only proper nontrivial normal subgroup of $\mathrm{Sym}(\Omega)$ is $\mathrm{Alt}(\Omega)$ and $\mathrm{Alt}(\Omega)$ is not a direct product of two nontrivial subgroups. This implies that the primitive groups of type III are not maximal in $\mathrm{Sym}(\Omega)$ hence we may ignore them.

Assume now G is primitive of type II with nonabelian socle $N = T^m = T_1 \times \dots \times T_m$. Set $H := N_G(T_1)$, $C := C_G(T_1)$. We know that $X := H/C$ is

an almost-simple group with socle isomorphic to T_1 and G embeds in the wreath product $X \wr K$, where $K \leq S_m$ is the transitive group induced by the action of G on the m direct factors of N . If $m = 1$ then $T_1 = N \trianglelefteq G$, $H = G$ and $C = C_G(N) = \{1\}$, therefore $G \cong X$ is almost-simple and we are in case (6) of the theorem. Assume now that $m > 1$. A subgroup of G is called U -invariant if its normalizer in G contains U . For example, since $U \cap N$ is normal in U , it is U -invariant.

Now we will prove that $U \cap N$ is a maximal proper U -invariant subgroup of N . It is clear that $U \cap N$ is a proper U -invariant subgroup of N . Now assume by contradiction that $U \cap N < L < N$ where L is U -invariant. In particular LU is a subgroup of G . We claim that $U < LU < G$, contradicting the maximality of U . Indeed, if $U = LU$ then $L \leq U$, a contradiction, and if $LU = G$ then $L \trianglelefteq G$ contradicting the fact that N is a minimal normal subgroup of G .

We want to show that we are in one of the following cases.

- *Twisted wreath product type.* This case is defined by the fact that $U \cap N = \{1\}$, in other words G is a semidirect product $N \rtimes U$. The corresponding primitivity degree is $|N|$.
- *Product type.* U is a conjugate of $N_G(R^m)$ where R is a proper non-trivial subgroup of T , which is the intersection between T and a core-free maximal subgroup of X . The corresponding primitivity degree is $|T : R|^m$.
- *Simple diagonal type.* $U = N_G(\Delta)$ where Δ is a diagonal subgroup of T^m , that is, a subgroup of the form

$$\{(x, x^{\phi_2}, \dots, x^{\phi_m}) : x \in T\} \leq N = T^m$$

where ϕ_2, \dots, ϕ_m are automorphisms of T . The corresponding primitivity degree is $|T|^{m-1}$.

- *Diagonal type in product action.* $U = N_G(\Delta_1 \times \dots \times \Delta_l)$ where l divides m , $l > 1$, $lk = m$ and each $\Delta_i \cong T$ is a diagonal subgroup of T^k . The corresponding primitivity degree is $|T|^{l(k-1)}$.

Call π_1, \dots, π_m the projections $\pi_i : T^m = T_1 \times \dots \times T_m \rightarrow T_i$. Observe that since N is a minimal normal subgroup of G and the normalizer $N_G(U \cap N)$ is a subgroup of G containing U , either U complements N in G or $N_G(U \cap N) = U$. Define $U_i := \pi_i(U \cap N)$ for $i = 1, \dots, m$. The same argument used in the proof of Lemma 3 shows that $U_i \cong U_j$ for every $i, j \in \{1, \dots, m\}$. If $U_1 \neq T_1$ then, since $U \cap N$ is contained in $U_1 \times \dots \times U_m$ and the latter is a proper U -invariant subgroup of N , $U \cap N = U_1 \times \dots \times U_m$ since $U \cap N$ is a maximal proper U -invariant subgroup of N .

There are three possibilities for U_1 . In the following discussion we will use Proposition 3.

Case 1. $U_1 = \{1\}$.

This implies that $U_i = \{1\}$ for every i , so $U \cap N = \{1\}$. In other words U complements N , so $G = N \rtimes U$ and the primitivity degree is $n = |N| = |T|^m$. This is the so-called twisted wreath product type. We know that G embeds in $X \wr S_m$ where $X = N_G(T_1)/C_G(T_1)$ is almost-simple with socle isomorphic to T , in particular X embeds in $\text{Aut}(T) \leq \text{Sym}(T)$. Setting $k = |T| = |T_1 : U_1|$, we obtain that G embeds in $S_k \wr S_m$ with product action of degree $n = k^m$.

Case 2. $\{1\} < U_1 < T_1$.

This implies that $\{1\} < U_i < T_i$ for every i . Since $U \cap N = U_1 \times \dots \times U_m$ and the U_i are pairwise isomorphic, the degree of the primitive action of G is

$$n = |G : U| = |UN : U| = |N : U \cap N| = |T^m : U_1 \times \dots \times U_m| = |T_1 : U_1|^m.$$

Let $H := N_G(T_1)$, $V := H \cap U = N_U(T_1)$ and $C := C_G(T_1)$.

We claim that U_1 is a maximal proper V -invariant subgroup of T_1 . Assume by contradiction that $U_1 < R < T_1$ and R is V -invariant. Since $UN = G$, the group U acts transitively on the m factors of N , hence for each $i \in \{1, \dots, m\}$ there exists $u_i \in U$ such that $T_1^{u_i} = T_i$. Set $\tilde{R} := R \times R^{u_2} \times \dots \times R^{u_m}$. Note that

$$U_1 = (U \cap N) \cap T_1 = U \cap T_1,$$

hence

$$U_1^{u_i} = (U \cap T_1)^{u_i} = U \cap T_1^{u_i} = U \cap T_i = (U \cap N) \cap T_i = U_i.$$

Therefore $U_i = U_1^{u_i} < R^{u_i}$. This implies that $U \cap N$ is properly contained in \widetilde{R} . Since $U \cap N$ is a maximal proper U -invariant subgroup of N , in order to obtain a contradiction it is enough to prove that \widetilde{R} is U -invariant. Let $x \in U$. Fix $i \in \{1, \dots, m\}$ and let j be such that $T_i^x = T_j$. Then $R^{u_i x} \leq T_j = T_1^{u_j}$, therefore $R^{u_i x u_j^{-1}} \leq T_1$. On the other hand $u_i x u_j^{-1}$ belongs to U and normalizes T_1 , therefore it belongs to $H \cap T_1 = V$. Since R is V -invariant, we deduce that $R^{u_i x u_j^{-1}} = R$, in other words $R^{u_i x} = R^{u_j}$. This implies that $\widetilde{R}^x = \widetilde{R}$. This holds for every $x \in U$, hence \widetilde{R} is U -invariant.

We have $VCT_1 = H$, since

$$H \supseteq VCT_1 \supseteq VN = (H \cap U)N = H \cap UN = H \cap G = H.$$

This implies that VC/C is a core-free subgroup of $X = H/C$. Indeed, since X is almost-simple, its unique minimal normal subgroup is T_1C/C and this is supplemented by VC/C since $VCT_1 = H$.

We claim that VC is a maximal subgroup of H , which implies that VC/C is a core-free maximal subgroup of the almost-simple group $X = H/C$, therefore X is a primitive group of degree $|X : VC/C|$. First, note that $VC \neq H$ because if this is not the case then $T_1 \leq H = VC = CV$, therefore, being $U_1 \neq \{1\}$, and being T_1 a simple group, we have

$$T_1 = \langle U_1^{T_1} \rangle \leq \langle U_1^{CV} \rangle = \langle U_1^V \rangle \leq U,$$

a contradiction. Assume the group M is such that $VC \leq M < H$, then $M \cap T_1$ is a V -invariant subgroup of T_1 and $U_1 \leq M \cap T_1$. If $T_1 \leq M$ then $H = VCT_1 \leq M$ and $H = M$, contradicting our assumption. Hence $U_1 \leq M \cap T_1 \neq T_1$. By maximality of U_1 as proper V -invariant subgroup of T_1 , we deduce that $U_1 = M \cap T_1$, hence

$$M = M \cap H = M \cap VCT_1 = VC(M \cap T_1) = VCU_1 = VC,$$

being $U_1 \leq V$. This proves the claim.

Since $U_1 \leq VC \cap T_1 < T_1$, U_1 is a maximal proper V -invariant subgroup of T_1 and $VC \cap T_1$ is V -invariant, we deduce that equality holds: $U_1 = VC \cap T_1$. Since $H = VCT_1$, we have

$$|H/C : VC/C| = |H : VC| = |VCT_1 : VC| = |T_1 : VC \cap T_1| = |T_1 : U_1|.$$

We deduce that $X = H/C$ is primitive of degree $k = |T_1 : U_1|$ with point stabilizer VC/C , hence X embeds into S_k . Moreover, U_1C/C equals the intersection between T_1C/C and the core-free maximal subgroup VC/C of H/C . Indeed, it is clear that $U_1C/C \leq T_1C/C \cap VC/C$, however, using that $H = VCT_1$, we have

$$|T_1C/C \cap VC/C| = \frac{|T_1C/C| \cdot |VC/C|}{|H/C|} = \frac{|T_1| \cdot |VC|}{|H|} = |T_1 \cap VC| = |U_1| = |U_1C/C|.$$

Now, G embeds into $X \wr K$ where K is a transitive subgroup of S_m and X embeds into S_k , therefore G embeds into $S_k \wr S_m$ and looking at the point stabilizers we deduce that the action of G is equivalent to the product action of degree $k^m = n$ induced by $S_k \wr S_m$ on $\{1, \dots, k\}^m$.

Case 3. $U_1 = T_1$.

This implies that $U_i = T_i$ for every i . For $x = (t_1, \dots, t_m) \in N$, let the support of x be the set

$$\text{supp}(x) := \{i \in \{1, \dots, m\} : t_i \neq 1\} \subseteq \{1, \dots, m\}.$$

Let Ω_1 be a minimal nonempty subset of $\{1, \dots, m\}$ such that $U \cap N$ contains an element whose support is Ω_1 . Let

$$A := A_{\Omega_1} = \{x \in U \cap N : \text{supp}(x) \subseteq \Omega_1\}.$$

By minimality of Ω_1 , if $x \in A$ and $x \neq 1$ then $\text{supp}(x) = \Omega_1$. Moreover, it is clear that A is a normal subgroup of $U \cap N$.

Fix $i \in \Omega_1$. We claim that for every $s \in T$ there exists a unique $g_{s,i} \in A$ such that $\pi_i(g_{s,i}) = s$ and that the map $f_i : T \rightarrow A$ defined by $f_i(s) := g_{s,i}$ is a group isomorphism whose inverse is $\pi_i|_A$. The uniqueness follows from the fact that if $g \in A$ is such that $\pi_i(g) = s$ then the element $gg_{s,i}^{-1}$ belongs to A and $\pi_i(gg_{s,i}^{-1}) = 1$, hence $gg_{s,i}^{-1} = 1$ by minimality of Ω_1 . To prove

the existence, we need to prove that $\pi_i(A) = T_i$. Let $L_i := \pi_i(A) \leq T_i$. Then $L_i \neq \{1\}$ by definition of Ω_1 . Since T_i is a simple group, to show that $L_i = T_i$ it is enough to show that L_i is normal in T_i . If $t \in T_i$ then, since $U_i = T_i$, there exists $u \in U \cap N$ with $\pi_i(u) = t$. If $x \in A$ then, since $u \in N$, x and x^u have the same support, hence $x^u \in A$. This implies that $\pi_i(x^u) \in L_i$ and this exactly says that $t^{-1}\pi_i(x)t \in L_i$. Now we prove that f_i is a group isomorphism. If $g \in A$ then, letting $s := \pi_i(g)$, it is clear that $f_i(s) = g$, this proves that f_i is surjective. If $s, t \in T$ are such that $f_i(s) = f_i(t)$ then applying π_i we find $s = t$, this proves injectivity. Since $\pi_i(g_{1,i}) = \pi_i(1) = 1$, it follows that $f_i(1) = g_{1,i} = 1$. If $s, t \in T$ then $\pi_i(g_{s,i}g_{t,i}) = \pi_i(g_{st,i}) = st$, it follows that $f_i(st) = f_i(s)f_i(t)$.

We deduce that A is a diagonal subgroup of T^{Ω_1} : indeed, setting $k := |\Omega_1|$,

$$A = \{(s, \phi_2(s), \dots, \phi_k(s)) : s \in T\} \leq T^{\Omega_1}$$

where $\phi_i = \pi_i|_A \circ f_1 \in \text{Aut}(T)$ for $i = 1, \dots, k$.

The natural action of G on the m direct factors of N gives an action of G on $\{1, \dots, m\}$. We claim that Ω_1 is an imprimitivity block for this action. Assume Ω_1 is the support of some $x \in U \cap N$. If $g = nu \in G$ with $n \in N$, $u \in U$, then $\Omega_2 := \Omega_1^g = \Omega_1^u$ is the support of $y := x^u \in U \cap N$. Assume $\Omega_1 \cap \Omega_2 \neq \emptyset$. We claim that $\Omega_1 = \Omega_2$. Let $i \in \Omega_1 \cap \Omega_2$, so that $\pi_i(x) \neq 1 \neq \pi_i(y)$. Since T_i is simple, the conjugacy class of $\pi_i(x)$ in T_i generates T_i and $Z(T_i) = \{1\}$. Since $\pi_i(y) \neq 1$ there exists $t \in T_i$ such that $\pi_i(x)^t$ does not commute with $\pi_i(y)$. Since $U_i = T_i$, there exists $v \in U \cap N$ such that $\pi_i(v) = t$, therefore $\pi_i(x^v) = \pi_i(x)^t$. Moreover $\text{supp}(x^v) = \text{supp}(x) = \Omega_1$ and $\pi_i(x^v) \neq 1$ being $\pi_i(x) \neq 1$. Up to replacing x with x^v , we may assume that $\pi_i(x)$ and $\pi_i(y)$ do not commute. If $j \in \Omega_1 - \Omega_2$ then $\pi_j(x) \neq 1$, $\pi_j(y) = 1$, and if $j \in \Omega_2 - \Omega_1$ then $\pi_j(x) = 1$, $\pi_j(y) \neq 1$, therefore $\pi_j([x, y]) = 1$ unless possibly if $j \in \Omega_1 \cap \Omega_2$, where $[x, y] := x^{-1}y^{-1}xy \in U \cap N$. This says that $\text{supp}([x, y]) \subseteq \Omega_1 \cap \Omega_2$, therefore $\Omega_1 = \Omega_1 \cap \Omega_2$ by minimality of Ω_1 , in other words $\Omega_1 \subseteq \Omega_2$. Since $\Omega_2 = \Omega_1^u$, $|\Omega_1| = |\Omega_2|$, hence $\Omega_1 = \Omega_2$.

We claim that $|\Omega_1| \neq 1$. If Ω_1 has size 1, say $\Omega_1 = \{i\}$, then there exists an element $x \in U \cap N$ such that $\pi_i(x) \neq 1$ and $\pi_j(x) = 1$ for every $j \neq i$.

Since $U_i = T_i$, for every $t \in T_i$ there exists $u \in U \cap N$ with $\pi_i(u) = t$, hence $U \cap N$ contains the whole conjugacy class of x , so it contains the i -th factor, being T a simple group. Since U acts transitively on the factors, U contains N , a contradiction.

Assume the block system consists of l blocks $\Omega_1, \dots, \Omega_l$, each of size $k > 1$. We have $N = T^{kl}$. We may consider the normal subgroups $A_{\Omega_j} \trianglelefteq U \cap N$, $j = 1, \dots, l$, defined in the same way as for A_{Ω_1} above. Note that the group they generate is a direct product $A_{\Omega_1} \times \dots \times A_{\Omega_l} \cong T^l$. Moreover this product equals $U \cap N$. To prove this, fix $g \in U \cap N$ and, for every $j \in \{1, \dots, l\}$, let $x_j \in A_{\Omega_j}$ be such that there exists $i = i(j) \in \Omega_j$ with the property that $\pi_i(g) = \pi_i(x_j)$. We claim that $g = x_1 \dots x_l$. We need to show that $\pi_r(g) = \pi_r(x_1 \dots x_l)$ for all $r = 1, \dots, m = kl$. Fix $r \in \{1, \dots, m\}$ and let $j \in \{1, \dots, l\}$ be such that $r \in \Omega_j$. By definition of x_j , there exists $i \in \Omega_j$ with $\pi_i(g) = \pi_i(x_j)$, in other words $\pi_i(h) = 1$ where $h = g^{-1}x_j \in U \cap N$. If x is any element of A_{Ω_j} then $\pi_i(h^{-1}xh) = \pi_i(x)$, therefore $h^{-1}xh = x$ being $A_{\Omega_j} \trianglelefteq U \cap N$ and being the restriction $\pi_i|_{A_{\Omega_j}} : A_{\Omega_j} \rightarrow T$ injective. This implies that $h \in C_{U \cap N}(A_{\Omega_j})$, therefore $\pi_r(h) = 1$, hence $\pi_r(g) = \pi_r(x_j) = \pi_r(x_1 \dots x_l)$.

We deduce that $U \cap N = A_{\Omega_1} \times \dots \times A_{\Omega_l}$, in particular $U \cap N \cong T^l$. Therefore

$$n = |G : U| = |UN : U| = |N : U \cap N| = |T|^{(k-1)l}.$$

Now consider

$$Y := T^{\Omega_1} = \prod_{i \in \Omega_1} T_i, \quad H := N_G(Y), \quad \xi : H \rightarrow \text{Aut}(Y), \quad C := \ker(\xi) = C_G(Y).$$

Observe that H is precisely the setwise stabilizer of the block Ω_1 , in particular H acts transitively on Ω_1 , therefore YC/C is a minimal normal subgroup of H/C .

Let $A := A_{\Omega_1}$, $V := U \cap H$. Note that since Y is a direct power of a nonabelian simple group and A is a full diagonal subgroup of Y , we have $\langle A^Y \rangle = Y$. Now, the argument used in the proof of the case $1 < U_1 < T_1$ with U_1 replaced by A , T_1 replaced by Y proves that $VCY = H$, $Y \cap VC = A$, YC/C is the unique minimal normal subgroup of H/C and $\xi(H) \cong H/C$

is a primitive group of type II with point stabilizer the core-free maximal subgroup VC/C . Moreover $VC/C \cap YC/C = AC/C \cong A$, therefore H/C is a primitive group of simple diagonal type. Now an application of the embedding argument gives that G lies inside a wreath product $H/C \wr S_l \leq S_r \wr S_l$ where $r = |T|^{k-1}$ and we are in case (3) of the theorem.

Now assume there is only one block, $l = 1$. Then $m = k > 1$ and $U \cap N \cong S$, $N \cong T^m$. In this case $n = |T|^{m-1}$. Without loss of generality, $\Delta := U \cap N = \{(s, \dots, s) : s \in T\}$. G is a subgroup of $X \wr S_m$ and $U = N_G(\Delta)$. Note that $(x_1, \dots, x_m)\pi \in X \wr S_m$ normalizes Δ if and only if

$$(s, \dots, s)^{(x_1, \dots, x_m)\pi} \in \Delta \quad \forall s \in T,$$

and this means $s^{x_1} = \dots = s^{x_m}$ for all $s \in T$. This implies that $s^{x_i x_j^{-1}} = s$ for all $s \in T$ and for all $i, j \in \{1, \dots, m\}$ and, since the x_i are automorphisms of T , we deduce the necessary and sufficient condition $x_1 = \dots = x_m$. This implies that

$$U = N_G(\Delta) \leq \{(a, a, \dots, a)\pi : a \in \text{Aut}(T), \pi \in S_m\} \cong \text{Aut}(T) \times S_m$$

hence $G = N \cdot N_G(\Delta)$ is contained in the group

$$\{(a_1, \dots, a_m)\pi \in \text{Aut}(T) \wr S_m : a_i \equiv a_j \pmod{\text{Inn}(T)} \forall i, j\},$$

which is an extension $T^m \cdot (\text{Out}(T) \times S_m)$ with point stabilizer isomorphic to $\text{Aut}(T) \times S_m$. We are in case (5) of the theorem, the simple diagonal type. This concludes the proof of O'Nan-Scott Theorem. \square

Chapter 2

Minimal coverings

In this chapter we present the content of the paper [2]. Specifically, we give constructive proofs for our results concerning $\sigma(G)$ for a family of primitive groups G with a unique minimal normal subgroup N , isomorphic to A_n^m , with n divisible by 6 and G/N cyclic. This is a generalization of a result of E. Swartz [40] concerning the symmetric groups.

