UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Matematica "Tullio Levi-Civita"

CORSO DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE
INDIRIZZO MATEMATICA
CICLO XXXIII

Generation and enumeration questions in finite groups and permutation groups

Coordinatore: Prof. Martino Bardi

Supervisore: Prof. Andrea Lucchini

Dottoranda: Mariapia Moscatiello

Abstract

This thesis contains results in abstract group theory, permutation group theory, and combinatorics.

In Chapter 2, we study invariants regarding the generation of finite groups. Let G be a finite group with all the Sylow subgroups d-generated, then the expected number of elements of G which have to be drawn, at random, with replacement before a set of generators is found, $e(G)$, is bounded above by $d+\kappa$, where κ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context. This result can be extended to the case of finitely generated profinite groups. The above bound can be improved under some additional assumptions on G. Moreover, if G is a permutation group of degree n, then either $G = \mathrm{Sym}(3)$ and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ and κ^* is best possible.

We prove that if G is a soluble group having, for every prime divisor p of the order of G, a subgroup G_p such that p does not divide $|G : G_p|$ and $e(G_p) \leq d$, then $e(G) \leq d + 9$. Generalizing the question to profinite groups, we prove that a finitely generated profinite group G having the 2-Sylow subgroups finitely generated is positively finitely generated (PFG). However, the following question is still open: *Is it true that if a finitely generated profinite group G contains a PFG closed subgroup with odd index, then G is PFG?*

We compare the expected number of elements of the symmetric group of degree n which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup is found and those of the alternating group.

We estimate $m(G)$, that is the largest size of a minimal generating set of a finite group G, in terms of a function of the minimal number of generators of the Sylow subgroups of G.

The Tarski irredundant basis theorem implies that for every k with $d(G) \leq k < m(G)$ there exist a minimal generating set ω of size k, an element g in ω and x, y in G such that $\omega^* = (\omega - \{g\}) \cup \{x, y\}$ is again a minimal generating set of G. In this case, we say that ω^* is an immediate descendant of ω. There are several examples of minimal generating sets of cardinality smaller than $m(G)$ which have no immediate descendant, so it appears an interesting problem to investigate under which conditions an immediate descendant exists. We discuss this problem for finite soluble groups.

In Chapter 3 we focus on the theory of permutation groups. We prove that the base size of a finite non large-base primitive permutation group of degree n is bounded above by the maximum between 7 and $\lceil \log n \rceil + 1$. Further, we show that there are infinitely many non-large base primitive groups for which the base size is bigger than $\log n + 1$, so our bound is optimal.

We present a polynomial estimation of the number of maximal systems of imprimitivity of a transitive permutation group of degree n given in terms of n. When the group is soluble a much stronger result holds.

Finally, we classify the subgroups H of G such that the overgroup lattice of H in G, is Boolean of rank at least 3 when G is a finite alternating or symmetric group. Besides some sporadic examples and some twisted versions, there are two different types of such lattices. One type arises by taking stabilizers of chains of regular partitions, and the other by taking stabilizers of chains of regular product structures. As an application, in these cases, we prove a conjecture on Boolean overgroup lattices related to a dual Ore's theorem and to a problem of Brown.

In Chapter 4 we are interested in the asymptotic enumeration of Cayley graphs. It has previously been shown that almost every Cayley digraph has the smallest possible automorphism group: that is, it is a digraphical regular representation. We approach the corresponding question for undirected Cayley graphs.

Riassunto

Questa tesi contiene risultati nella teoria dei gruppi astratti, nella teoria dei gruppi di permutazione e in combinatoria.

Sia G un gruppo finito avente tutti i sottogruppi di Sylow d-generati, allora $e(G)$, ovvero il valore atteso del numero di elementi di G che devono essere estratti, casualmente e con ripetizione, prima di ottenere un insieme di generatori, è superiormente limitato da $d + \kappa$, dove κ è una costante assoluta che può essere esplicitamente determinata in termini della funzione zeta di Riemann ed è ottimale in questo contesto. Tale risultato può essere esteso al caso di gruppi profiniti finitamente generati. La suddetta stima è migliorabile ponendo ulteriori ipotesi sul gruppo G. Inoltre se G è un gruppo di permutazione di grado n, allora $G = \mathrm{Sym}(3)$ e $e(G) = 2.9$ oppure $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ e κ^* è ottimale.