2.1 The function $\sigma(G)$

Definition 5. *A covering of a group G is a family of proper subgroups of G whose union is G . The covering number of G , denoted $\sigma(G)$, is the smallest size of a covering of G . 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 .*

Proposition 9. *Let G a finite group. Then $\sigma(G) > 2$.*

Proof. Suppose by contradiction that $G = H \cup K$ with H and K distinct proper subgroups of G . Let $h \in H - K$. For all $k \in K$, $hk \in H$ or $hk \in K$. Since $hk \in K$ implies $h \in K$, we have $hk \in H$. Then for all $k \in K$ we have $k \in H$, so $K \subseteq H$ and therefore $G = H$, contradiction. \square

Proposition 10. *If $N \trianglelefteq G$, then $\sigma(G) \leq \sigma(G/N)$.*

Proof. It suffices to observe that every covering of the quotient G/N gives us a covering of G . \square

In particular, the above Proposition implies that

$$\sigma(G_1 \times \dots \times G_n) \leq \min\{\sigma(G_1), \dots, \sigma(G_n)\}.$$

Proposition 11. *If p is a prime number, then $\sigma(C_p \times C_p) = p + 1$.*

Proof. A minimal covering of $C_p \times C_p$ must contain all the $p + 1$ maximal subgroups. \square

Lemma 4. *Let G be a non-cyclic group. Write $G = \bigcup_{i=1}^n H_i$, as a union of $n = \sigma(G)$ subgroups of G . For all $i \in \{1, \dots, n - 1\}$ suppose that $|G : H_i| \leq |G : H_{i+1}|$. Then $|G : H_1| < \sigma(G)$.*

Proof. Since $1 \in H_1 \cap \dots \cap H_n$, we have

$$|G| < \sum_{i=1}^n |H_i| = \sum_{i=1}^n \frac{|G|}{|G : H_i|} \leq n \cdot \frac{|G|}{|G : H_1|}.$$

Therefore $|G : H_1| < n = \sigma(G)$. \square

Lemma 5. *Let G a non-cyclic p -group. Then $\sigma(G) = p + 1$.*

Proof. Since any non-trivial proper subgroup of G has index at least p , by Lemma 4, $p + 1 \leq \sigma(G)$.

If G is non-cyclic, G has a quotient isomorphic to $C_p \times C_p$, then $\sigma(G) \leq \sigma(C_p \times C_p) = p + 1$.

If $|G| = p^k$ with $k \geq 2$, we prove $\sigma(G) \leq p + 1$ by induction on k . For $k = 2$, G is $C_p \times C_p$ and the result follows from Proposition 11. For $k \geq 3$, if G is abelian the result is shown above, otherwise $G/Z(G)$ is a non-trivial non-cyclic p -group with $|G/Z(G)| < |G|$, since $Z(G)$ is non-trivial. By induction hypothesis, $\sigma(G) \leq \sigma(G/Z(G)) = p + 1$. Therefore $\sigma(G) = p + 1$. \square

Proposition 12. [9, Lemma 4] *If $(|H|, |K|) = 1$, then $\sigma(H \times K) = \min\{\sigma(H), \sigma(K)\}$.*

Proposition 13. *If G is a non-cyclic nilpotent group then $\sigma(G) = p + 1$, where p is the smallest prime for which the Sylow p -subgroup is non-cyclic.*

Proof. Since G is the direct product of its Sylows p -subgroups, by Proposition 12

$$\sigma(G) = \min\{\sigma(P) : P \text{ is a Sylow } p\text{-subgroup of } G\}.$$

Therefore, by Lemma 5, $\sigma(G) = p + 1$. \square

Tomkinson [41, Theorem 2.2] computed the covering number of solvable groups. Recall that a chief factor of a group G is a quotient H/K where $K \trianglelefteq G$ and H/K is a minimal normal subgroup of G/K . A subgroup L of G is called a complement of a chief factor H/K of G if $HL = G$ and $H \cap L = K$. In other words $K \leq L$ and L/K is a complement of H/K in G/K .

Example. Let $p > 2$ be a prime and $G = \langle a, b : a^{2p} = b^2 = 1, a^b = a^{-1} \rangle$, the Dihedral group with $4p$ elements. Let $H = \langle a \rangle \cong C_{2p}$ and $K = \langle a^2 \rangle \cong C_p$. The quotient H/K is a chief factor of G and the subgroups $L_1 = \langle a^2, b \rangle$ and $L_2 = \langle a^2, ab \rangle$ (isomorphic to the Dihedral group with $2p$ elements) are complements of H/K in G . The minimal normal subgroups of G are also chief factors of G . The subgroups $H = \langle a^2 \rangle \cong C_p$ and $N = \langle a^p \rangle \cong C_2$ are the minimal normal subgroups of G . H has p complements in G , they are of the form $\langle a^p \rangle \cdot \langle a^i b \rangle$, for $i = 0, \dots, p-1$, and N has two complements in G , they are L_1 and L_2 .

Theorem 7 (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.*

As a consequence, if G is a primitive solvable noncyclic group then either $\sigma(G) = \sigma(G/\text{soc}(G))$ or $\sigma(G) = |\text{soc}(G)| + 1$. This is a consequence of the following theorem of Gaschütz.

Theorem 8 (Gaschütz [21]). *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 $|V|$.*

2.1.1 $\sigma(G)$ for some groups

In this section we present tables that summarize what is currently known about covering numbers of symmetric groups, alternating groups and projective linear groups of dimension 2. The reference for these tables is [19].

Group	Covering Number	Citation
S_3	4	
S_4	4	
S_5	16	[9]
S_6	13	[1]
S_8	64	[25]
S_9	256	[25]
S_{10}	221	[25]
S_{12}	761	[25]
S_{14}	3096	[36]
S_{18}	36773	[40]
$S_{6k}, k \geq 4$	$\frac{1}{2} \binom{6k}{3k} + \sum_{i=0}^{2k-1} \binom{6k}{i}$	[40]
$S_{2k+1}, k \neq 4$	2^{2k}	[34]
$S_{2k}, k \geq 16$	$> \frac{1}{2} \binom{2k}{k}$	[34]

Table 2.1: Covering numbers of symmetric groups.

Group	Covering Number	Citation
A_5	10	[9]
A_6	16	[8]
A_7	31	[26]
A_8	71	[26]
A_9	157	[12]
A_{10}	256	[34]
A_{11}	2751	[12]
A_{4k+2}	2^{4k}	[34]
$A_{18k+3}, k > 0$	$\sum_{i=1}^{6k-1} \binom{18k+3}{i} + \frac{(18k+3)!}{6(6k+1)!^3}$	[14]
$A_n, n \geq 12$	$\geq 2^{n-2}$	[34]

Table 2.2: Covering numbers of alternating groups.

Group	Covering Number	Citation
PSL(2, 5)	10	[9]
PGL(2, 5)	16	[9]
PSL(2, 7)	15	[8]
PGL(2, 7)	29	[8]
PSL(2, 9)	16	[8]
PGL(2, 9)	46	[8]
PGL(2, 8)	29	[18]
PSL(2, q), PGL(2, q), $q \geq 8$ even	$\frac{1}{2}q(q+1)$	[8]
PSL(2, q), PGL(2, q), $q > 9$ odd	$\frac{1}{2}q(q+1) + 1$	[8]

Table 2.3: Covering numbers of 2-dimensional linear groups.

2.2 A sufficient condition for a covering to be minimal

Assume G is a finite group whose conjugacy classes of maximal subgroups are indexed by a set I_G . For $j \in I_G$, let \mathcal{M}_j be the corresponding conjugacy class of maximal subgroups of G . Let J be a subset of I_G and let $\mathcal{C} = \cup_{j \in J} \mathcal{M}_j$ be the union of the conjugacy classes \mathcal{M}_j . Assume that \mathcal{C} is a covering of G ; that is, $\cup_{M \in \mathcal{C}} M = G$. Let Π be a subset of G closed under conjugation and denote by Π_j the subset of Π covered by the conjugacy class \mathcal{M}_j , so that Π_j is closed under conjugation. If M, M' are conjugate maximal subgroups of G and $j \in J$, then $|M \cap \Pi| = |M' \cap \Pi|$ and $|M \cap \Pi_j| = |M' \cap \Pi_j|$.

For a maximal subgroup M of G such that $M \notin \mathcal{C}$, let

$$c_{\mathcal{C}, \Pi}(M) := \sum_{j \in J} \frac{|M \cap \Pi_j|}{|M_j \cap \Pi_j|}$$

where M_j is any fixed member of \mathcal{M}_j .

For simplicity of notation, let us denote $c_{\mathcal{C}, \Pi}(M)$ by $c(M)$.

Lemma 6 (Lemma 3.1 of [40]). *Assume that the following conditions hold for the covering \mathcal{C} and the set Π defined above.*

1. $x^g \in \Pi$, for all $x \in \Pi$ and $g \in G$, i.e. Π is closed under conjugation.
2. For every $\pi \in \Pi$, there is a unique member of \mathcal{C} containing π .

3. $c(H) < 1$ for every maximal subgroup H of G not in \mathcal{C} .

Then \mathcal{C} is a minimal covering of G , meaning that $\sigma(G) = |\mathcal{C}|$. Moreover \mathcal{C} is the unique minimal covering of G consisting of maximal subgroups.

Proof. Assume that $c(M) < 1$ for all maximal subgroups not in \mathcal{C} . Suppose that \mathcal{B} is another covering of the elements of Π , and let $\mathcal{C}' = \mathcal{C} \setminus (\mathcal{C} \cap \mathcal{B})$ and $\mathcal{B}' = \mathcal{B} \setminus (\mathcal{C} \cap \mathcal{B})$. The collection \mathcal{C}' consists only of subgroups from classes \mathcal{M}_j , where $j \in J$, and we let a_j be the number of subgroups from \mathcal{M}_j in \mathcal{C}' . Similarly, the collection \mathcal{B}' consists only of subgroups from classes \mathcal{M}_i , where $i \notin J$, and we let b_i be the number of subgroups from \mathcal{M}_i in \mathcal{B}' . Note that, since \mathcal{B} is a different cover, for some $i \notin J$, we have $b_i > 0$.

By removing a_j subgroups from class \mathcal{M}_j from \mathcal{C} , the new subgroups in \mathcal{B}' must cover the elements of Π that were in these subgroups. Hence, for all $j \in J$, if M_k denotes a subgroup in class \mathcal{M}_k for each k ,

$$a_j |M_j \cap \Pi_j| \leq \sum_{i \notin J} b_i |M_i \cap \Pi_j|,$$

which in turn implies that, for all $j \in J$,

$$a_j \leq \sum_{i \notin J} b_i \frac{|M_i \cap \Pi_j|}{|M_j \cap \Pi_j|}.$$

This means that:

$$\begin{aligned} |\mathcal{C}'| &= \sum_{j \in J} a_j \leq \sum_{j \in J} \sum_{i \notin J} b_i \frac{|M_i \cap \Pi_j|}{|M_j \cap \Pi_j|} = \sum_{i \notin J} \sum_{j \in J} b_i \frac{|M_i \cap \Pi_j|}{|M_j \cap \Pi_j|} \\ &= \sum_{i \notin J} \left(\sum_{j \in J} \frac{|M_i \cap \Pi_j|}{|M_j \cap \Pi_j|} \right) b_i = \sum_{i \notin J} c(M_i) b_i < \sum_{i \notin J} b_i = |\mathcal{B}'|. \end{aligned}$$

which shows that

$$|\mathcal{C}| = |\mathcal{C}'| + |\mathcal{C} \cap \mathcal{B}| < |\mathcal{B}'| + |\mathcal{C} \cap \mathcal{B}| = |\mathcal{B}|.$$

Hence, any other cover of the elements of Π using only maximal subgroups has size strictly larger than the size of \mathcal{C} . Therefore, \mathcal{C} is a minimal cover of the elements of Π , and it is the unique minimal cover of the elements of Π that uses only maximal subgroups. \square

It is worth noting that, with the above result, the computation of $\sigma(G)$ for some families of groups existing in the literature (for example [34]) can be refined proving that for many of these groups there exists a unique minimal covering consisting of maximal subgroups.

2.3 Proof of Theorem 1

2.3.1 The group $G_{n,m}$

Let G be a primitive monolithic group with non-abelian socle $N = S^m$, and S a non-abelian simple group. For $i \in \{1, \dots, m\}$, let S_i be the subgroup of N equal to $\prod_{j=1}^m U_j$ where $U_i = S$ and $U_j = \{1\}$ for all $j \neq i$ (coordinate subgroup), so that $S_i \cong S$ for all i .

Let $X := N_G(S_1)/C_G(S_1)$. The group X is an almost simple group with socle $S_1 C_G(S_1)/C_G(S_1) \cong S_1$.

The minimal normal subgroups of $S^m = S_1 \times \dots \times S_m$ 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 $\rho : G \rightarrow \text{Sym}(m)$ be the homomorphism induced by the conjugation action of G on the set $\{S_1, \dots, S_m\}$.

Let $K := \rho(G)$. K is a transitive permutation group of degree m . By [5, 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:

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

Call $\pi_G : G \rightarrow G/\text{soc}(G)$ and $\pi_X : X \rightarrow X/S$ the natural projections.

Lemma 7. *X/S is cyclic and $L = X$. More precisely, assume that $G/\text{soc}(G)$ is cyclic and let g in G be such that $\pi_G(g)$ generates $G/\text{soc}(G)$. Write $g = (x_1, \dots, x_m)\delta$ with $x_1, \dots, x_m \in X$, and $\delta \in \text{Sym}(m)$ an m -cycle. Then $\pi_X(x_1 x_{\delta(1)} \dots x_{\delta(m-1)})$ generates X/S and $|G| = |S|^m \cdot m \cdot |X/S|$.*

Proof. $N_G(S_1)/\text{soc}(G)$ is a subgroup of $G/\text{soc}(G)$, hence cyclic, and it

projects onto $N_G(S_1)/S_1C_G(S_1) = X/S$. Thus X/S is cyclic.

Let $x \in X$ be such that $X/S = \langle xS \rangle$. For $i = 1, \dots, m$, write $x_i = s_i x^{k_i}$, where $s_i \in S$ and $k_i \in N$. 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 $(x^k, \dots, x^k) \text{soc}(G)$ generates $G \cap X^m / \text{soc}(G)$. 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. \square

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

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

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

Let n, m positive integers with $n \geq 5, n \neq 6$, and $S = A_n \cong S_i, i = 1, \dots, m$. Since $X = N_G(S_1)/C_G(S_1)$, X is isomorphic to a subgroup of $\text{Aut}(S) \cong S_n$ then either $X \cong A_n$ ("even case") or $X \cong S_n$ ("odd case"). In the even case $G \cong A_n \wr C_m$ ([5, Definition 1.1.8 and Remark 1.1.40.13]). The odd case is the group $G_{n,m}$ and will be considered below.

Let $G = G_{n,m}$ be the semidirect product $A_n^m \rtimes \langle \gamma \rangle$ where

$$\gamma = (1, \dots, 1, \tau)\delta \in S_n \wr S_m,$$

with $\tau = (1\ 2)$ and $\delta = (1\ \dots\ m)$.

For $x_1, \dots, x_m \in A_n$, the action of γ is given by

$$(x_1, \dots, x_m)^\gamma = (x_1, \dots, x_m)^{(1, \dots, 1, \tau)\delta} = (x_1, \dots, x_m^\tau)^\delta = (x_m^\tau, x_1, \dots, x_{m-1}).$$

Observe that G is a generalization of the Symmetric Group S_n : if $m = 1$ then $G = A_n \rtimes \langle (1\ 2) \rangle \cong S_n$.

The group G is a primitive group of type II, meaning that G has a core-free maximal subgroup and it admits precisely one minimal normal subgroup, which is nonabelian: its socle, $N = A_n^m$.

The element γ has order $2m$. We will compute some powers of γ . For this we use that $\delta^{-1} = (1\ m\ m-1\ \dots\ 3\ 2)$. Note that,

$$\begin{aligned} \gamma^2 &= (1, \dots, 1, \tau)\delta \cdot (1, \dots, 1, \tau)\delta = (1, \dots, 1, \tau)\delta(1, \dots, 1, \tau)\delta^{m-1}\delta^2 \\ &= (1, \dots, 1, \tau)(1, \dots, 1, \tau)^{\delta^{-1}}\delta^2 = (1, \dots, 1, \tau)(1, \dots, 1, \tau, 1)\delta^2 = (1, \dots, 1, \tau, \tau)\delta^2. \end{aligned}$$

Analogously, for $1 \leq k < m$, $\gamma^k = (1, \dots, 1, \tau, \dots, \tau)\delta^k$, where the last k coordinates are equal to τ , and $\gamma^m = (\tau, \dots, \tau)$.

We also have $\gamma^{-1} = (\tau, 1, \dots, 1)\delta^{-1}$.

Now let's calculate some useful conjugates of elements of group G . Let $x_i, y_i \in A_n$, for $1 \leq i \leq m$. Observe that

$$(x_1, \dots, x_m)^{\gamma^{-1}} = (x_2, x_3, \dots, x_m, x_1^\tau).$$

For the element $(x_1, \dots, x_m)\gamma \in G$ we have

$$((x_1, \dots, x_m)\gamma)^\gamma = \gamma^{-1}(x_1, \dots, x_m)\gamma \cdot \gamma = (x_m^\tau, x_1, \dots, x_{m-1})\gamma,$$

and

$$\begin{aligned}
& ((x_1, \dots, x_m)\gamma)^{(y_1, \dots, y_m)} \\
&= (y_1, \dots, y_m)^{-1}(x_1, \dots, x_m)\gamma(y_1, \dots, y_m) \cdot \gamma^{-1}\gamma \\
&= (y_1^{-1}x_1, \dots, y_m^{-1}x_m)(y_1, \dots, y_m)^{\gamma^{-1}}\gamma \\
&= (y_1^{-1}x_1, \dots, y_m^{-1}x_m)(y_2, y_3, \dots, y_m, y_1^\tau)\gamma \\
&= (y_1^{-1}x_1y_2, y_2^{-1}x_2y_3, \dots, y_{m-1}^{-1}x_{m-1}y_m, y_m^{-1}x_my_1^\tau)\gamma.
\end{aligned}$$

For $1 \leq k < m$, for the element $(x_1, \dots, x_m)\gamma^k \in G$, we have

$$\begin{aligned}
((x_1, \dots, x_m)\gamma^k)^\gamma &= \gamma^{-1}(x_1, \dots, x_m)\gamma \cdot \gamma^k \\
&= (\tau x_m \tau, x_1, \dots, x_{m-1}) \cdot \gamma^k,
\end{aligned}$$

and, since $(y_1, \dots, y_m)^{\gamma^{-k}} = (y_1, \dots, y_m)^{(\gamma^{-1})^k}$,

$$\begin{aligned}
& ((x_1, \dots, x_m)\gamma^k)^{(y_1, \dots, y_m)} \\
&= (y_1, \dots, y_m)^{-1}(x_1, \dots, x_m)\gamma^k(y_1, \dots, y_m) \\
&= (y_1^{-1}x_1, \dots, y_m^{-1}x_m)(y_1, \dots, y_m)^{\gamma^{-k}} \cdot \gamma^k \\
&= (y_1^{-1}x_1, \dots, y_m^{-1}x_m)(y_{k+1}, y_{k+2}, \dots, y_m, y_1^\tau, y_2^\tau, \dots, y_k^\tau) \cdot \gamma^k \\
&= (y_1^{-1}x_1y_{k+1}, \dots, y_{m-k}^{-1}x_{m-k}y_m, y_{m-k+1}^{-1}x_{m-k+1}y_1^\tau, \dots, y_m^{-1}x_my_k^\tau) \cdot \gamma^k.
\end{aligned}$$

About $\sigma(G)$ we already know:

Theorem 9. [17, Theorem 1] *Let m, n be positive integers, and let $G = G_{m,n}$. Let $\alpha(x)$ denote the number of prime factors of the positive integer x . The following holds:*

(1) *Suppose that $n \geq 7$ is odd and $m \neq 1$ if $n = 9$. Then*

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

(2) If $n = 5$, then

$$10^m \leq \sigma(G) \leq \alpha(2m) + 5^m + 10^m.$$

(3) Suppose that $n \geq 8$ is even. Then

$$\left(\frac{1}{2} \binom{n}{n/2}\right)^m \leq \sigma(G) \leq \alpha(2m) + \left(\frac{1}{2} \binom{n}{n/2}\right)^m + \sum_{i=1}^{\lfloor n/3 \rfloor} \binom{n}{i}^m.$$

In particular, $\sigma(G) \sim \left(\frac{1}{2} \binom{n}{n/2}\right)^m$ as $n \rightarrow \infty$.

(4) If $n = 6$, then

$$\sigma(G) = \alpha(2m) + 2 \cdot 6^m.$$

We will construct sets J , Π and \mathcal{C} to apply Lemma 6 to determine the value of $\sigma(G_{n,m})$ for $n \geq 30$ divisible by 6 and $m \geq 2$.

2.3.2 The set Π

For simplicity of notation, let us denote by $[a_1, \dots, a_k]$ the conjugacy class of S_n corresponding to the elements of cycle structure (a_1, \dots, a_k) , where the a_i 's are positive integers and $a_1 + \dots + a_k = n$. Let $I = \{-1, 1, 2, \dots, n/3 - 1\}$. As in [40], we define collections B_i , $i \in I$, as follows.

$$B_{-1} := [n],$$

$$B_1 := [1, n/2 - 2, n/2 + 1],$$

$$B_2 := \begin{cases} [2, n/2 - 1, n/2 - 1], & \text{if } n/2 \text{ is even,} \\ [2, n/2 - 4, n/2 + 2], & \text{if } n/2 \text{ is odd,} \end{cases}$$

$$B_i := \begin{cases} [i, (n - i - 1)/2, (n - i + 1)/2], & \text{if } i \text{ is odd, } 3 \leq i < n/3, \\ [i, (n - i)/2, (n - i)/2], & \text{if } i \text{ is even, } (n - i)/2 \text{ is odd, } 4 \leq i < n/3, \\ [i, (n - i)/2 - 1, (n - i)/2 + 1], & \text{if } i \text{ is even, } (n - i)/2 \text{ is even, } 4 \leq i < n/3. \end{cases}$$

Note that $B_i \cap A_n = \emptyset$ for all $i \in I$.

Let $G = G_{n,m}$ be the group defined in Section 2.3.1, that is, $G = A_n^m \rtimes \langle \gamma \rangle$, where $\gamma = (1, \dots, 1, \tau)\delta$, $\tau = (1\ 2)$ and $\delta = (1 \dots m)$.

We define the set Π_i for all $i \in I$ as follows:

$$\Pi_i = \{(x_1, x_2, \dots, x_m)\gamma \in G : x_1x_2 \dots x_m\tau \in B_i\}.$$

Note that the sets Π_i are pairwise disjoint as are the sets B_i .

Note that we did not define Π_0 yet. Rather than defining a unique Π_0 , we will define several sets, which we will call $\Pi_{0,r}$, for every prime r dividing m . For such r , let D_1 be the conjugacy class of $(n-2)$ -cycles in S_n , and let D_i be the conjugacy class of n -cycles in S_n for $i = 2, \dots, r$. Let $\nu := (1 \dots r)$. For all $\sigma \in \langle \nu \rangle$, let

$$\Pi_{0,r,\sigma} := \{(x_1, \dots, x_m)\gamma^r \in G : x_i x_{i+r} x_{i+2r} \dots x_{i+m-r} \tau \in D_{\sigma(i)} \forall i = 1, \dots, r\}.$$

Assume that either m is even or $r \neq 2$. We define

$$\Pi_{0,r} := \bigcup_{\sigma \in \langle \nu \rangle} \Pi_{0,r,\sigma}.$$

This is a disjoint union. Indeed, let $\sigma_1, \sigma_2 \in \langle \nu \rangle$ with $\sigma_1 \neq \sigma_2$ and assume by contradiction that there exists $(x_1, \dots, x_m)\gamma^r \in \Pi_{0,r,\sigma_1} \cap \Pi_{0,r,\sigma_2}$. Since $\sigma_1 \neq \sigma_2$ and r is a prime, there exists $i \in \{1, \dots, r\}$ such that $\sigma_1(i) = 1$ and $j = \sigma_2(i) \neq 1$. Since $x_i x_{i+r} \dots x_{i+m-r} \tau$ belongs to $D_{\sigma_1(i)} \cap D_{\sigma_2(i)} = D_1 \cap D_j$, we deduce that $D_1 = D_j$, a contradiction. It follows that

$$|\Pi_{0,r}| = r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^r |D_i|.$$

Assume now that m is odd. We will define $\Pi_{0,2}$. Consider the conjugacy class C of S_n consisting of the elements of cycle structure $(p, n-p)$ where p is a fixed prime number such that $n/3 < p < 2n/3$. Note that p exists by Bertrand's postulate (see [43]). In this case, we define

$$\Pi_{0,2} := \{(x_1, \dots, x_m)\gamma^2 \in G : x_1x_3 \dots x_m\tau \cdot x_2x_4 \dots x_{m-1}\tau \in C\}.$$

Note that

$$|\Pi_{0,2}| = |A_n|^{m-1} \cdot |C|.$$

Definition 6. We define J to be the set of indices consisting of the elements of I and the pairs $(0, r)$ where r is a prime divisor of $2m$. We also set

$$\Pi := \bigcup_{j \in J} \Pi_j.$$

The following proposition shows that every Π_j is closed under conjugation, proving that condition (1) of Lemma 6 holds.

Proposition 14. For all $i \in I$, the sets Π_i , $i \in I$, and $\Pi_{0,r}$, where r is a prime divisor of $2m$, are closed under conjugation.

Proof. Fix $i \in I$. If $(x_1, \dots, x_m)\gamma \in \Pi_i$, the element

$$((x_1, \dots, x_m)\gamma)^\gamma = (\tau x_m \tau, x_1, \dots, x_{m-1}) \cdot \gamma$$

belongs to Π_i because

$$\tau x_m \tau \cdot x_1 \dots x_{m-1} \cdot \tau = (x_1 \dots x_m \tau)^{\tau x_m^{-1} \tau} \in B_i,$$

and if $(y_1, \dots, y_m) \in A_n^m$, the element

$$((x_1, \dots, x_m)\gamma)^{(y_1, \dots, y_m)} = (y_1^{-1} x_1 y_2, y_2^{-1} x_2 y_3, \dots, y_{m-1}^{-1} x_{m-1} y_m, y_m^{-1} x_m \tau y_1 \tau) \gamma$$

belongs to Π_i because

$$y_1^{-1} x_1 y_2 \cdot y_2^{-1} x_2 y_3 \cdot \dots \cdot y_{m-1}^{-1} x_{m-1} y_m \cdot y_m^{-1} x_m \tau y_1 \tau \cdot \tau = (x_1 \dots x_m \tau)^{y_1} \in B_i.$$

Since G is generated by A_n^m and γ , this proves that Π_i is closed under conjugation.

We now prove that $\Pi_{0,r}$ is closed under conjugation. The following argument can be applied to the case $r = 2$ when m is odd, so we will assume that either m is even or $r \neq 2$. Let $(x_1, \dots, x_m)\gamma^r \in \Pi_{0,r,\sigma}$. Note that

$$((x_1, \dots, x_m)\gamma^r)^\gamma = (\tau x_m \tau, x_1, \dots, x_{m-1})\gamma^r$$

and we have the following.

$$\begin{aligned} \tau x_m \tau x_r x_{2r} \dots x_{m-r} \tau &= (x_r x_{2r} \dots x_{m-r} x_m \tau)^{\tau x_m^{-1} \tau} \in D_{\sigma(r)} = D_{\sigma\nu^{-1}(1)} \\ x_i x_{i+r} x_{i+2r} \dots x_{i+m-r} \tau &\in D_{\sigma(i)} = D_{\sigma\nu^{-1}(i+1)} \quad \forall i = 1, \dots, r-1. \end{aligned}$$

It follows that $((x_1, \dots, x_m)\gamma^r)^\gamma \in \Pi_{0,r,\sigma\nu^{-1}} \subseteq \Pi_{0,r}$.

For $(y_1, \dots, y_m) \in A_n^m$ we have that $((x_1, \dots, x_m)\gamma^r)^{(y_1, \dots, y_m)}$ equals

$$(y_1^{-1}x_1y_{r+1}, \dots, y_{m-r}^{-1}x_{m-r}y_m, y_{m-r+1}^{-1}x_{m-r+1}\tau y_1\tau, \dots, y_m^{-1}x_m\tau y_r\tau) \cdot \gamma^r.$$

Moreover, if $1 \leq i \leq r$,

$$y_i^{-1}x_iy_{r+i}y_{r+i}^{-1}x_{r+i}y_{2r+i} \cdots y_{m-r+i}^{-1}x_{m-r+i}\tau y_i\tau \cdot \tau = (x_i x_{i+r} x_{i+2r} \cdots x_{i+m-r}\tau)^{y_i}$$

belongs to $D_{\sigma(i)}$. This implies that $\Pi_{0,r}$ is closed under conjugation. \square

Note that to apply Lemma 6 it is not necessary for the sets Π_i , $i \in I$, and $\Pi_{0,r}$, r any prime divisor of $2m$, are conjugacy classes. Despite this, we prove:

Proposition 15. *For all $i \in I$, the sets Π_i , $i \in I$, and $\Pi_{0,r}$, where r is a prime divisor of $2m$, are conjugacy classes.*

Proof. Let $i \in I$. Note that $B_i \not\subseteq A_n$, so there is $z \in A_n$ such that $z\tau \in B_i$. It follows that $\pi := (z, 1, \dots, 1)\gamma \in \Pi_i$. We prove that Π_i is the conjugacy class of π in G . Let $(x_1, \dots, x_m)\gamma \in \Pi_i$, we will prove that this element is conjugate to π in G . There exists $a \in S_n$ with $(x_1 \dots x_m\tau)^a = z\tau$. If $a \notin A_n$, then $b = x_1 \dots x_m\tau a \in A_n$ and $(x_1 \dots x_m\tau)^b = (x_1 \dots x_m\tau)^a$, so we may assume that $a \in A_n$. Set $y_1 := a$ and $y_i := x_i \dots x_m\tau a\tau$ for $i = 2, \dots, m$. Then $((x_1, \dots, x_m)\gamma)^{(y_1, \dots, y_m)}$ equals

$$(y_1^{-1}x_1y_2, y_2^{-1}x_2y_3, \dots, y_{m-1}^{-1}x_{m-1}y_m, y_m^{-1}x_m\tau y_1\tau)\gamma = (z, 1, \dots, 1)\gamma = \pi.$$

Now suppose that m is odd or m is even with $r \neq 2$. We will prove that $\Pi_{0,r}$ is a conjugacy class in G . Since $D_i \not\subseteq A_n$ for all $i = 1, \dots, r$, exist $x_1, \dots, x_r \in A_n$ such that $x_i\tau \in D_i$ for all $i = 1, \dots, r$, therefore

$$g = (x_1, \dots, x_r, 1, \dots, 1)\gamma^r \in \Pi_{0,r}.$$

We will show that $\Pi_{0,r}$ is the conjugacy class of g . For this, it is sufficient to show that $|G : C_G(g)| = |\Pi_{0,r}|$, because g belongs to $\Pi_{0,r}$, which is closed by conjugation, and $|G : C_G(g)|$ is the size of the conjugacy class of g in G .

Let $H = C_G(g)$ and $N = A_n^m$. We will initially show that $HN < G$. Suppose by contradiction that $HN = G$. So there are $h \in H$, $n \in N$ such that $hn = \gamma$. It follows that

$$h = \gamma n^{-1} = \gamma n^{-1} \gamma^{-1} \gamma \in N\gamma,$$

because $N \trianglelefteq G$. Therefore $h \in H \cap N\gamma$, i. e., $H \cap N\gamma \neq \emptyset$.

Consider then $(y_1, \dots, y_m)\gamma \in H \cap N\gamma$. We have $((x_1, \dots, x_r, 1, \dots, 1)\gamma^r)^{(y_1, \dots, y_m)\gamma}$ equals

$$(\tau y_m^{-1} \tau y_r, y_1^{-1} x_1 y_{r+1}, \dots, y_r^{-1} x_r y_{2r}, y_{r+1}^{-1} y_{2r+1}, \dots, y_{m-r}^{-1} y_m, y_{m-r+1}^{-1} \tau y_1 \tau, \dots, y_{m-1}^{-1} \tau y_{r-1} \tau)$$

From the $r+1$ -th coordinate we get that $y_r = x_r y_{2r}$ and from the $r+2$ -th coordinate to the $m-r+1$ -th coordinate we get that $y_i = y_{i+r}$ if $r+1 \leq i \leq m-r$. Then

$$x_1 \tau = \tau y_m^{-1} \tau y_r \tau = \tau y_m^{-1} \tau x_r y_{2r} \tau = \tau y_m^{-1} \tau x_r y_m \tau = (x_r \tau)^{\tau y_m \tau},$$

that is, x_1 and x_r are conjugate, and this implies that $D_1 = D_r$, contradiction. Therefore $HN < G$.

Let us now calculate the order of $H \cap N$. For that consider $(y_1, \dots, y_m) \in H \cap N$. We have already seen that $(x_1, \dots, x_r, 1, \dots, 1)\gamma^r)^{(y_1, \dots, y_m)}$ equals

$$(y_1^{-1} x_1 y_{r+1}, \dots, y_r^{-1} x_r y_{2r}, y_{r+1}^{-1} y_{2r+1}, \dots, y_{m-r}^{-1} y_m, y_{m-r+1}^{-1} \tau y_1 \tau, \dots, y_m^{-1} \tau y_r \tau) \gamma^r.$$

Then for all $1 \leq i \leq r$,

$$x_i \tau = y_i^{-1} x_i \tau y_i.$$

This means that for $1 \leq i \leq r$,

$$y_i \in C_{S_n}(x_i \tau).$$

Since the order of $H \cap N$ is the number of choices for (y_1, \dots, y_m) , we get that

$$|H \cap N| = \prod_{i=1}^r |A_n \cap C_{S_n}(x_i \tau)| = \prod_{i=1}^r \frac{1}{2} |C_{S_n}(x_i \tau)|.$$

Let's now show that $HN = N\langle \gamma^r \rangle$. First, $HN \supseteq N\langle \gamma^r \rangle$ because $g \in H$. Furthermore, $N\langle \gamma^r \rangle$ is a maximal subgroup of G because it has prime index r . Since $HN < G$, it follows that $HN = N\langle \gamma^r \rangle$.

Then

$$\frac{N\langle\gamma^r\rangle}{N} = \frac{HN}{N} \cong \frac{H}{H \cap N},$$

and as the order of $\frac{N\langle\gamma^r\rangle}{N}$ is $2m/r$, we get that

$$|H| = (2m/r) \cdot |H \cap N| = (2m/r) \cdot \prod_{i=1}^r \frac{1}{2} |C_{S_n}(x_i\tau)|.$$

We deduce that

$$|G : H| = \frac{|G|}{|H|} = \frac{2m \cdot |A_n|^m}{(2m/r) \cdot (1/2)^r \cdot \prod_{i=1}^r n! / |D_i|} = r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^r |D_i| = |\Pi_{0,r}|.$$

It follows that $g \in \Pi_{0,r}$ has $|\Pi_{0,r}|$ conjugated in G . Since $\Pi_{0,r}$ is closed by conjugation, it follows that $\Pi_{0,r}$ is exactly the conjugacy class of g in G , proving that $\Pi_{0,r}$ is a conjugacy class in G .

Now suppose m odd. It remains to be proven that $\Pi_{0,2}$ is a conjugacy class in G . Let $x_1 \in C \subseteq A_n$, then $g = (x_1, 1, \dots, 1)\gamma^2 \in \Pi_{0,2}$. Let $H = C_G(g)$ and $N = A_n^m$, let's calculate $|H \cap N|$. Let $(y_1, \dots, y_m) \in H \cap N$, then $((x_1, 1, \dots, 1)\gamma^2)^{(y_1, \dots, y_m)}$ equals

$$(y_1^{-1}x_1y_3, y_2^{-1}y_4, y_3^{-1}y_5, \dots, y_{m-2}^{-1}y_m, y_{m-1}^{-1}\tau y_1\tau, y_m^{-1}\tau y_2\tau).$$

This implies,

$$x_1^{-1}y_1x_1 = y_3 = \dots = y_m = \tau y_2\tau = \tau y_4\tau = \dots = \tau y_{m-1}\tau = y_1.$$

Therefore $x_1y_1 = y_1x_1$, i. e., $y_1 \in C_{A_n}(x_1)$. By the equations above, the choice of y_1 determines the choice of all others y_i . Therefore

$$|H \cap N| = |C_{A_n}(x_1)| = \frac{|A_n|}{|C|}.$$

Now, if $HN \neq G$ then $HN = N\langle\gamma^2\rangle$. In fact, $g \in H$ which implies that $N\langle\gamma^2\rangle \subseteq HN$ and $|G : N\langle\gamma^2\rangle| = 2$ because $G = N\langle\gamma\rangle$. Then $N\langle\gamma^2\rangle$ is a subgroup of index 2 of G with $N\langle\gamma^2\rangle \subseteq HN \neq G$, therefore $HN = N\langle\gamma^2\rangle$. Then the size of the conjugacy class of g in G is $|G : H|$ which is

$$\begin{aligned} |G : H| &= \frac{|G|}{|H|} = \frac{2 \cdot |HN|}{|H|} = \frac{2 \cdot |N|}{|H \cap N|} = \frac{2 \cdot |A_n|^m}{\frac{|A_n|}{|C|}} \\ &= 2 \cdot |A_n|^{m-1}|C| > |A_n|^{m-1}|C| = |\Pi_{0,2}|. \end{aligned}$$

This contradicts the fact that $\Pi_{0,2}$ is closed for conjugation. Therefore $HN = G$.

Therefore, the size of the conjugacy class of g in G is

$$|G : H| = \frac{|G|}{|H|} = \frac{|HN|}{|H|} = \frac{|N|}{|H \cap N|} = \frac{|A_n|^m}{\frac{|A_n|}{|C|}} = |A_n|^{m-1}|C| = |\Pi_{0,2}|.$$

This concludes the proof. \square

2.3.3 The covering \mathcal{C}

For $i \in I$, $i \neq -1$, define

$\mathcal{E}_i := \{\text{maximal intransitive subgroups of } A_n \text{ whose orbits have size } i \text{ and } n-i\}$,

and let

$\mathcal{E}_{-1} := \{\text{maximal imprimitive subgroups of } A_n \text{ with 2 blocks}\}$.

For all $i \in I$, let

$$\mathcal{F}_i := \{N_{S_n}(M) : M \in \mathcal{E}_i\},$$

and define

$$\mathcal{E} := \bigcup_{i \in I} \mathcal{E}_i, \quad \mathcal{F} := \bigcup_{i \in I} \mathcal{F}_i.$$

Note that $\{A_n\} \cup \mathcal{F}$ is a covering of S_n , as observed in [40].