Dimostriamo che, se G è un gruppo risolubile avente per ogni divisore primo dell'ordine di G un sottogruppo G_p con indice non divisibile per p e tale che $e(G_p) \leq d$, allora $e(G) \leq d+9$. Generalizzando ai gruppi profiniti, proviamo che un gruppo profinito finitamente generato avente i 2-Sylow finitamente generati è positivamente finitamente generato (PFG). Tuttavia, il seguente problema è ancora aperto: *E' vero che se un gruppo profinito finitamente generato G contiene un sottogruppo chiuso di indice dispari e PFG, allora G è PFG?*

Confrontiamo il numero atteso di elementi del gruppo simmetrico di grado n che devono essere estratti, casualmente e con ripetizione, prima che si trovi un insieme di generatori di un sottogruppo transitivo con quelli del gruppo alternato.

Stimiamo $m(G)$, ovvero la cardinalità massima di un insieme minimale di generatori di un gruppo finito G, in termini di una funzione del numero minimo di generatori dei sottogruppi di Sylow di G.

Il teorema della base ridondante di Tarski implica che per ogni k con $d(G) \leq k < m(G)$, esiste un insieme minimale di generatori ω di dimensione k, un elemento g in ω e x, y in G tale che $\omega^* = (\omega - \{g\}) \cup \{x, y\}$ è ancora un insieme minimo di generatori di G. In questo caso, diciamo che ω^* è un discendente immediato di ω. Esistono diversi esempi di gruppi aventi generatori minimali di cardinalità inferiori a $m(G)$ senza discendenti immediati, quindi sembra interessante indagare sotto quali condizioni esiste un discendente immediato. Discutiamo questo problema per gruppi risolubili finiti.

Nel Capitolo 3 ci siamo soffermati sulla teoria dei gruppi di permutazione. Dimostriamo che la dimensione della base di un gruppo di permutazioni primitivo finito di base non ampia e di grado n è al più il massimo tra 7 e $\lceil \log n \rceil + 1$. Inoltre, mostriamo che ci sono infiniti gruppi primitivi di base non ampia la cui dimensione della base è maggiore di $\log n + 1$, per cui la nostra stima è ottimale.

Presentiamo una stima polinomiale del numero dei sistemi massimali di imprimitività di un gruppo di permutazione transitivo di grado n data in termini di n. Se G è risolubile otteniamo una stima migliore.

In fine, abbiamo classificato i sottogruppi H di G tali che il reticolo dei gruppi contenenti H in G sia Booleano di rango almeno 3 quando G è un gruppo alterno o simmetrico finito. Eccetto alcuni esempi sporadici o versioni intrecciate, ci sono due tipi distinti di tali reticoli. Un tipo nasce prendendo gli stabilizzatori di catene di partizioni regolari e l'altro prendendo gli stabilizzatori di catene di strutture prodotto regolari. Come applicazione, proviamo in questi casi una congettura sui reticoli Booleani legati ad un problema duale di Ore e ad un problema di Brown.

Nel Capitolo 4 siamo interessati all'enumerazione asintotica dei grafi di Cayley. Precedentemente è stato provato che quasi ogni digrafo di Cayley ha il più piccolo possibile gruppo di automorfismi: cioè, esso è una rappresentazione digrafica regolare. Abbiamo approcciato la

corrispondente questione per grafi di Cayley indiretti.

Introduction

This thesis consists of four Chapter and contains themes regarding the theory of generation and random generation of groups, the theory of permutation groups, and combinatorics. In the first Chapter we summarize very briefly some tools and some famous results used through the thesis.

Generation of groups

The problem of investigating generating sets for a finite group has a rich history. Let G be a finitely generated group and let $d(G) := \min\{|S| \mid G = \langle S \rangle\}$ be the minimal number of generators for G. The invariant $d(G)$ has been deeply studied for many groups G. Gaschütz [55] gave a formula to compute the minimal number of generators of a finite soluble group in terms of certain 'local' and 'global' parameters associated to a chief series of the group. On the other side, it follows from the classification of finite simple group (CFSG) that every finite simple group can be generated by just two of its elements ([156], [7]). The classification of finite simple groups is involved heavily and plays a central role in most general results on generation of a finite group. The fact that every finite simple group can be generated by just two of its elements leads naturally to a wide range of interesting questions concerning the abundance of generating pairs and their distribution across the group. Burness's survey article [23] provides some of the more recent developments.