By [40, Lemma 5.2], for $n \equiv 0 \pmod{6}$, $n \geq 30$ and $i \in I$, the only subgroups in \mathcal{F} that contain elements of B_i are the ones belonging to \mathcal{F}_i , so that the elements of $\bigcup_{i \in I} B_i$ are partitioned by the subgroups in \mathcal{F} . Moreover \mathcal{E}_i and \mathcal{F}_i are conjugacy classes of subgroups of S_n for all $i \in I$.

Let $G = G_{n,m}$ be the group defined in Section 2.3.1, that is, $G = A_n^m \rtimes \langle \gamma \rangle$, where $\gamma = (1, \dots, 1, \tau)\delta$, $\tau = (1 \ 2)$ and $\delta = (1 \dots m)$.

For $i \in I$, define

$$\mathcal{M}_i := \{H \leq G : H = N_G(M^{a_1} \times \dots \times M^{a_m}), a_1, \dots, a_m \in A_n, \\ M \in \mathcal{E}_i, N_{S_n}(M) \cap B_i \neq \emptyset\}.$$

By [5, Proposition 1.1.44] and [27], H is a maximal subgroup of G supplementing the socle $N = A_n^m$ of G . Moreover, $H \cap N$ is conjugate to M^m in N . It follows that $|H| = 2m \cdot |M|^m$ and H has $|G : H| = |A_n : M|^m$ conjugates in G .

For every prime divisor r of $2m$, set

$$\mathcal{M}_{0,r} := \{M_{0,r}\},$$

where $M_{0,r} = A_n^m \rtimes \langle \gamma^r \rangle$ is a normal subgroup of G of index r .

Let

$$\mathcal{C} := \bigcup_{j \in J} \mathcal{M}_j.$$

The size of \mathcal{C} equals the claimed value for $\sigma(G)$ in the statement of Theorem 1.

Proposition 16. \mathcal{C} is a covering of G .

Proof. Let $g = (x_1, \dots, x_m)\gamma^k \in G$ where $x_i \in A_n$ for all i . If $(k, 2m) \neq 1$ then g belongs to one of the $\alpha(2m)$ subgroups of G containing the socle, now suppose that $(k, 2m) = 1$, in particular k is odd. For $d \in \{1, \dots, m\}$ define τ_d to be τ if $d > m - k$, and 1 if $d \leq m - k$. Since k, m are coprime, the set of numbers $\{1 + ik : i = 0, \dots, m - 1\}$, reduced modulo m , equals $\{1, \dots, m\}$, so the following definition makes sense. Define $b_1 := 1$ and

$$b_{1+ik} := x_1\tau_1x_{1+k}\tau_{1+k} \cdots x_{1+(i-1)k}\tau_{1+(i-1)k}, \quad i = 1, \dots, m - 1,$$

where the subscripts are considered modulo m . Set

$$x := x_1\tau_1x_{1+k}\tau_{1+k}x_{1+2k}\tau_{1+2k} \cdots x_{1+(m-1)k}\tau_{1+(m-1)k}.$$

Since $x \equiv \tau^k \pmod{A_n}$ and k is odd, $x \notin A_n$. Since $\{A_n\} \cup \mathcal{F}$ is a covering of S_n , there exists $M \in \mathcal{E}$ such that $x \in H := N_{S_n}(M)$. We claim that $(x_1, \dots, x_m)\gamma^k$ belongs to $N_G(M^{b_1} \times M^{b_2} \times \cdots \times M^{b_m}) \in \mathcal{C}$. This is equivalent to saying that $M^{b_1} \times M^{b_2} \times \cdots \times M^{b_m}$ equals

$$\begin{aligned} (M^{b_1} \times M^{b_2} \times \cdots \times M^{b_m})^{(x_1, \dots, x_m)\gamma^k} &= (M^{b_1x_1} \times M^{b_2x_2} \times \cdots \times M^{b_mx_m})\gamma^k \\ &= M^{b_{m-k+1}x_{m-k+1}\tau} \times \cdots \times M^{b_mx_m\tau} \times M^{b_1x_1} \times \cdots \times M^{b_{m-k}x_{m-k}}. \end{aligned}$$

That is, $b_{m-k+i}x_{m-k+i}\tau b_i^{-1} \in H$ for $i \in \{1, \dots, k\}$ and $b_i x_i b_{i+k}^{-1} \in H$ for $i \in \{1, \dots, m-k\}$. This can be written as $b_d x_d \tau_d b_{d+k}^{-1} \in H$ for all $d \in \{1, \dots, m\}$, equivalently,

$$\ell_i := b_{1+ik} x_{1+ik} \tau_{1+ik} b_{1+(i+1)k}^{-1} \in H \quad \forall i \in \{1, \dots, m\}.$$

We have $\ell_i = 1$ for $i \neq m-1$ and $\ell_{m-1} = x$. They all belong to H . \square

Proposition 17. *The sets \mathcal{M}_i , $i \in I$, are conjugacy classes of subgroups of G .*

Proof. A given subgroup in \mathcal{M}_i is A_n^m -conjugate to $H = N_G(M^m)$ where $M \in \mathcal{E}_i$, so since every member of \mathcal{E}_i is an A_n -conjugate of M , being $N_{S_n}(M)A_n = S_n$, we only need to show that $H^\gamma = N_G(M^\tau \times M^{m-1})$ is A_n^m -conjugate to H . This follows from the fact that M^τ is A_n -conjugate to M , being $N_{S_n}(M)A_n = S_n$. \square

2.3.4 Maximal subgroups of $G_{n,m}$

We will now describe the maximal subgroups of $G = G_{n,m}$, the group defined in Section 2.3.1, that is, $G = A_n^m \rtimes \langle \gamma \rangle$, where $\gamma = (1, \dots, 1, \tau)\delta$, $\tau = (1 \ 2)$ and $\delta = (1 \dots m)$. A reference for the following discussion is Chapter 1.

The maximal subgroups of G containing the socle $N = A_n^m = \text{soc}(G)$ are the $M_{0,r} = A_n^m \rtimes \langle \gamma^r \rangle$, where r is any prime divisor of $2m$.

Let U be a maximal subgroup of G not containing N , so that $UN = G$. Observe that $U \cap N \neq \{1\}$. Indeed, if by contradiction $U \cap N = \{1\}$, then $U \cong G/N$ would be cyclic, generated by a coset uN , therefore the only proper subgroup of G containing u would be U , and this contradicts the fact that \mathcal{C} is a covering of G whose members are not cyclic. Then U can be of one of the following two types.

The first type is $U = N_G(U \cap N)$ where

$$U \cap N = M \times M^{a_2} \times \dots \times M^{a_m}, \quad a_2, \dots, a_m \in A_n,$$

and M is the intersection between A_n and a maximal subgroup of S_n . In this first case, U is called a maximal subgroup of product type (see [5, Proposition 1.1.44, Definition 1.1.45]).

The second type consists of maximal subgroups of diagonal type (see [5, Proposition 1.1.55]). Fix a partition $\{P_1, \dots, P_k\}$ of $\Omega = \{1, \dots, m\}$ and write

$$P_i = \{a_{ij} : j = 1, \dots, r_i\}.$$

Given a collection of automorphisms φ_{ij} of A_n , with $i = 1, \dots, k$ and $j = 2, \dots, r_i$, let Δ_φ be the set of m -tuples $(x_1, \dots, x_m) \in A_n^m$ with the property that

$$x_{a_{ij}} = x_{a_{i1}}^{\varphi_{ij}},$$

for all i, j . Then we set U to be the normalizer of Δ_φ in G . If U supplements N , there is in U an element $u = (y_1, \dots, y_m)\delta$ where each y_i belongs to S_n and it is easy to see that the partition P is stabilized by δ . If U is a maximal subgroup of G , then we may assume that P is minimal, with respect to the relation of refinement, among the nontrivial partitions stabilized by δ , in other words

$$\Delta_\varphi = \{(y_1, \dots, y_{m/t}, y_1^{\varphi_{1,2}}, \dots, y_{m/t}^{\varphi_{m/t,2}}, \dots, y_1^{\varphi_{1,t}}, \dots, y_{m/t}^{\varphi_{m/t,t}}) : y_1, \dots, y_{m/t} \in A_n\}$$

where t is a prime divisor of m , $\varphi_{i,j}$ is an automorphism of A_n for $1 \leq i \leq m/t$, $2 \leq j \leq t$, and the matrix $(\varphi_{i,j})_{i,j}$ is denoted by φ . If U is a maximal subgroup of G , supplementing the socle N , and of the form $N_G(\Delta_\varphi)$ with φ as above then U is called a maximal subgroup of diagonal type. If this is the case, then $U \cap N = \Delta_\varphi$.

We now explicit two generators of G . Recall that the symmetric group S_n is 2-generated, and

$$\langle (12), (12 \dots n) \rangle = S_n.$$

Therefore there exist $x_1, x_2 \in A_n$ such that $\langle x_1\tau, x_2\tau \rangle = S_n$ (recall that $\tau = (12)$). For example, we can choose $x_1 = 1$ and $x_2 = (12 \dots n)(12)$ for n even, $x_2 = (12 \dots n)$ for n odd.

Proposition 18. *Let $x_1, x_2 \in A_n$ be such that $\langle x_1\tau, x_2\tau \rangle = S_n$. Let $\alpha_i = (x_i, 1, \dots, 1)\gamma$ for $i = 1, 2$. Then $\langle \alpha_1, \alpha_2 \rangle = G$.*

Proof. Suppose by contradiction that $\langle \alpha_1, \alpha_2 \rangle \neq G$. Then $\langle \alpha_1, \alpha_2 \rangle \subseteq H$ where H is a maximal subgroup of G . The subgroup H is not one of the $M_{0,r}$ subgroups since the elements α_1, α_2 have the permutation part γ .

Suppose that H is a maximal subgroup of product type, that is, $H = N_G(M \times M^{a_2} \times \dots \times M^{a_m})$, $a_2, \dots, a_m \in A_n$, and M is the intersection between A_n and a maximal subgroup of S_n . Then, for $i = 1, 2$, $M \times M^{a_2} \times \dots \times M^{a_m}$ equals

$$(M^{x_i} \times M^{a_2} \times \dots \times M^{a_m})^\gamma = M^{a_m\tau} \times M^{x_i} \times M^{a_2} \times \dots \times M^{a_{m-1}}.$$

Therefore

$$a_m\tau, x_i a_2^{-1}, a_2 a_3^{-1}, \dots, a_{m-1} a_m^{-1} \in N_{S_n}(M).$$

Multiplying these elements starting from $x_i a_2^{-1}$, we obtain that $x_1\tau, x_2\tau \in N_{S_n}(M)$, and therefore $S_n = \langle x_1\tau, x_2\tau \rangle \subseteq N_{S_n}(M) < S_n$, contradiction.

Suppose now that H is a maximal subgroup of diagonal type, say $N_G(\Delta_\varphi)$. We will use the notation used in the first part of this section. If $m = t$, then

$$\Delta_\varphi = \{(y, y^{\varphi_2}, \dots, y^{\varphi_t}) : y \in A_n\}.$$

Since $\alpha_i \in N_G(\Delta_\varphi)$, for $i = 1, 2$ we have that $(y, y^{\varphi_2}, \dots, y^{\varphi_t})^{\alpha_i}$ equals

$$(y, y^{\varphi_2}, \dots, y^{\varphi_t})^{(x_i, 1, \dots, 1)\gamma} = (y^{x_i}, y^{\varphi_2}, \dots, y^{\varphi_t\tau})^\delta = (y^{\varphi_t\tau}, y^{x_i}, y^{\varphi_2}, \dots, y^{\varphi_{t-1}})$$

for all $y \in A_n$. By the definition of Δ_φ ,

$$y^{\varphi_t\tau\varphi_2} = y^{x_i}, \quad \forall y \in A_n, \quad i = 1, 2,$$

that is

$$\varphi_t\tau\varphi_2 = x_i, \quad i = 1, 2.$$

This implies that $x_1 = \varphi_t\tau\varphi_2 = x_2$, contradicting the fact that $\langle x_1\tau, x_2\tau \rangle = S_n$. If $m/t > 1$,

$$\Delta_\varphi = \{(y_1, \dots, y_{m/t}, y_1^{\varphi_{1,2}}, \dots, y_{m/t}^{\varphi_{m/t,2}}, \dots, y_1^{\varphi_{1,t}}, \dots, y_{m/t}^{\varphi_{m/t,t}}) : y_1, \dots, y_{m/t} \in A_n\}.$$

We have

$$\begin{aligned} & (y_1, \dots, y_{m/t}, y_1^{\varphi_{1,2}}, \dots, y_{m/t}^{\varphi_{m/t,2}}, \dots, y_1^{\varphi_{1,t}}, \dots, y_{m/t}^{\varphi_{m/t,t}})^{\alpha_i} \\ &= (y_1^{x_i}, \dots, y_{m/t}, y_1^{\varphi_{1,2}}, \dots, y_{m/t}^{\varphi_{m/t,2}}, \dots, y_1^{\varphi_{1,t}}, \dots, y_{m/t}^{\varphi_{m/t,t}\tau})^\delta \\ &= (y_{m/t}^{\varphi_{m/t,t}\tau}, y_1^{x_i}, \dots, y_{m/t}, y_1^{\varphi_{1,2}}, \dots, y_{m/t}^{\varphi_{m/t,2}}, \dots, y_1^{\varphi_{1,t}}, \dots, y_{m/t-1}^{\varphi_{m/t-1,t}}). \end{aligned}$$

Since $\alpha_i \in N_G(\Delta_\varphi)$, for $i = 1, 2$ we have

$$y_1^{x_i \varphi_{2,2}} = y_1^{\varphi_{1,2}}, \quad \forall y_1 \in A_n, \quad i = 1, 2,$$

that is

$$x_i = \varphi_{1,2} \varphi_{2,2}^{-1}, \quad i = 1, 2.$$

This implies that $x_1 = x_2$, contradicting the fact that $\langle x_1 \tau, x_2 \tau \rangle = S_n$. \square

2.3.5 Proof of Theorem 1

Let $G = G_{n,m} = A_n^m \rtimes \langle \gamma \rangle$, where $\gamma = (1, \dots, 1, \tau)\delta$, $\tau = (1 \ 2)$ and $\delta = (1 \dots m)$. Our objective in this section is to prove our first Theorem:

Theorem. [2, Theorem 1] *Let $G = G_{n,m}$, for $n \geq 30$ divisible by 6 and $m \geq 2$. Denote by $\alpha(x)$ the number of distinct prime factors of the positive integer x . Then*

$$\sigma(G) = \alpha(2m) + \left(\frac{1}{2} \binom{n}{n/2} \right)^m + \sum_{i=1}^{n/3-1} \binom{n}{i}^m.$$

Moreover, G has a unique minimal covering consisting of maximal subgroups.

In the following discussion, we fix a subgroup M of A_n such that $N_G(M^m)$ is a maximal subgroup of G which supplements the socle $N = \text{soc}(G)$, in other words $N_G(M^m)N = G$.

Lemma 8. $N_{S_n}(M)A_n = S_n$, in particular $N_{S_n}(M) \not\subseteq A_n$.

Proof. Let $\alpha \in S_n$. If $\alpha \in A_n$ then $\alpha \in N_{S_n}(M)A_n$, so now assume that $\alpha \notin A_n$. Then $\alpha\tau \in A_n$ and so $(\alpha, \dots, \alpha) = (\alpha\tau, \dots, \alpha\tau)(\tau, \dots, \tau) \in G$, being $(\tau, \dots, \tau) = \gamma^m$. By assumption, we can write $(\alpha, \dots, \alpha) = nh$, where $n = (a_1, \dots, a_m) \in A_n^m$ and $h = (b_1, \dots, b_m)\gamma^k \in N_G(M^m)$. It follows that $k = 0$ and hence $b_i \in N_{S_n}(M)$ for all $i = 1, \dots, m$. Therefore $\alpha = a_1 b_1 \in A_n N_{S_n}(M)$. \square

Lemma 9. *Let $g \in G$ and let r be a prime divisor of $2m$. If either m is even or $r \neq 2$, then*

$$|N_G(M^m)^g \cap \Pi_{0,r}| = r \cdot \left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-r} \cdot \prod_{i=1}^r |D_i \cap N_{S_n}(M)|.$$

If m is odd, then

$$|N_G(M^m)^g \cap \Pi_{0,2}| = \left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-1} \cdot |C \cap N_{S_n}(M)|.$$

Proof. Since $\Pi_{0,r}$ is closed under conjugation, the size of $N_G(M^m)^g \cap \Pi_{0,r}$ equals the size of $N_G(M^m) \cap \Pi_{0,r}$, therefore we may assume that $g = 1$. Assume first that either m is even or $r \neq 2$. We will compute $|N_G(M^m) \cap \Pi_{0,r,\sigma}|$ for each $\sigma \in \langle \nu \rangle$ and sum all the contributions. Fix $\sigma \in \langle \nu \rangle$. Let $(x_1, \dots, x_m)\gamma^r \in N_G(M^m) \cap \Pi_{0,r,\sigma}$, then M^m equals

$$(M \times \dots \times M)^{(x_1, \dots, x_m)\gamma^r} = M^{x_{m-r+1}\tau} \times \dots \times M^{x_m\tau} \times M^{x_1} \times \dots \times M^{x_{m-r}}.$$

So $x_{m-r+1}\tau, \dots, x_m\tau \in N_{S_n}(M) \cap (S_n \setminus A_n)$ and $x_1, \dots, x_{m-r} \in N_{S_n}(M) \cap A_n$. Since $N_{S_n}(M)$ is not contained in A_n , the sets $N_{S_n}(M) \cap A_n$ and $N_{S_n}(M) \cap (S_n \setminus A_n)$ have the same cardinality. Since $(x_1, \dots, x_m)\gamma^r \in \Pi_{0,r}$, the x_i 's must also satisfy the equations of the definition of $\Pi_{0,r,\sigma}$. So for each equation

$$x_i x_{i+r} \dots x_{i+m-r}\tau \in D_{\sigma(i)},$$

where $i = 1, \dots, r$, we can freely choose the elements $x_{i+r}, \dots, x_{i+m-r}$, with

$$|N_{S_n}(M) \cap A_n| = \frac{1}{2} |N_{S_n}(M)|$$

choices for each, and only the elements x_i , $i = 1, \dots, r$, need to be chosen in order to satisfy the equation defining $\Pi_{0,r,\sigma}$, which is $x_i z_i \in D_{\sigma(i)}$, where $z_i = x_{i+r} \dots x_{i+m-r}\tau \in N_{S_n}(M)$. Since

$$D_{\sigma(i)} z_i^{-1} \cap N_{S_n}(M) = (D_{\sigma(i)} \cap N_{S_n}(M)) z_i^{-1},$$

there are $|D_{\sigma(i)} \cap N_{S_n}(M)|$ choices for each x_i , $i = 1, \dots, r$, and the result follows.

Assume now that m is odd. Let $(x_1, \dots, x_m)\gamma^2 \in N_G(M^m) \cap \Pi_{0,2}$. Then M^m equals

$$(M \times \dots \times M)^{(x_1, \dots, x_m)\gamma^2} = M^{x_{m-1}\tau} \times M^{x_m\tau} \times M^{x_1} \times \dots \times M^{x_{m-2}}.$$

So $x_{m-1}\tau, x_m\tau \in N_{S_n}(M) \cap (S_n \setminus A_n)$ and $x_1, \dots, x_{m-2} \in N_{S_n}(M) \cap A_n$. Since $N_{S_n}(M)$ is not contained in A_n , we have $\frac{1}{2}|N_{S_n}(M)|$ choices for each of x_{m-1} and x_m . Now we can choose x_2, \dots, x_{m-2} freely in $N_{S_n}(M) \cap A_n$ and we need to choose x_1 in order to satisfy the equation that defines $\Pi_{0,2}$, which is $x_1 t \in C$, where $t = x_3 x_5 \dots x_m \tau x_2 x_4 \dots x_{m-1} \tau \in N_{S_n}(M)$. We can choose x_1 freely in $C t^{-1} \cap N_{S_n}(M) = (C \cap N_{S_n}(M)) t^{-1}$, so we have $|C \cap N_{S_n}(M)|$ choices for x_1 . The result follows. \square

Corollary 1. *Assume that either m is even or $r \neq 2$. Then $N_G(M^m) \cap \Pi_{0,r} = \emptyset$ if and only if $N_{S_n}(M) \cap D_i = \emptyset$ for at least one $i \in \{1, \dots, r\}$. Moreover, if m is odd and $r = 2$, then $N_G(M^m) \cap \Pi_{0,2} = \emptyset$ if and only if $N_{S_n}(M) \cap C = \emptyset$.*

Lemma 10. *If $i \in I$, then $|N_G(M^m) \cap \Pi_i| = \left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M)|$.*

Proof. Let $(x_1, \dots, x_m)\gamma \in N_G(M^m) \cap \Pi_i$, then M^m equals

$$(M^m)^{(x_1, \dots, x_m)\gamma} = (M^{x_1} \times \dots \times M^{x_m})^\gamma = M^{x_m\tau} \times M^{x_1} \times \dots \times M^{x_{m-1}}.$$

So $x_m\tau \in N_{S_n}(M) \cap (S_n \setminus A_n)$ and $x_1, \dots, x_{m-1} \in N_{S_n}(M) \cap A_n$. Since $N_{S_n}(M)$ is not contained in A_n , the number of choices for x_m is $\frac{1}{2}|N_{S_n}(M)|$. Now we can choose x_2, \dots, x_{m-1} freely in $N_{S_n}(M) \cap A_n$ and we need to choose x_1 in order to satisfy the equation that defines Π_i , which is $x_1 t \in B_i$, where $t = x_2 \dots x_{m-1} \tau \in N_{S_n}(M)$. In other words, we can choose x_1 freely in $B_i t^{-1} \cap N_{S_n}(M) = (B_i \cap N_{S_n}(M)) t^{-1}$ so the number of choices for x_1 is $|B_i \cap N_{S_n}(M)|$. The result follows. \square

Corollary 2. *If $i \in I$, then $N_G(M^m) \cap \Pi_i = \emptyset$ if and only if $B_i \cap N_{S_n}(M) = \emptyset$.*

The following proposition implies that condition (2) of Lemma 6 holds.

Proposition 19. *Let $\pi \in \Pi$, then there is a unique $L \in \mathcal{C}$ such that $\pi \in L$.*

Proof. If $\pi \in \Pi_{0,r}$ for some prime r that divides $2m$, then $M_{0,r}$ is the only subgroup in \mathcal{C} that contains π . This follows from Corollary 1 and the fact that no subgroup in \mathcal{F} has non-empty intersection with all sets D_1, \dots, D_r , because n -cycles do not belong to intransitive subgroups and $(n-2)$ -cycles do not stabilize partitions with 2 blocks.

Now suppose that $\pi \in \Pi_i$ for some $i \in I$. Then

$$\pi = (x_1, \dots, x_m)\gamma,$$

with $x_1 \dots x_m \tau \in B_i$. In particular $\pi \notin M_{0,r}$ for every prime r that divides $2m$.

There is a unique $H \in \mathcal{F}$ such that $x_1 \dots x_m \tau \in H$ and $H = N_{S_n}(M)$ where $M = H \cap A_n \in \mathcal{E}$. Suppose that $\pi = (x_1, \dots, x_m)\gamma$ belongs to $N_G(M^{a_1} \times \dots \times M^{a_m})$. Then $M^{a_1} \times \dots \times M^{a_m}$ equals

$$(M^{a_1} \times \dots \times M^{a_m})^{(x_1, \dots, x_m)\gamma} = M^{a_m x_m \tau} \times M^{a_1 x_1} \times \dots \times M^{a_{m-1} x_{m-1}}.$$

So, for i with $1 \leq i \leq m-1$, $a_i x_i a_{i+1}^{-1} \in H$ and $a_m x_m \tau a_1^{-1} \in H$. Multiplying all these elements starting from the i -th one, we have

$$a_i x_i x_{i+1} \dots x_m \tau x_1 x_2 \dots x_{i-1} a_i^{-1} \in H,$$

which can be written as

$$(x_1 \dots x_m \tau)^{x_1 \dots x_{i-1}} = x_i x_{i+1} \dots x_m \tau x_1 x_2 \dots x_{i-1} \in H^{a_i}.$$

In particular $x_1 \dots x_m \tau \in H^{a_1}$. Since \mathcal{F} is closed under conjugation, the uniqueness of H implies that $H^{a_1} = H$, therefore $a_1 \in N_{S_n}(H) = H$, being H a maximal subgroup of S_n . Now we can rewrite the above equations as

$$a_i \in H x_1 x_2 \dots x_{i-1}, \quad \forall i = 2, \dots, m.$$

It follows that $M^{a_1} = M$ and $M^{a_i} = M^{x_1 \dots x_{i-1}}$ for all $i = 2, \dots, m$, hence the only subgroup in \mathcal{C} that contains π is

$$N_G(M \times M^{x_1} \times M^{x_1 x_2} \times \dots \times M^{x_1 \dots x_{m-1}}).$$

This concludes the proof. □

In order to conclude the proof of Theorem 1, we are left to show that condition (3) of Lemma 6 holds, in other words that $c(H) < 1$ for every maximal subgroup H of G not in \mathcal{C} . This will be done in Proposition 20. Its proof will make use of the following lemmas.

Lemma 11. *For $n \geq 30$, the value of $|\Pi_{0,2}|$ is smallest when m is even. Moreover, if $g \in G$, then*

$$\frac{|N_G(M^m)^g \cap \Pi_{0,2}|}{|\Pi_{0,2}|} \leq \frac{2n(n-2)}{|S_n : N_{S_n}(M)|^m}.$$

Proof. We have

$$|D_1| = \frac{n!}{2(n-2)}, \quad |D_2| = (n-1)!, \quad |C| = \frac{n!}{p(n-p)},$$

and

$$|\Pi_{0,2}| = \begin{cases} 2|A_n|^{m-2}|D_1||D_2| = \frac{4|A_n|^m}{n(n-2)}, & \text{if } m \text{ is even.} \\ |A_n|^{m-1}|C| = \frac{4|A_n|^m}{2p(n-p)}, & \text{if } m \text{ is odd.} \end{cases}$$

Note that

$$2p(n-p) < 2(2n/3)^2 \leq n(n-2),$$

being $n/3 < p < 2n/3$ and $n \geq 30$. So the value of $|\Pi_{0,2}|$ is smallest when m is even.

We now prove the stated inequality. Since $\Pi_{0,2}$ is closed under conjugation, we may assume that $g = 1$. By Lemma 9,

$$\frac{|N_G(M^m) \cap \Pi_{0,2}|}{|\Pi_{0,2}|} = \begin{cases} \left(\frac{|N_{S_n}(M)|}{|S_n|} \right)^{m-2} \cdot \frac{|D_1 \cap N_{S_n}(M)||D_2 \cap N_{S_n}(M)|}{|D_1||D_2|}, & \text{if } m \text{ is even} \\ \left(\frac{|N_{S_n}(M)|}{|S_n|} \right)^{m-1} \cdot \frac{|C \cap N_{S_n}(M)|}{|C|}, & \text{if } m \text{ is odd} \end{cases}$$

The inequality in the statement follows by using the fact that the size of the intersection of any one of D_1 , D_2 , C with $N_{S_n}(M)$ is at most $|N_{S_n}(M)|$. \square

Lemma 12. *If d is a divisor of n such that $2 \leq d \leq n/2$ then $(n/d)!^d \cdot d! \leq 2(n/2)!^2$.*

Proof. We do as in the proof of [33, Lemma 2.1]. Assume first that $d \leq n/d$.

$$\begin{aligned} (n/d)!^d \cdot d! &\leq (n/d)!^2 \cdot 2 \cdot ((n/d)! \cdot d)^{d-2} \leq (n/d)!^2 \cdot 2 \cdot ((n/d)! \cdot n/d)^{d-2} \\ &\leq (n/d)!^2 \cdot 2 \cdot ((n/d)^{n/d})^{d-2} = (n/d)!^2 \cdot 2 \cdot (n/d)^{2(n/2-n/d)} \\ &\leq (n/d)!^2 \cdot ((n/d) + 1)^2 \cdot \dots \cdot (n/2)^2 \cdot 2 = 2(n/2)!^2, \end{aligned}$$

where, in the fourth inequality, we used that $r! \leq r^{r-1}$, for all $r \geq 2$.

Suppose now that $d > n/d$. Since $2 \leq n/d \leq n/2$, exchanging the role of n/d and d in the above inequality we obtain

$$d!^{n/d} \cdot (n/d)! \leq 2(n/2)!^2.$$

If $a > b \geq 2$ are integers, then $a!^b \cdot b! > b!^a \cdot a!$, since

$$\begin{aligned} a!^{b-1} &= (a \cdot (a-1) \cdot \dots \cdot (b+1))^{b-1} \cdot b!^{b-1} \geq ((b+1)^{(a-b)})^{b-1} \cdot b!^{b-1} \\ &> b^{(a-b)(b-1)} \cdot b!^{b-1} \geq b!^{(a-b)} \cdot b!^{b-1} = b!^{a-1}. \end{aligned}$$

Applying this to $a = d$, $b = n/d$ we have

$$(n/d)!^d \cdot d! < d!^{n/d} \cdot (n/d)! \leq 2(n/2)!^2.$$

This concludes the proof. □

Lemma 13. *Let H be a maximal subgroup of S_n such that $H \notin \mathcal{F}$ and fix $i \in I$, $M \in \mathcal{E}_i$. Then either $|H| \leq |N_{S_n}(M)|$ or $H \cap B_i = \emptyset$.*

Proof. By the O’Nan-Scott Theorem, the maximal subgroups of S_n are of one of the following types: (1) primitive, (2) maximal intransitive, isomorphic to $S_k \times S_{n-k}$ for some $k \in \{1, \dots, n/2 - 1\}$ and (3) maximal imprimitive, isomorphic to $S_a \wr S_b$ for $2 \leq a, b < n$ with $ab = n$. If H is intransitive then $H \cong S_k \times S_{n-k}$ with $n/3 \leq k < n/2$, therefore

$$|H| \leq (n/3)!(2n/3)! \leq (n/3 - 1)!(2n/3 + 1)! \leq |N_{S_n}(M)|$$

if $N_{S_n}(M)$ is intransitive. On the other hand, if $N_{S_n}(M)$ is transitive, then $i = -1$ and $H \cap B_{-1} = \emptyset$.

Now suppose that H is transitive. If H is imprimitive then $|H| = (n/d)!^d \cdot d!$, where d is a divisor of n , $d \neq 1, 2, n$. By Lemma 12, if $N_{S_n}(M)$ is imprimitive, then

$$|H| = (n/d)!^d \cdot d! \leq (n/2)!^2 \cdot 2! = |N_{S_n}(M)|.$$

If $N_{S_n}(M)$ is intransitive, then

$$|H| = (n/d)!^d \cdot d! \leq (n/2)!^2 \cdot 2! \leq (n/3 - 1)!(2n/3 + 1)! \leq |N_{S_n}(M)|.$$

If H is primitive then either $H = A_n$, in which case $H \cap B_i = \emptyset$, or $H \neq A_n$, in which case $|H| < 4^n$ by [37]. Since $n \geq 30$ we have

$$4^n \leq (n/2)!^2 \cdot 2 \leq (n/3 - 1)!(2n/3 + 1)!$$

and the result follows. □

We are now ready to prove that $c(H) < 1$ for every maximal subgroup H of G not in \mathcal{C} .

Proposition 20. *Let H be a maximal subgroup of G not in \mathcal{C} . Then $c(H) < 1$.*

Proof. Assume H has product type. Then H is conjugate to $N_G(M^m)$ where M is the intersection between A_n and a maximal subgroup of S_n not of the form A_n nor $S_{n/2} \wr S_2$ nor $S_i \times S_{n-i}$, $i = 1, 2, \dots, n/3 - 1$, so that

$$|N_{S_n}(M)| \leq (n/3)! (2n/3)!$$

by Lemma 12 and the fact that $2(n/2)!^2 \leq (n/3)! (2n/3)!$ being $n \geq 30$.

If M is primitive, by [37] we have

$$|N_{S_n}(M)| < 4^n \leq 2(n/2)!^2 \leq (n/3)! (2n/3)!.$$

Since Π_j is closed under conjugation for all $j \in J$, we have

$$|H \cap \Pi_j| = |N_G(M^m) \cap \Pi_j|, \quad \forall j \in J.$$

We will use Stirling's inequalities, which are valid for all $k \geq 2$:

$$\sqrt{2\pi k} (k/e)^k \leq k! \leq e\sqrt{k} (k/e)^k.$$

Assume that either m is even or $r \neq 2$. By Lemma 9 and the fact that $\Pi_{0,r} \subseteq M_{0,r}$,

$$\begin{aligned} \frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} &= \frac{r \cdot \left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-r} \cdot \prod_{i=1}^r |D_i \cap N_{S_n}(M)|}{r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^r |D_i|} \\ &\leq \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^{m-r} \cdot \prod_{i=1}^r \frac{|N_{S_n}(M)|}{|D_i|} = \left(\frac{|N_{S_n}(M)|}{|S_n|}\right)^m \cdot 2(n-2)n^{r-1} \\ &\leq \left(\frac{(n/3)! (2n/3)!}{n!}\right)^m \cdot 2n^r \leq 2 \cdot \left(\frac{2^{2/3}}{3}\right)^{nm} \cdot \left(\frac{ne^2\sqrt{n}}{3\sqrt{\pi}}\right)^m. \end{aligned}$$

By Lemma 11,

$$\frac{|N_G(M^m) \cap \Pi_{0,2}|}{|\Pi_{0,2}|} \leq \frac{2n(n-2)}{|S_n : N_{S_n}(M)|^m},$$

so we have the above inequality also in the case $r = 2$ when m is odd.

According to the proof of [40, Lemmas 5.4, 5.5, 5.9, 5.10], the largest value of

$$\sum_{i \in I} \frac{|B_i \cap N_{S_n}(M)|}{|B_i \cap N_{S_n}(M_i)|}$$

is obtained by substituting $n = 30$ in the expression

$$\frac{3n^2 + 27n + 54}{4n^2 - 9},$$

so it is less than 0.9925. By Lemma 13,

$$\begin{aligned} \sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} &= \sum_{i \in I} \frac{\left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M)|}{\left(\frac{1}{2} |N_{S_n}(M_i)|\right)^{m-1} \cdot |B_i \cap N_{S_n}(M_i)|} \\ &\leq \sum_{i \in I} \frac{|B_i \cap N_{S_n}(M)|}{|B_i \cap N_{S_n}(M_i)|} < 0.9925 \end{aligned}$$

We obtain

$$\begin{aligned} c(H) &= \sum_{r \in P(2m)} \frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} + \sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} \\ &< 2m \cdot \left[\left(\frac{2^{2/3}}{3} \right)^n \cdot \frac{ne^2 \sqrt{n}}{3\sqrt{\pi}} \right]^m + 0.9925 \end{aligned}$$

This is less than 1 since $n \geq 30$.

We now turn our attention to the maximal subgroups of G of diagonal type and supplementing the socle N . Let H be such a subgroup. Recall that $H \cap N = \Delta_\varphi$ has order $|A_n|^{m/t}$ where t is a prime divisor of m .

We have

$$\begin{aligned} c(H) &= \sum_{r \in P(2m)} \frac{|H \cap \Pi_{0,r}|}{|M_{0,r} \cap \Pi_{0,r}|} + \sum_{i \in I} \frac{|H \cap \Pi_i|}{|N_G(M_i^m) \cap \Pi_i|} \\ &\leq |H| \cdot \left(\sum_{r \in P(2m)} \frac{1}{|\Pi_{0,r}|} + \sum_{i \in I} \frac{1}{|N_G(M_i^m) \cap \Pi_i|} \right). \end{aligned}$$

Since $HN = G$, we have

$$C_{2m} \cong \frac{G}{N} = \frac{HN}{N} \cong \frac{H}{H \cap N},$$

hence

$$|H| = |H : H \cap N| \cdot |H \cap N| = 2m \cdot |\Delta_\varphi| = 2m \cdot (n!/2)^{m/t}.$$

Assume first that either m is even or $r \neq 2$. Since $2 \leq r \leq m$,

$$\begin{aligned} |\Pi_{0,r}| &= r \cdot |A_n|^{m-r} \cdot \prod_{i=1}^r |D_i| = r \cdot \left(\frac{n!}{2} \right)^{m-r} \cdot \frac{n!}{n} \cdot \left(\frac{n!}{2(n-2)} \right)^{r-1} \\ &= \frac{r \cdot n!^m}{2^{m-1} n (n-2)^{r-1}} \geq \frac{2 \cdot n!^m}{2^{m-1} n^r} \geq \frac{n!^m}{2^{m-2} n^m}. \end{aligned}$$

By Lemma 11, the smallest value of $|\Pi_{0,2}|$ is when m is even, so the above inequality for $|\Pi_{0,r}|$ holds in all cases.

Fix $M_i \in \mathcal{E}_i$ for all $i \in I$. The smallest possible order of $N_{S_n}(M_i)$, $i \in I$, is when M_i is imprimitive with two blocks, so

$$|N_{S_n}(M_i)| \geq 2(n/2)!^2.$$

Since $B_i \cap N_{S_n}(M_i) \neq \emptyset$, by Lemma 10 we have

$$|N_G(M_i^m) \cap \Pi_i| = \left(\frac{1}{2} |N_{S_n}(M_i)|\right)^{m-1} |B_i \cap N_{S_n}(M_i)| \geq (n/2)!^{2(m-1)}.$$

We deduce that

$$\begin{aligned} c(H) &\leq 2m \left(\frac{n!}{2}\right)^{m/t} \cdot \left(\sum_{r \in P(2m)} \frac{2^{m-2} n^m}{(n!)^m} + \sum_{i \in I} \frac{1}{(n/2)!^{2(m-1)}} \right) \\ &\leq 2m \left(\frac{1}{2}(n/e)^n e\sqrt{n}\right)^{m/t} \cdot \left(2^{m-1} \frac{mn^m}{(n/e)^{nm}} + \frac{n}{(n/(2e))^{n(m-1)}} \right) < 1 \end{aligned}$$

for $m \geq 3$ and $n \geq 30$, where we used the fact that $t \geq 2$ and $t = 3$ if $m = 3$.

Now assume that $m = 2$. We will show that $c(H) = 0$ by proving that $H \cap \Pi_{0,2}$ and $H \cap \Pi_i$ are empty for all $i \in I$. We have $H = N_G(\Delta_\varphi)$ where

$$\Delta_\varphi = \{(\alpha, \alpha^\varphi) : \alpha \in A_n\},$$

for $\varphi \in \text{Aut}(A_n) \cong S_n$, and

$$\Pi_{0,2} = \{(x_1, x_2)\gamma^2 : x_1\tau \in D_1, x_2\tau \in D_2\} \cup \{(x_1, x_2)\gamma^2 : x_1\tau \in D_2, x_2\tau \in D_1\},$$

$$\Pi_i = \{(x_1, x_2)\gamma : x_1x_2\tau \in B_i\}, \quad i \in I.$$

For $i \in I$ we have that if $(x_1, x_2)\gamma \in H \cap \Pi_i$ then

$$(\alpha, \alpha^\varphi)^{(x_1, x_2)\gamma} = (\alpha, \alpha^\varphi)^{(x_1, x_2)(1, \tau)\delta} = (\alpha^{x_1}, \alpha^{\varphi x_2\tau})^\delta = (\alpha^{\varphi x_2\tau}, \alpha^{x_1}) \in \Delta_\varphi.$$

So $\varphi x_2\tau\varphi = x_1$, equivalently $(\varphi x_2\tau)^2 = x_1x_2\tau$ which is false since $(\varphi x_2\tau)^2 \in A_n$ and $x_1x_2\tau \notin A_n$. Therefore $H \cap \Pi_i = \emptyset$ for all $i \in I$.

If $(x_1, x_2)\gamma^2 \in H \cap \Pi_{0,2}$ then, for all $\alpha \in A_n$,

$$(\alpha, \alpha^\varphi)^{(x_1, x_2)\gamma^2} = (\alpha, \alpha^\varphi)^{(x_1, x_2)(\tau, \tau)} = (\alpha^{x_1\tau}, \alpha^{\varphi x_2\tau}) \in \Delta_\varphi.$$

So $x_1\tau\varphi = \varphi x_2\tau$, i.e. $\varphi^{-1}x_1\tau\varphi = x_2\tau$. This is a contradiction because $x_1\tau$ and $x_2\tau$ are not conjugated in S_n by definition of $\Pi_{0,2}$. Therefore $H \cap \Pi_{0,2} = \emptyset$. \square

Chapter 3

Pairwise generation

3.1 The function $\omega(G)$

Definition 7. Let G be a finite group which can be generated by 2 elements. The generating graph of G is the simple graph whose vertices are the elements of G and two vertices are connected by an edge if together they generate G . That is, for $x, y \in G$, $x \neq y$, $\{x, y\}$ is an edge if and only if $\langle x, y \rangle = G$.

As an example, we present the generating graph of the Symmetric group S_3 and the Quaternions group Q_8



Definition 8. A complete graph is a simple graph in which each pair of graph vertices is connected by an edge. A clique of a simple graph is a complete subgraph and its clique number is the maximal size of a clique. We denote by $\omega(G)$ the clique number of the generating graph of G . In

other words, $\omega(G)$ is the maximal size of a subset S of G with the property that $\langle x, y \rangle = G$ whenever $x, y \in S$ and $x \neq y$.

Note that $\omega(G) \geq 3$ if $|G| \geq 3$. Indeed, if x, y are two distinct elements of G different from 1 and such that $\langle x, y \rangle = G$ then $\{x, y, xy\}$ is a clique of size 3. There are groups that realize this lower bound, for example $\omega(C_2 \times C_2) = 3$.

From the generating graph of the groups S_3 and Q_8 we see that $\omega(S_3) = 4$ and $\omega(Q_8) = 3$.

Let φ be Euler's totient function and let $\pi(n)$ be the number of distinct prime divisors of n .

Proposition 21. $\omega(C_n) = \varphi(n) + \pi(n)$.

Proof. Let $G := C_n$ and let $Y := \{g \in G : \langle g \rangle = G\}$. Note that G has t maximal subgroups, where $t = \pi(n)$, call them $M_i = \langle x_i \rangle$ for $i = 1, \dots, t$. Clearly, $Y \cup \{x_1, \dots, x_t\}$ is a clique, so $\omega(G) \geq \varphi(n) + \pi(n)$. Now assume X is a clique of G . Then of course $|X \cap M_i| \leq 1$ for all $i = 1, \dots, t$ hence there exist $y_i \in M_i$ with $\langle y_i \rangle = M_i$ for $i = 1, \dots, t$ such that

$$X \subseteq \left(G - \bigcup_{i=1}^t M_i \right) \cup \{y_1, \dots, y_t\}.$$

Note that the elements of G that do not belong to the union $\bigcup_{i=1}^t M_i$ are precisely the generators of G , i.e. the elements $g \in G$ such that $G = \langle g \rangle$. Therefore $\omega(G) \leq \varphi(n) + t$. \square

Let $d(G)$ the minimal size of a subset S of G which generates G , i.e. $\langle S \rangle = G$. The group G is called d -generated if $d(G) \leq d$.

Proposition 22. *If G is a finite 2-generated group and $N \trianglelefteq G$ then either G/N is cyclic or $\omega(G) \leq \omega(G/N)$.*

Proof. If X is a clique of G of size $\omega(G)$ then $\{xN : x \in X\}$ is a clique of G/N , for obvious reasons. This implies that $\omega(G) = |X| \leq \omega(G/N)$ unless there exist $x, y \in X$ distinct such that $xN = yN$. In this case, $y^{-1}x = n \in N$ hence $G = \langle x, y \rangle = \langle x, n \rangle \leq N\langle x \rangle$ hence G/N is cyclic. \square

3.2 $\omega(S \times S)$

Let S be a nonabelian simple group. We want to study $\omega(S \times S)$. By Proposition 22, we know that $\omega(S \times S) \leq \omega(S)$. It is natural to ask whether $\omega(S \times S) = \omega(S)$. In this section we prove that

Theorem 10. $\omega(A_n \times A_n) = \omega(A_n)$ for $n \in \{5, 6, 7, 10\}$ and for all $n \geq 22$ such that $n \equiv 2 \pmod{4}$.

Let $m = \omega(S)$ and $\{x_1, \dots, x_m\}$ be a clique of S . We want to find a permutation $\sigma \in \text{Sym}(m)$ such that

$$T_\sigma = \{(x_i, x_{\sigma(i)}) : i = 1, \dots, m\}$$

is a clique of $S \times S$. It is easy to show that the maximal subgroups of $S \times S$ are of one of the following three types: $M \times S$ or $S \times M$, where M is a maximal subgroup of S , or $\{(x, x^\varphi) : x \in S\}$ where $\varphi \in \text{Aut}(S)$. Therefore T_σ is a clique if and only if the following condition is satisfied: whenever $i \in \{1, \dots, m\}$, if there exists $\varphi \in \text{Aut}(S)$ such that $x_i^\varphi = x_{\sigma(i)}$ then $x_j^\varphi \neq x_{\sigma(j)}$ for every $j \neq i$. This is equivalent to saying that, whenever $i \neq j$, the element (x_i, x_j) is not in the same $\text{Aut}(S)$ -orbit as $(x_{\sigma(i)}, x_{\sigma(j)})$. Here $\text{Aut}(S)$ acts on $S \times S$ by the rule $(a, b)^\varphi = (a^\varphi, b^\varphi)$.

In the following, with GAP [16] and Gurobi [22] we compute sets C of elements of A_n for $n \in \{5, 6, 7\}$ that are cliques for these groups (see Appendix A.1), and try to construct sets T_σ that are cliques for $A_n \times A_n$. For $m = \omega(S)$, we write the elements x_1, \dots, x_m of the clique $C = \{x_1, \dots, x_m\}$ in the order in which they appear.

In the case of $S = A_5$, we have $\omega(S) = 8$ and we choose

$$C = \{(145), (235), (12354), (15342), (12453), (15423), (14235), (12345)\},$$

$$\sigma = (12435)(678).$$

In this case, we can check with GAP that T_σ is a clique of $A_5 \times A_5$.

In the case of $S = A_6$ we have $\omega(S) = 11$ and we choose

$$C = \{(14)(2653), (12)(3456), (1425)(36), (1546)(23), (1352)(46),$$

$$(14653), (12536), (24635), (13452), (12346), (12456)\},$$

$$\sigma = (1, 6)(2, 7)(3, 8)(4, 9)(5, 10)(11).$$

In this case T_σ is a clique of $A_6 \times A_6$ because x_i and $x_{\sigma(i)}$ have distinct orders unless $i = 11$.

In the case of $S = A_7$ we have $\omega(S) = 27$ and we choose

$$\begin{aligned} C = \{ & (13642), (23745), (14657), (17)(26)(345), (12)(357)(46), \\ & (15)(264)(37), (176)(24)(35), (152)(34)(67), (143)(27)(56), (13)(256)(47), \\ & (127)(36)(45), (14)(25)(376), (1345276), (1634752), (1634257), (1632475), \\ & (1234567), (1275364), (1536427), (1762534), (1723645), (1276534), \\ & (1746253), (1643572), (1263745), (1653274), (1276534), (1742365)\}. \end{aligned}$$

Let σ be the permutation of order 2 defined by $\sigma(i) := i + 12$ for $1 \leq i \leq 12$ and $\sigma(25) = 25$, $\sigma(26) = 27$, $\sigma(27) = 26$. The reason T_σ is a clique of $A_7 \times A_7$ is that x_i and $x_{\sigma(i)}$ have different orders if $i \leq 24$ and, for all $i \in \{1, \dots, 7\}$, setting $a = x_{25}$, $b = x_{26}$, $c = x_{27}$, we have

$$b^{a^i} \neq c, \quad c^{a^i} \neq b, \quad c^{b^i \tau} \neq b.$$

Here τ is any element of S_7 such that $c = b^\tau$. Since $C_{S_7}(x) = \langle x \rangle$ for all $x \in \{a, b, c\}$, this means that, for all $\phi \in \text{Aut}(A_7)$ such that $\phi(a) = a$ we have $\phi(b) \neq c$ and $\phi(c) \neq b$, moreover for all $\psi \in \text{Aut}(A_7)$ such that $\psi(b) = c$ we have $\psi(c) \neq b$.

In the case $S = A_{10}$, we have (see [34])

$$\sigma(A_{10}) = 2^{10-2} = \binom{10}{1} + \binom{10}{3} + \frac{1}{2} \binom{10}{5} = 256.$$

In an unpublished paper, E. Swartz proved that $\sigma(A_{10}) = \omega(A_{10})$. Since $\sigma(A_{10}) = \omega(A_{10})$, there exists a clique $C = \{x_1, \dots, x_{256}\}$ of A_{10} such that $x_i \in H_i - \bigcup_{j \neq i} H_j$, $\forall i \in \{1, \dots, 256\}$, where $\mathcal{H} = \{H_1, \dots, H_{256}\}$ is the minimal covering of A_{10} consisting of the maximal intransitive subgroups $(S_k \times S_{10-k}) \cap A_{10}$ with $k \in \{1, 3\}$ and the maximal imprimitive subgroups $(S_5 \wr S_2) \cap A_{10}$.

In the clique C there are $\frac{1}{2} \binom{10}{5} = 126$ elements of cycle structure $(5, 5)$,

$\binom{10}{3} = 120$ elements of cycle structure $(7, 3)$ and $\binom{10}{1} = 10$ elements of cycle structure $(9, 1)$. We order the elements of C in the following way:

$$\begin{aligned} \text{for } 1 \leq i \leq 126, \quad & x_i \text{ has cycle structure } (5, 5), \\ \text{for } 127 \leq i \leq 246, \quad & x_i \text{ has cycle structure } (7, 3), \\ \text{for } 247 \leq i \leq 256, \quad & x_i \text{ has cycle structure } (9, 1). \end{aligned}$$

Let σ be the permutation defined by $\sigma(i) := i + 126$ for $1 \leq i \leq 130$ and $\sigma(i) := i - 130$ for $131 \leq i \leq 256$.

x_i	(5, 5)	...	(5, 5)	(7, 3)	...	(7, 3)	(7, 3)	...	(7, 3)	(9, 1)	...	(9, 1)
i	1	...	126	127	...	130	131	...	246	247	...	256
$\sigma(i)$	127	...	252	253	...	256	1	...	116	117	...	126

The reason why T_σ is a clique of $A_{10} \times A_{10}$ is because x_i and $x_{\sigma(i)}$ have different cycle structures, so they are not conjugate in $\text{Aut}(A_{10}) \cong S_{10}$, for $i = 1, \dots, 256$.

We can repeat the above argument in the case $n \equiv 2 \pmod{4}$, $n \geq 22$. In this case, we have (see [34] and [39])

$$\omega(A_n) = \sigma(A_n) = 2^{n-2} = \binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{n/2-2} + \frac{1}{2} \binom{n}{n/2}.$$

Lemma 14. *Let m_1, \dots, m_t be positive integers, $m = m_1 + \dots + m_t$, and assume that $\max\{m_1, \dots, m_t\} \leq m/2$. Let A_j , $j = 1, \dots, t$, be pairwise disjoint subsets of $\Omega = \{1, \dots, m\}$ such that $|A_j| = m_j$ for $j = 1, \dots, t$. Then there exists a permutation σ of Ω such that $\sigma(x) \notin A_j$ for all $x \in A_j$, for all $j = 1, \dots, t$.*

Proof. Order the elements of Ω so that $A_1 = \{1, \dots, m_1\}$, $A_2 = \{m_1 + 1, \dots, m_1 + m_2\}$ and so on. We can also assume that $\max\{m_1, \dots, m_t\} = m_1$. Define $\sigma : \Omega \rightarrow \Omega$ by setting $\sigma(i) := i + m_1$ for all $i = 1, \dots, m - m_1$ and $\sigma(i) := i - m + m_1$ for all $i = m - m_1 + 1, \dots, m$. Since $m_1 \leq m/2$, we have $m - m_1 \geq m_1$, so this permutation σ satisfies the requirement. \square

Let $m = 2^{n-2}$. Order the clique C so that the first $\ell = \frac{1}{2} \binom{n}{n/2}$ elements have cycle structure $(n/2, n/2)$ and the others follow grouped together

according to their cycle structures. Since the maximum of $\frac{1}{2}\binom{n}{n/2}$ and $\binom{n}{j}$, j odd, $1 \leq j \leq n/2 - 2$ is at most $m/2$, we know that there exists a permutation σ of $\{1, \dots, m\}$ as in Lemma 14, where of course the indices i are partitioned according to the cycle structures of the x_i 's. Then T_σ is a clique because x_i and $x_{\sigma(i)}$ have distinct cycle structures, so they are not conjugate in $\text{Aut}(A_n) \cong S_n$.

3.3 $\omega(G_S)$

Let S be a nonabelian simple group. Then S is 2-generated. This was proved by Steinberg [38] for Chevalley groups, and by Aschbacher and Guralnick [4, Theorem B] for the other simple groups, using the classification of the finite simple groups. It is also possible to show that the direct powers S^m are not all 2-generated [10]. Therefore there exists a maximal n such that S^n is 2-generated, call it $\delta(S)$. Set $G_S = S^{\delta(S)}$. Proposition 22 implies that $\omega(G_S) \leq \omega(S^k)$ for all k with $1 \leq k \leq \delta(S)$.

$\delta(S)$ can be computed as follows. Consider the set U consisting of pairs (x, y) of elements of S such that $\langle x, y \rangle = S$. The group $\text{Aut}(S)$ acts naturally on U by $(x, y)^a := (x^a, y^a)$. This action is semiregular, in other words its stabilizers are trivial. Indeed if a fixes (x, y) then $x^a = x$ and $y^a = y$ so, being $\langle x, y \rangle = S$, a must be the identity. In other words, the $\text{Aut}(S)$ -orbits of U have size $|\text{Aut}(S)|$. It is possible to prove that

$$\delta(S) = \frac{|\{(x, y) \in S \times S : \langle x, y \rangle = S\}|}{|\text{Aut}(S)|} \quad (\text{see [10]})$$

equals the number of $\text{Aut}(S)$ -orbits of U .

For example, if $S = A_5$, then $\delta(S) = 19$ and $\omega(G_S) \leq \omega(S) = 8$.

In [35] A. Lucchini and G. Niero wrote numerous programs in GAP language to show how the clique number of A_5^n decrease as n increase. The result obtained is shown in the following Table:

n	$\omega(A_5^n)$
1, 2, 3, 4	8
5, 6	7 or 8
7, 8	7
9, 10, 11, 12, 13	6 or 7
14	5, 6 or 7
15	5 or 6
16	5
17	4 or 5
18, 19	4

Table 3.1: The clique number of A_5^n .

This implies that $\omega(G_{A_5}) = 4$.

The problem of understanding $\omega(G_S)$ is quite open at the moment. We could even ask whether it is true that $\omega(G_S)$ is bounded above by a constant for every nonabelian simple group S . In [30, Theorem 1.2] it is proved that, denoting with $m(S)$ the minimal index of a proper subgroup of S , we have $\omega(G_S) \leq C \cdot m(S)$ for all nonabelian simple group S , where C is an absolute constant. In particular $\omega(G_{A_n}) \leq C \cdot n$.

3.4 The Lovász Local Lemma

For the calculation of $\omega(G_{n,m})$, we follow the same strategy used in [15]. We use the following very important result that was proved by Lovász and Erdős in [13]. The formulation we use is taken from [3, Corollary 5.1.2] (the “symmetric case”). Given an event E of a probability space, we denote by $P(E)$ its probability and by \overline{E} its complement. As usual e denotes the base of the natural logarithm.

Theorem 11 (Lovász Local Lemma). *Let E_1, E_2, \dots, E_n be events in an arbitrary probability space. Let (V, E) be a directed graph, where $V = \{1, \dots, n\}$ is the set of vertices, and assume that, for every $i \in V$, the event E_i is mutually independent of the set of events E_j such that $(i, j) \notin E$, meaning that*

$$P\left(E_i \mid \bigcap_{j \in S} \overline{E_j}\right) = P(E_i),$$

for all nonempty subset S of $\{j \in V : (i, j) \notin E\}$. Let d be the maximum valency of a vertex of the graph (V, E) . If for every $i \in V$

$$P(E_i) \leq \frac{1}{e(d+1)}$$

then $P\left(\bigcap_{i \in V} \overline{E}_i\right) > 0$.

First we prove the General Case. Recall that, if A, B are two events, then $P(A | B) = P(A \cap B)/P(B)$ if $P(B) > 0$ and $P(A | B) = 0$ if $P(B) = 0$. In the following proof we will use the following equalities, which are easy to prove. If A, B, C are events, then

$$\begin{aligned} P(A | B \cap C) &= \frac{P(A \cap B | C)}{P(B | C)}, \\ P(\overline{A} \cap \overline{B} | C) &= (1 - P(A | C)) \cdot (1 - P(B | \overline{A} \cap C)), \\ P(\overline{A} \cap \overline{B}) &= (1 - P(A)) \cdot (1 - P(B | \overline{A})). \end{aligned}$$

Note that the third equality is a particular case of the second one.

Theorem 12 (The Local Lemma; General Case). *Let E_1, E_2, \dots, E_n be events in an arbitrary probability space. A directed graph $D = (V, E)$ on the set of vertices $V = \{1, 2, \dots, n\}$ is called a dependency digraph for the events E_1, \dots, E_n if for each i , $1 \leq i \leq n$, the event E_i is mutually independent of all the events $\{E_j : (i, j) \notin E\}$. Suppose that $D = (V, E)$ is a dependency digraph for the above events and suppose there are real numbers x_1, \dots, x_n such that $0 \leq x_i < 1$ and*

$$P(E_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j),$$

for all $1 \leq i \leq n$. Then

$$P\left(\bigcap_{i=1}^n \overline{E}_i\right) \geq \prod_{i=1}^n (1 - x_i).$$

In particular, with positive probability, no event E_i holds.

Proof. We first prove, by induction on s , that for any $S \subseteq \{1, \dots, n\}$, $|S| = s < n$, and any $i \notin S$,

$$P\left(E_i \mid \bigcap_{j \in S} \overline{E}_j\right) \leq x_i. \quad (3.1)$$

This is certainly true for $s = 0$. Assuming it holds for all $s' < s$, we prove it for s . Put $S_1 = \{j \in S : (i, j) \in E\}$, $S_2 = S \setminus S_1$. Then

$$P\left(E_i \mid \bigcap_{j \in S} \overline{E_j}\right) = \frac{P\left(E_i \cap \left(\bigcap_{j \in S_1} \overline{E_j}\right) \mid \bigcap_{l \in S_2} \overline{E_l}\right)}{P\left(\bigcap_{j \in S_1} \overline{E_j} \mid \bigcap_{l \in S_2} \overline{E_l}\right)}. \quad (3.2)$$

To bound the numerator, observe that, since E_i is mutually independent of the events $\{E_l : l \in S_2\}$,

$$P\left(E_i \cap \left(\bigcap_{j \in S_1} \overline{E_j}\right) \mid \bigcap_{l \in S_2} \overline{E_l}\right) \leq P\left(E_i \mid \bigcap_{l \in S_2} \overline{E_l}\right) = P(E_i) \leq x_i \prod_{(i,j) \in E} (1 - x_j). \quad (3.3)$$

The denominator, on the other hand, can be bounded by the induction hypothesis. Indeed, suppose $S_1 = \{j_1, j_2, \dots, j_r\}$. If $r = 0$, then the denominator is 1, and 3.1 follows. Otherwise

$$\begin{aligned} & P\left(\overline{E_{j_1}} \cap \overline{E_{j_2}} \cap \dots \cap \overline{E_{j_r}} \mid \bigcap_{l \in S_2} \overline{E_l}\right) \\ &= \left(1 - P\left(E_{j_1} \mid \bigcap_{l \in S_2} \overline{E_l}\right)\right) \cdot \left(1 - P\left(E_{j_2} \mid \overline{E_{j_1}} \cap \bigcap_{l \in S_2} \overline{E_l}\right)\right) \cdot \dots \\ & \dots \cdot \left(1 - P\left(E_{j_r} \mid \overline{E_{j_1}} \cap \dots \cap \overline{E_{j_{r-1}}} \cap \bigcap_{l \in S_2} \overline{E_l}\right)\right) \\ & \geq (1 - x_{j_1})(1 - x_{j_2}) \dots (1 - x_{j_r}) = \prod_{(i,j) \in E} (1 - x_j). \end{aligned} \quad (3.4)$$

Substituting 3.3 and 3.4 into 3.2, we conclude that

$$P\left(E_i \mid \bigcap_{j \in S} \overline{E_j}\right) \leq x_i,$$

completing the proof of the induction.

The assertion of the Theorem now follows easily, as

$$\begin{aligned} P\left(\bigcap_{i=1}^n \overline{E_i}\right) &= (1 - P(E_1)) \cdot (1 - P(E_2 \mid \overline{E_1})) \cdot \dots \\ & \dots \cdot \left(1 - P\left(E_n \mid \bigcap_{i=1}^{n-1} \overline{E_i}\right)\right) \geq \prod_{i=1}^n (1 - x_i), \end{aligned}$$

completing the proof. \square

Now we prove Theorem 11.

Proof. If $d = 0$, the events E_i are all independent from each other hence

$$P\left(\bigcap_{i \in V} \overline{E}_i\right) = \prod_{i \in V} (1 - P(E_i)) \geq \prod_{i \in V} (1 - 1/e) > 0.$$

Otherwise, by the assumption there is a dependency digraph graph (V, E) for the events E_1, \dots, E_n in which, for each i , $|\{j : (i, j) \in E\}| \leq d$. The result now follows from Theorem 12 by taking $x_i = 1/(d+1) < 1$ for all i and using the fact that, for any $d \geq 1$, $(1 - 1/(d+1))^d > 1/e$. \square

3.5 Proof of Theorem 2

Let $G = G_{n,m}$ be the group defined in Section 2.3.1, that is, $G = A_n^m \rtimes \langle \gamma \rangle$, where $\gamma = (1, \dots, 1, \tau)\delta$, $\tau = (1\ 2)$ and $\delta = (1 \dots m)$. Our objective in this section is to prove our second Theorem:

Theorem. [2, Theorem 2] *Set $G := G_{n,m}$. For fixed $m \geq 2$, $\omega(G)$ is asymptotically equal to $\left(\frac{1}{2} \binom{n}{n/2}\right)^m$ for $n \rightarrow \infty$, n even, and $\omega(G)/\sigma(G)$ tends to 1 as $n \rightarrow \infty$, n even.*

Define

$$\mathcal{N} = \{N_G(M \times M^{a_2} \times \dots \times M^{a_m}) : M \in \mathcal{F}\},$$

where \mathcal{F} is the family of maximal imprimitive subgroups of A_n with 2 blocks, $(S_{n/2} \wr S_2) \cap A_n$, and $a_2, \dots, a_m \in A_n$.

Note that if $H \in \mathcal{N}$ then H is conjugate to $N_G(M^m)$ in G , for some $M \in \mathcal{F}$. The subgroups of G contained in \mathcal{N} are maximal in G by [5, Proposition 1.1.44] and [27].

Let B be the set of n -cycles in S_n and let Π be the set of elements of G of the form $(x_1, \dots, x_m)\gamma$ with the property that $x_1 \dots x_m \tau \in B$. Note that these sets are precisely what are called B_{-1} and Π_{-1} in Section 2.3. By Proposition 15, Π is a conjugacy class of G .

For $H \in \mathcal{N}$ and $K \leq G$, define

$$C(H) = \Pi \cap H, \quad f_H(K) = \frac{|C(H) \cap K|}{|C(H)|}.$$

Let $g \in G$ be such that $H = (N_G(M^m))^g$. By Lemma 10 and Proposition 15,

$$\begin{aligned} |C(H)| &= |H \cap \Pi| = |(N_G(M^m))^g \cap \Pi| = |N_G(M^m) \cap \Pi| \\ &= \left(\frac{1}{2} |N_{S_n}(M)|\right)^{m-1} \cdot |B \cap N_{S_n}(M)| = 2/n \cdot (n/2)!^{2m}. \end{aligned}$$

Since H is a non-normal maximal subgroup of G , it is self-normalizing.

Since \mathcal{N} is the conjugacy class of H in G ,

$$l = |\mathcal{N}| = |G : H| = \frac{(n!/2)^m \cdot 2m}{(n/2)!^{2m} \cdot 2m} = \frac{1}{2^m} \binom{n}{n/2}^m < 2^{m(n-1)}.$$

Define the graph Γ whose vertices are the two-element subsets $v = \{H_1, H_2\}$ of \mathcal{N} , with $H_1 \neq H_2$. There is an edge between two vertices v and w if $v \cap w \neq \emptyset$. Every vertex of Γ has valency

$$d = 2(l - 2) < 2^{m(n-1)+1}.$$

Choose $g_H \in C(H)$ uniformly and independently, for all $H \in \mathcal{N}$, and let E_v be the event $\langle g_{H_1}, g_{H_2} \rangle \neq G$, equivalently $\langle g_{H_1}, g_{H_2} \rangle$ is contained in a maximal subgroup of G . It is easy to see that the mutual independence condition is satisfied (see also [15, Section 3]).

Our aim is to prove that $P(E_v) \leq 1/(e(d+1))$ for every vertex v of Γ . If this is true, then the Local Lemma implies that there exists a choice of g_H in each $C(H)$, $H \in \mathcal{N}$, with the property that $\langle g_{H_1}, g_{H_2} \rangle = G$ for all $H_1 \neq H_2$ in \mathcal{N} , therefore these elements form a clique of the generating graph of G , in other words $\omega(G) \geq |\mathcal{N}|$. This, together with item (3) of Theorem 9, gives the claim of Theorem 2.

In the following discussion we will talk about the various types of maximal subgroups of G , which we described in Section 2.3.

Let \mathcal{M}_1 be the family of maximal intransitive subgroups of S_n , \mathcal{M}_2 the family of primitive maximal subgroups of S_n different from A_n , \mathcal{M}_j the

family of maximal imprimitive subgroups of S_n with j blocks for $j \in \{3, 4\}$, \mathcal{M}_5 the family of maximal imprimitive subgroups of S_n with at least 5 blocks.

Let \mathcal{H} be the family of all maximal subgroups of G not in \mathcal{N} and $J = \{1, 2, 3, 4, 5, 6\}$. We write \mathcal{H} as the union $\mathcal{H}_1 \cup \dots \cup \mathcal{H}_6$ where the \mathcal{H}_j 's are defined as follows. For j with $1 \leq j \leq 5$, \mathcal{H}_j is the subset of \mathcal{H} consisting of subgroups of the form $N_G(M \times M^{a_2} \times \dots \times M^{a_m})$, where $a_2, \dots, a_m \in A_n$, $N_{S_n}(M) \in \mathcal{M}_j$ and $N_{S_n}(M) \cap A_n = M$. \mathcal{H}_6 is the family of maximal subgroups of G of diagonal type.

Fix a vertex $v = \{H_1, H_2\}$ of Γ . For $j \in J$, let $E_{v,j}$ be the probability that $\langle g_{H_1}, g_{H_2} \rangle$ is contained in a member of \mathcal{H}_j . We clearly have

$$P(E_v) \leq \sum_{j \in J} P(E_{v,j}).$$

Let $[H]$ be the conjugacy class in G of a subgroup H of G and $m_{H_i}([H])$ the number of different conjugates of H that contain a fixed element of $C(H_i)$, $i = 1, 2$. This is well defined since Π is a conjugacy class of G .

In the following sum, $[H]$ varies over the set of conjugacy classes of elements of \mathcal{H}_j . Arguing as in [15] we have, for $j \in J$,

$$P(E_{v,j}) \leq \sum_{[H]} m_{H_1}([H]) \max_{K \in [H]} (f_{H_2}(K)).$$

Let $c_{v,j}$ the number of conjugacy classes of subgroups in \mathcal{H}_j such that there exists H in such a class such that $H \cap C(H_1) \neq \emptyset$ and $H \cap C(H_2) \neq \emptyset$. We deduce that

$$P(E_{v,j}) \leq c_{v,j} \cdot \min_{\{i_1, i_2\}=\{1,2\}} \left(\max_{H \in \mathcal{H}_j, K \in [H]} (m_{H_{i_1}}([H]) \cdot f_{H_{i_2}}(K)) \right). \quad (\star)$$

Let $s_{v,j}$ be the number of subgroups H in \mathcal{H}_j such that $H \cap C(H_1) \neq \emptyset$ and $H \cap C(H_2) \neq \emptyset$. Then

$$P(E_{v,j}) \leq \sum_{H \in \mathcal{H}_j} f_{H_1}(H) f_{H_2}(H) \leq s_{v,j} \cdot \max_{H \in \mathcal{H}_j} (f_{H_1}(H) \cdot f_{H_2}(H)). \quad (\star\star)$$

Lemma 15. *Let $v = \{H_1, H_2\}$ be a vertex of Γ . Then $c_{v,2} \leq n$ for large enough n , $c_{v,j} \leq 1$ for $j \in \{3, 4\}$, $c_{v,5} \leq 2\sqrt{n}$ and $c_{v,6} \leq m \cdot 2^m$.*

The bound $c_{v,2} \leq n$ depends on the classification of finite simple groups.

Proof. Note that $c_{v,j}$ is less than or equal to the number of conjugacy classes of subgroups in \mathcal{H}_j . Also, if $H \in \mathcal{H}$ then we can write $H = N_G(H \cap N)$ and this allows to reduce to counting G -conjugacy classes of subgroups of the form $H \cap N$ in N . Also note that if M and L are conjugate in A_n , then $N_G(M^m)$ and $N_G(L^m)$ are conjugate in G by an element of the form $(c, c, \dots, c) \in A_n^m$ such that $M^c = L$. Therefore, for j with $1 \leq j \leq 5$, the number of conjugacy classes of subgroups in \mathcal{H}_j is less than or equal to the number of conjugacy classes of subgroups of S_n belonging to \mathcal{M}_j . Therefore, for $j \neq 6$, we can use the bounds for $c_{v,j}$ calculated in [15, Lemma 5]. In other words $c_{v,2} \leq n$ for large enough n , $c_{v,j} \leq 1$ for $j \in \{3, 4\}$ and $c_{v,5} \leq 2\sqrt{n}$.

It remains to bound $c_{v,6}$. We will use the fact that if $X \leq Y$ are finite groups with Y acting on a finite set Ω , then denoting by u_X the number of X -orbits and by u_Y the number of Y -orbits of this action, we have $u_Y \leq u_X \leq |Y : X| \cdot u_Y$. Since n is larger than 6, $\text{Aut}(A_n) \cong S_n$, therefore any two isomorphic diagonal subgroups $\Delta_{\varphi_1}, \Delta_{\varphi_2}$ of the socle $N = A_n^m$ are conjugate in the group $S_n^m \rtimes \langle \delta \rangle$, which contains G , via an element of S_n^m . It follows that the number of G -classes of isomorphic diagonal subgroups is at most the number of A_n^m -classes, which is at most $|S_n : A_n|^m = 2^m$. We know that the number of isomorphism classes of diagonal subgroups equals the number of prime divisors of m (see Section 2.3). Therefore $c_{v,6} \leq m \cdot 2^m$. \square

Lemma 16. *Let v be a vertex of Γ and assume that 4 divides n . Then $s_{v,4} \leq 1$.*

Proof. Let $v = \{H_1, H_2\}$ and let $H \in \mathcal{H}_4$. Write

$$H = N_G(R^{b_1} \times \dots \times R^{b_m}) \in \mathcal{H}_4, \quad H_i = N_G(M_i^{a_{i1}} \times \dots \times M_i^{a_{im}}) \in \mathcal{N},$$

for $i = 1, 2$, where each a_{ij} and each b_j belongs to A_n , $N_{S_n}(M_i)$ is a maximal imprimitive subgroup of S_n with 2 blocks for $i = 1, 2$ and $N_{S_n}(R)$ is a maximal imprimitive subgroup of S_n with 4 blocks. Suppose that $H \cap C(H_i) = H \cap \Pi \cap H_i \neq \emptyset$ for $i = 1, 2$. We need to show that H is

uniquely determined by these conditions, in other words, that each R^{b_j} is uniquely determined. By [15, Proof of Lemma 5], it is enough to prove that $B \cap N_{S_n}(M_i^{a_{ij}}) \cap N_{S_n}(R^{b_j}) \neq \emptyset$ for $i = 1, 2$ and for $j = 1, \dots, m$.

Fix $i \in \{1, 2\}$ and let

$$h = (x_1, \dots, x_m)\gamma \in H \cap C(H_i) = H \cap H_i \cap \Pi.$$

Since $h \in \Pi$, by definition $x_1 \dots x_m \tau \in B$. On the other hand, being $h \in H$, $R^{b_1} \times \dots \times R^{b_m}$ equals

$$(R^{b_1} \times \dots \times R^{b_m})^{(x_1, \dots, x_m)\gamma} = R^{b_m x_m \tau} \times R^{b_1 x_1} \times R^{b_2 x_2} \times \dots \times R^{b_{m-1} x_{m-1}}.$$

We deduce that $b_m x_m \tau b_1^{-1} \in N_{S_n}(R)$ and $b_j x_j b_{j+1}^{-1} \in N_{S_n}(R)$ for $j = 1, \dots, m-1$. Fix $j \in \{1, \dots, m\}$. Multiplying everything starting from the j -th term, we have

$$b_j x_j x_{j+1} \dots x_m \tau x_1 x_2 \dots x_{j-1} b_j^{-1} \in N_{S_n}(R).$$

It follows that the element $x := x_j x_{j+1} \dots x_m \tau x_1 x_2 \dots x_{j-1}$ belongs to $N_{S_n}(R^{b_j})$. Since $h \in H_i$, the same argument shows that x belongs to $N_{S_n}(M_i^{a_{ij}})$. Furthermore

$$x = (x_j x_{j+1} \dots x_m \tau) \cdot x_1 \dots x_m \tau \cdot (x_j x_{j+1} \dots x_m \tau)^{-1},$$

so x belongs to B . Therefore $x \in B \cap N_{S_n}(M_i^{a_{ij}}) \cap N_{S_n}(R^{b_j})$. \square

Lemma 17. *Let $L \leq G$ and $g \in \Pi$, then the number of conjugates of L containing g is at most nm .*

Proof. We argue as in the proof of [6, Lemma 4]. Let $a(L)$ the number of conjugates of L containing g . Note that $a(L)$ does not depend on g because Π is a conjugacy class in G . Consider the set R of pairs (h, H) such that $h \in H \cap \Pi$ and H is conjugated to L in G . On the one hand, since Π is a conjugacy class of G , $|R| = |\Pi| \cdot a(L)$. On the other hand, since L has $|G : N_G(L)|$ conjugates in G and $|L^g \cap \Pi| = |L \cap \Pi|$ for all $g \in G$,

$$|R| = |G : N_G(L)| \cdot |L \cap \Pi| \leq |G : L| \cdot |L| = |G|.$$

Therefore $|\Pi| \cdot a(L) \leq |G|$ hence

$$a(L) \leq \frac{|G|}{|\Pi|} = \frac{2m \cdot (n!/2)^m}{(n-1)! \cdot (n!/2)^{m-1}} = nm.$$

This concludes the proof. \square

Fix a vertex $v = \{H_1, H_2\}$ of Γ and let $i \in \{1, 2\}$, $H := H_i$. By Lemma 17,

$$m_H([K]) \leq nm, \quad \forall K \leq G.$$

We now bound $f_H(K) = |C(H) \cap K|/|C(H)|$ for $K \in \mathcal{H}_j$ and $P(E_{v,j})$ for $j = 1, \dots, 6$. Since Π is closed under conjugation, when bounding $f_H(K)$ we may assume that $H = N_G(L^m)$ where L is a maximal imprimitive subgroup of A_n with 2 blocks. As in Section 2.3, we will use Stirling's inequalities. By Lemma 10, $C(H) = H \cap \Pi$ has size

$$(2/n) \cdot (n/2)!^{2m} \geq (2/n)(n/(2e))^{nm}.$$

(1) Case $j = 1$.

Let $K \in \mathcal{H}_1$ be a conjugate of $N_G(M^m)$ in G , where M is a maximal intransitive subgroup of A_n . Notice that $K \cap \Pi = \emptyset$ by Lemma 10, because $N_{S_n}(M)$ is intransitive and hence it does not contain n -cycles. Therefore $f_H(K) = 0$, implying that $P(E_{v,1}) = 0$.

(2) Case $j = 2$.

Assume K is a maximal subgroup of G conjugate to $N_G(M^m)$ where $M^m = K \cap N$, M is the intersection between A_n and a primitive maximal subgroup of S_n distinct from A_n . Since $|M| \leq 4^n$ by [37], $KN = G$ and $K \cap N$ is conjugate to M^m , we have

$$|C(H) \cap K| \leq |K| = 2m \cdot |M|^m \leq 2m \cdot 4^{mn}.$$

Therefore, by Inequality (\star) and Lemmas 15, 17,

$$P(E_{v,2}) \leq n \cdot mn \cdot \frac{mn \cdot 4^{mn}}{(n/(2e))^{mn}} = m^2 n^3 \cdot \left(\frac{8e}{n}\right)^{nm}.$$

(3) Case $j = 3$.

Assume $K = N_G(M \times M^{a_2} \times \dots \times M^{a_m})$, M is a maximal imprimitive subgroup of A_n with 3 blocks, and $a_2, \dots, a_m \in A_n$. We will bound the size of $C(H) \cap K$. Let $g \in C(H) \cap K = H \cap \Pi \cap K$, then $g = (x_1, \dots, x_m)\gamma$, where $x_1 \dots x_m \tau \in B$, and the fact that $g \in H \cap K$

implies that

$$\begin{aligned} x_1, \dots, x_{m-1}, x_m \tau &\in N_{S_n}(L), \\ a_i x_i a_{i+1}^{-1} &\in N_{S_n}(M), \quad \text{for } i = 1, \dots, m-1, \end{aligned}$$

where $a_1 = 1$, and $a_m x_m \tau \in N_{S_n}(M)$.

We deduce that

$$\begin{aligned} x_1 \dots x_i &\in N_{S_n}(L) \cap N_{S_n}(M) a_{i+1}, \quad \forall i = 1, \dots, m-1. \\ x_1 \dots x_m \tau &\in B \cap N_{S_n}(L) \cap N_{S_n}(M). \end{aligned}$$

By induction, the number of choices for x_i is $|N_{S_n}(L) \cap N_{S_n}(M) a_{i+1}|$, which is at most $|N_{S_n}(L) \cap N_{S_n}(M)|$, for every $i = 1, \dots, m-1$. Moreover, after choosing x_1, \dots, x_{m-1} , the number of choices for x_m is $|B \cap N_{S_n}(L) \cap N_{S_n}(M)|$, which is at most $|N_{S_n}(L) \cap N_{S_n}(M)|$. Therefore

$$|C(H) \cap K| \leq |N_{S_n}(L) \cap N_{S_n}(M)|^m.$$

The above discussion implies that, if $B \cap N_{S_n}(L) \cap N_{S_n}(M)$ is empty, then $f_H(K) = 0$, so now we may assume that there is an element $\sigma \in B \cap N_{S_n}(L) \cap N_{S_n}(M)$. Then σ is an n -cycle normalizing L and M . Let Δ and $\bar{\Delta}$ be the blocks of L , i.e. the two orbits of $\langle \sigma^2 \rangle$, and let B_1, B_2, B_3 be the blocks of M , i.e. the three orbits of $\langle \sigma^3 \rangle$. Then the six orbits of $\langle \sigma^6 \rangle$ are $\Delta \cap B_i$, $i = 1, 2, 3$, and $\bar{\Delta} \cap B_i$, $i = 1, 2, 3$, forming a partition P of $\{1, \dots, n\}$ consisting of 6 blocks of size $n/6$. Clearly, $N_{S_n}(L) \cap N_{S_n}(M)$ is contained in the stabilizer of the partition P , which is isomorphic to $S_{n/6} \wr S_6$, hence

$$f_H(K) = \frac{|C(H) \cap K|}{|C(H)|} \leq \frac{|N_{S_n}(L) \cap N_{S_n}(M)|^m}{|C(H)|} \leq \frac{n}{2} \cdot \left(\frac{(n/6)!^6 \cdot 6!}{(n/2)!^2} \right)^m.$$

Applying Stirling's inequalities we have that this is at most $n^{O(1)m} (1/3)^{nm}$.

By Inequality (\star) and Lemmas 15, 17, the same bound holds for $P(E_{v,3})$.

(4) Case $j = 4$.

Assume K is a maximal subgroup of G conjugate to $N_G(M^m)$ where $K \cap N = M^m$ and M is a maximal imprimitive subgroup of A_n with 4 blocks. Since $KN = G$ and $K \cap N$ is conjugate to M^m , $|K| = 2m \cdot |M|^m$, hence an application of Stirling's inequalities gives

$$f_H(K) \leq \frac{|K|}{|C(H)|} = \frac{2m \cdot ((n/4)!^4 \cdot 4!)^m}{2/n \cdot (n/2)!^{2m}} \leq n^{O(1)m} \cdot \left(\frac{1}{2}\right)^{nm}.$$

Therefore, by Inequality ($\star\star$) and Lemma 16, $P(E_{v,4}) \leq n^{O(1)m} (1/4)^{nm}$.

(5) Case $j = 5$.

Assume K is a maximal subgroup of G conjugate to $N_G(M^m)$ where $K \cap N = M^m$ and M is a maximal imprimitive subgroup of A_n with 5 or more blocks. By [6, Theorem 3], $|M| \leq n^{O(1)} \cdot (n/(5e))^n$, and since $|K| = 2m \cdot |M|^m$,

$$f_H(K) \leq \frac{2m \cdot ((n/(5e))^n \cdot n^{O(1)})^m}{2/n \cdot (n/(2e))^{nm}} \leq n^{O(1)m} \cdot \left(\frac{2}{5}\right)^{nm}.$$

By Inequality (\star) and Lemmas 15, 17, the same bound holds for $P(E_{v,5})$.

(6) Case $j = 6$.

Assume $K = N_G(\Delta_\varphi)$ is a maximal subgroup of G of diagonal type, so that $|K| = 2m \cdot |A_n|^{m/t}$ where t is a prime divisor of m . Using $t \geq 2$ and Stirling's inequalities,

$$f_H(K) \leq \frac{|K|}{|C(H)|} = \frac{2m(n!/2)^{m/t}}{(2/n)(n/2)!^{2m}} \leq n^{O(1)m} \cdot \left(\frac{2\sqrt{e}}{\sqrt{n}}\right)^{mn}.$$

By Inequality (\star) and Lemmas 15, 17, the same bound holds for $P(E_{v,6})$.

We now finish the proof of Theorem 2 by showing that $P(E_v) \leq \frac{1}{e^{(d+1)}}$ for sufficiently large n . Recall that $d \leq 2^{mn}$. The above discussion implies that

$$P(E_{v,j}) \leq n^{O(1)m} (2/5)^{nm}$$

for all $j = 1, \dots, 6$, and since

$$P(E_v) \leq \sum_{j=1}^6 P(E_{v,j}),$$

it suffices to show that $n^{O(1)m}(2/5)^{mn} \leq (1/2)^{mn}$, which is true for large enough n .

Appendix A

$\omega(G)$ for small groups G

As we discussed in the introduction, using GAP [16] and GUROBI [22], it is possible to calculate $\omega(G)$ for groups G of small orders. We will discuss some cliques and coverings of some small groups. The stated facts about the symmetric groups are known.

A.1 Computing a clique for A_5 with Gurobi

Using a GAP code, as used in [25] and [19] for the calculation of $\sigma(G)$, we can compute the value of $\omega(G)$. We will show an exemple of this calculation for $G = A_5$. We generate a file ("filename.lp") on GAP. The first step is read the file generated by GAP on Gurobi in the following way:

```
model=read("filename.lp"),
```

and optimize

```
model.optimize().
```

After optimizing, the command

```
model.getVars()
```

shows the values of all the variables.

In many models, only a small portion of the variables have nonzero values. In that case, it is usually more convenient to get a list of only the variables that have nonzero values, as follows:

```
[v.varName for v in model.getVars() if v.x>1e-6].
```

This will generate a list, in which the values that appear are the elements of G that form the clique.

For $G = A_5$, on GAP, doing

```
e1:=Enumerator(G);
```

The list obtained is

```
[e1[3], e1[16], e1[39], e1[52], e1[54], e1[57], e1[58],
  e1[59]];
```

and, in this case, these elements form a clique. The elements are, respectively, (145), (235), (12354), (15342), (12453), (15423), (14235), and (12345).

A.2 The symmetric group S_5

The minimal covering of S_5 consists of A_5 together with the intransitive maximal subgroups $S_1 \times S_4$ and $S_2 \times S_3$. The number of copies of $S_1 \times S_4$ in S_5 is $\binom{5}{1} = 5$ subgroups, and the number of copies of $S_2 \times S_3$ in S_5 is $\binom{5}{2} = 10$ subgroups. Therefore

$$\sigma(S_5) = 1 + \binom{5}{1} + \binom{5}{2} = 16 = 2^{5-1}. \text{ (See [9])}$$

On the other hand, a clique of S_5 is given by the set

$$C = \{(1532), (1534), (1234), (142)(35), (123)(45), (135)(24), (12)(354), \\ (154)(23), (15)(243), (152)(34), (14)(235), (13)(245), (143)(25)\},$$

and $|C| = 13$.

In [39] L. Stringer showed that this clique has maximal size. Therefore

$$\omega(S_5) = 13 < \sigma(S_5) = 16 = 2^{5-1}.$$

A.3 The symmetric group S_6

The unique minimal covering \mathcal{M} of S_6 is given by A_6 and the two conjugacy classes (each of size 6) of maximal subgroups isomorphic to S_5 (one consists of intransitive subgroups, the other one consists of primitive subgroups), and

$$\sigma(S_6) = 1 + 6 + 6 = 13. \text{ (See [1])}$$

A maximal clique is given by the set

$$C = \{(23)(456), (12456), (124356), (124536), (126)(34), \\ (13)(245), (135264), (145236), (15)(346), (152346), (16)(235)\}.$$

In this case $\omega(S_6) = 11 < \sigma(S_6) = 13$.

A.4 The symmetric group S_8

A minimal covering of S_8 is given by A_8 , the intransitive maximal subgroups of type $S_2 \times S_6$ and the imprimitive maximal subgroups of type $S_4 \wr S_2$. The number of copies of $S_2 \times S_6$ in S_8 is $\binom{8}{2} = 28$ subgroups, and the number of copies of $S_4 \wr S_2$ in S_8 is $\frac{1}{2} \binom{8}{4} = 35$ subgroups. Let the set of these subgroups be called \mathcal{M} .

$$\sigma(S_8) = 1 + \binom{8}{2} + \frac{1}{2} \binom{8}{4} = 64. \text{ (See [25])}$$

Using the optimization method, we can prove that $\omega(S_8) = \sigma(S_8) = 64$.

A maximal clique is given by the set

$$C = \{(27)(35486), (12)(36847), (12458367), (12573648), (12586)(37), (12647583), (12645738), (132)(475)(68), (135)(24)(678), (13724586), (13)(25478), (13647258), (13762584), (13847256), (13268745), (134)(26)(578), (13482756), (13856427), (138)(274)(56), (13286574), (13672845), (14653782), (142)(38)(576), (14863)(25), (146)(253)(78), (14862753), (14563278), (14)(276)(358), (147)(285)(36), (15372)(46), (15)(236)(478), (15326478), (15368274), (162)(387)(45), (16753)(48), (16783524), (16)(273)(458), (16273485), (16542738), (165)(283)(47), (16428)(57), (167)(28)(354), (178)(23)(465), (17243)(586), (17324685), (17825643), (17863254), (17)(256)(348), (17638254), (173)(264)(58), (17546328), (175)(286)(34), (17453628), (18764532), (18435762), (182)(35)(467), (185)(234)(67), (18623745), (18524376), (18256734), (18)(254)(367), (18742653), (18754326), (18426375)\}.$$

A.5 The symmetric group S_9

L. Stringer [39] proved that

$$235 \leq \omega(S_9) \leq 244 < 256 = \sigma(S_9),$$

and the value of $\sigma(S_9)$ comes from [25]. Let us see how she managed this. We know that $G = S_9$ has a minimal covering \mathcal{M} of size 256 consisting of A_9 and all of the maximal intransitive subgroups,

$$\sigma(S_9) = 1 + \binom{9}{1} + \binom{9}{2} + \binom{9}{3} + \binom{9}{4} = 256.$$

Let $G := S_9$ and let X be a maximal clique of G , $|X| = \omega(G)$. Since any two even permutations belong to A_9 , there is at most one element in X which is a product of an odd number of disjoint cycles. Let a be the

number of elements of type $(3, 6)$ in X , let b be the number of elements of “even” type, $(1, 8)$, $(2, 7)$ or $(4, 5)$ in X and let c be the number of elements which are product of 4 or more disjoint cycles in X , so that $|X| = a + b + c$. We have

$$b \leq 1 + \binom{9}{1} + \binom{9}{2} + \binom{9}{4} = 172.$$

Every element of type $(3, 6)$ belongs to 4 imprimitive maximal subgroups of G , and since there are precisely $\frac{|S_9|}{|S_3 \wr S_3|} = 280$ imprimitive maximal subgroups, we obtain

$$a \leq 280/4 = 70,$$

which is less than $\binom{9}{3} = 84$. An easy inspection shows that any element of S_9 which is a product of 4 or more disjoint cycles lies in at least 10 members of \mathcal{M} , so since each member of \mathcal{M} contains at most one element of X , we deduce that

$$|X| + 9c = a + b + 10c \leq \sigma(G) = 256,$$

so $|X| \leq 256 - 9c$. We deduce that

$$|X| = a + b + c \leq 70 + 172 + \frac{256 - |X|}{9}.$$

Therefore $\omega(G) = |X| \leq 243$.

Stringer also found a clique of size 235, proving that $\omega(G) \geq 235$.

Using the optimization method, we can prove that $239 \leq \omega(G) \leq 241$.

A.6 The symmetric group S_{10}

A minimal covering \mathcal{M} of S_{10} is given by A_{10} , the intransitive maximal subgroups of type $S_1 \times S_9$, the imprimitive maximal subgroups of type $S_5 \wr S_2$ and the maximal subgroups of type $S_3 \times S_7$ with 1 not belonging to the orbit of size 3. This last set partitions the elements of cycle type

$(3, 3, 4)$. The number of copies of $S_1 \times S_9$ in S_{10} is $\binom{10}{1} = 10$, the number of copies of $S_5 \wr S_2$ in S_{10} is $\frac{1}{2} \binom{10}{5} = 126$ subgroups and the number of copies of $S_3 \times S_7$ with 1 not belonging to the orbit of size 3 in S_{10} is $\binom{9}{3} = 84$ subgroups. These subgroups could be our \mathcal{M} .

$$\sigma(S_{10}) = 1 + \binom{10}{1} + \binom{10-1}{3} + \frac{1}{2} \binom{10}{5} = 221. \text{ (See [25])}$$

Using the optimization method, we can prove that $\omega(S_{10}) = 191$.

Bibliography

- [1] A. Abdollahi, F. Ashraf, and 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). 30:1 (2007), 57–58.
- [2] J. Almeida, M. Garonzi. “On minimal coverings and pairwise generation of some primitive groups of wreath product type.” *Journal of Algebra and its Applications*. (2023). <https://doi.org/10.1142/S0219498824501883>
- [3] N. Alon, J. H. Spencer. *The Probabilistic Method*. Fourth edition. Wiley Series in Discrete Mathematics and Optimization. John Wiley and Sons, Inc., Hoboken, NJ, 2016.
- [4] M. Aschbacher, R. Guralnick, “Some applications of the first cohomology group.” *Journal of Algebra*, Volume 90, Issue 2. (1984), 446–460.
- [5] A. Ballester-Bolinches, L. M. Ezquerro. *Classes of Finite Groups*. Mathematics and Its Applications (Springer), 584. Springer, Dordrecht, 2006.
- [6] S. R. Blackburn. “Sets of permutations that generate the symmetric group pairwise.” *J. Combin. Theory Ser. A*. 113:7 (2006), 1572–1581.
- [7] J. R. Britnell, A. Evseev, R. M. Guralnick, P. E. Holmes, A. Maróti. “Sets of elements that pairwise generate a linear group.” *J. Comb. Theory Ser. A*, Volume 115, Issue 3, (2008), 442–465.
- [8] R. A. Bryce, V. Fedri, and L. Serena. “Subgroup coverings of some linear groups.” *Bull. Austral. Math. Soc.*, 60(2) (1999), 227–238.
- [9] J. H. E. Cohn. “On n -sum groups.” *Math. Scand*. 75:1 (1994), 44–58.

- [10] F. Dalla Volta, A. Lucchini A. “Finite groups that need more generators than any proper quotient.” *Journal of the Australian Mathematical Society Series A Pure Mathematics and Statistics*, 64(1) (1998), 82–91.
- [11] E. Detomi, A. Lucchini. “On the structure of primitive n -sum groups.” *Cubo* 10, no. 3 (2008), 195–210.
- [12] M. Epstein, S. Magliveras, and D. Nikolova-Popova. “The covering numbers of A_9 and A_{11} .” *J. Combin. Math. Combin. Comput.* 101 (2017), 23–36.
- [13] P. Erdős, L. Lovász. “Problems and results on 3-chromatic hypergraphs and some related questions.” *Infinite and finite sets*, Vols. I, II, III, pp. 609–627. *Colloq. Math. Soc. János Bolyai*, Vol. 10, North-Holland, Amsterdam, 1975.
- [14] F. Fumagalli, M. Garonzi, P. Gheri. “On the maximal number of elements pairwise generating the finite alternating group.” (2022). <https://doi.org/10.48550/arXiv.2206.11388>
- [15] F. Fumagalli, M. Garonzi, A. Maróti. “On the maximal number of elements pairwise generating the symmetric group of even degree.” *Discrete Math.* 345 (2022), no. 4, Paper No. 112776, 7 pp.
- [16] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.
- [17] M. Garonzi. “Covering certain monolithic groups with proper subgroups.” *Comm. Algebra.* 41:2 (2013), 471–491.
- [18] M. Garonzi. “Finite groups that are the union of at most 25 proper subgroups.” *J. Algebra Appl.*, 12(4):1350002 (2013), 11.
- [19] M. Garonzi, L.-C. Kappe, E. Swartz. “On Integers that are Covering Numbers of Groups.” *Experimental Mathematics*, 31:2 (2022), 425–443.
- [20] M. Garonzi, A. Maróti. “Covering certain wreath products with proper subgroups.” *J. Group Theory*, vol. 14, no. 1, (2011), 103–125.

- [21] W. Gaschütz, Existenz und Konjugiertsein von Untergruppen, die in endlichen auflösbaren Gruppen durch gewisse Indexschränken definiert sind; *Journal of Algebra* 53 (1978), 1–20.
- [22] Gurobi Optimizer Reference Manual, Gurobi Optimization, Inc., 2024, ([gurobi.com](https://www.gurobi.com)).
- [23] B. Huppert. *Endlich Gruppen I*. Springer-Verlag Berlin, 1967.
- [24] I. N. Jacobson. *Basic Algebra*. Freeman and Company, 2 edition. 1995.
- [25] L.-C. Kappe, D. Nikolova-Popova, E. Swartz. “On the covering number of small symmetric groups and some sporadic simple groups.” *Groups Complex. Cryptol.* 8:2 (2016), 135–154. **Files related to this paper can be found in** <https://www.math.wm.edu/~eswartz/coverings>. Accessed 26 February 2024.
- [26] L.-C. Kappe, J. L. Redden. “On the covering number of small alternating groups.” *Computational group theory and the theory of groups, II*, *Contemp. Math.*, vol. 511 (2010), 109–125.
- [27] M. W. Liebeck, C. E. Praeger, J. Saxl. “A classification of the maximal subgroups of the finite alternating and symmetric groups.” *J. Algebra* 111 (1987), no. 2, 365–383.
- [28] M. W. Liebeck, C. E. Praeger, J. Saxl. “On the O’Nan-Scott theorem for finite primitive permutation groups.” *J. Austral. Math. Soc. Ser. A* 44 (1988), no. 3, 389–396.
- [29] A. Lucchini, A. Maróti. “On finite simple groups and Kneser graphs.” *J. Algebr. Comb.*, 30, (2009) 549–566
- [30] A. Lucchini, A. Maróti. “On the clique number of the generating graph of a finite group.” *Proc. Amer. Math. Soc.*, Volume 137, Number 10, (2009), 3207–3217.
- [31] A. Lucchini, F. Menegazzo, Generators for finite groups with a unique minimal normal subgroup. *Rend. Semin. Mat. Univ. Padova* 98 (1997), p. 173–191

- [32] M. S. Lucido, On the covers of finite groups; Groups St. Andrews 2001 in Oxford. Vol. II, 395–399, London Math. Soc. Lecture Note Ser., 305, Cambridge Univ. Press, Cambridge, 2003.
- [33] A. Maróti. “On the orders of primitive groups.” *J. Algebra*, Volume 258, Issue 2, (2002), 631–640.
- [34] A. Maróti. “Covering the symmetric groups with proper subgroups.” *J. Combin. Theory Ser. A*. 110:1 (2005), 97–111.
- [35] G. Niero. Il grafo di generazione delle potenze del gruppo alterno di grado 5. Master’s thesis, Università degli Studi di Padova, 2018.
- [36] R. Oppenheim, E. Swartz. “On the covering number of S_{14} .” *Involve*. 12:1 (2019), 89–96. **Supplementary material:** GAP code: <https://msp.org/involve/2019/12-1/involve-v12-n1-x07-GAPCode.pdf>. Accessed 26 February 2024.
- [37] C. E. Praeger, J. Saxl. “On the orders of primitive permutation groups.” *Bull. Lond. Math. Soc.*, Volume 12, Issue 4, (1980) 303–307.
- [38] R. Steinberg, R. “Generators for Simple Groups.” *Canadian Journal of Mathematics*, 14, (1962). 277–283
- [39] L. Stringer. Pairwise generating sets for the symmetric and alternating groups. PhD thesis, Royal Holloway, University of London, 2008.
- [40] E. Swartz. “On the covering number of symmetric groups having degree divisible by six.” *Discrete Math.* 339:11 (2016), 2593–2604.
- [41] M.J. Tomkinson, Groups as the union of proper subgroups; *Math. Scand.*, 81(2) (1997), 191–198.
- [42] H. Wielandt. *Finite Permutation Groups*. Academic Press. 1964.
- [43] Wikipedia. “Bertrand’s postulate.” https://en.wikipedia.org/wiki/Bertrand%27s_postulate. Accessed 26 February 2024.
- [44] R. Wilson. *The finite simple groups*. 2009, Springer.