A well known result proved by Dixon [47], Kantor and Lubotzky [77], Liebeck and Shalev [91] states that every sufficiently large finite simple group is 2-generated, without constructing a pair of generators. Already from this result, it appear clear that, in the context of generation of groups, a central role is played by probabilistic methods. For a review on the technique and on recent results on the probabilistic method in group theory see [87].

We denote by $e(G)$ the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. In [64, 103], it was showed that the invariants $P_G(t)$ and $e(G)$ can be express by using the Möbius function on the subgroup lattice of G (See Chapter 2 for more details on this). Hence these results are really appealing when the subgroup structure of the group G is well known.

Pomerance [137] showed that if G is a nilpotent group, then $e(G) \leq d(G) + \sigma$ where the constant $\sigma \sim 2.1185$ is explicitly described in terms of the Riemann zeta function and is the best possible. Whilst Kantor and Lubotzky proved that, for every positive real number ϵ and every positive integer k, there exists a 2-generated finite group $G_{\epsilon,k}$ with $P_{G_{\epsilon,k}}(t) \leq \epsilon$ for every $t \leq k$. From this result, it is easy to deduce that $e(G) - d(G)$ is unbounded in general (in Chapter 2, we explain this more precisely). Others key estimation on $e(G)$ can be found in [44] and [96].

Here, we pass from the theory of random generation to a question regarding the theory of minimal generation. A generating set X of a finite group G is said to be *minimal* if no proper subset of X generates G. We denote by $m(G)$ the largest size of a minimal generating set of G.

First steps toward investigating $m(G)$ have been taken in the context of permutation groups. An exhaustive investigation has been done for finite symmetric groups [34, 163], proving that $m(\mathrm{Sym}(n)) = n - 1$ and giving a complete description of the independent generating sets of $\mathrm{Sym}(n)$ having cardinality $n-1$. Partial results for some families of simple groups are in [152]: it turns out that already in the case $G = \mathrm{PSL}(2, q)$, the precise value of $m(G)$ is quite difficult to obtain. Moreover, Apisa and Klopsch [1] classified the finite groups for which the equality $m(G) = d(G)$ holds. During the same period, Lucchini started in [104, 105] a systematic investigation of how $m(G)$ can be estimated for an arbitrary finite group G. Finally, there is a nice result in universal algebra, known with the name of Tarski irredundant basis theorem (see for example [29, Theorem 4.4]), which implies that G contains an independent generating set of cardinality k, for every positive integer $d(G) \leq k \leq m(G)$.

In this thesis, the Chapter 2 is devoted to the presentation of some results concerning the generation of finite (and profinite) groups based on joint works with A. Lucchini and P. Spiga [82], [107], [108], [109], [110], [113]. Before passing to the organization of this Chapter, it is worth noting that the importance of the topics here presented can be conduct to an algorithm in computational group theory, the Product Replacement Algorithm. Indeed, estimations on $e(G)$, $m(G)$ and $d(G)$ can be used to analyze the efficiency of this algorithm.

Section 2.1. [109] Let G be a finite group with all the Sylow subgroups of G d-generated. In this Section, we proved that $e(G) \leq d + \kappa$, where $\kappa \sim 2.752394$ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context. This bound can be further improved under some additional assumptions on G. For example, when G is not soluble, then $e(G) \leq d + 2.750065$. A stronger result holds if $|G|$ is odd. Indeed, we show that $e(G) \leq d + \tilde{\kappa}$ with $\tilde{\kappa} \sim 2.148668$. From the proof of this case, it is possible to deduce that a precise estimation of $e(G)$ for $|G|$ odd would require a complete knowledge of the distribution of the Fermat primes.

Moreover we proved that a permutation group G of degree n, then either $G = \mathrm{Sym}(3)$ and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ with $\kappa^* \sim 1.606695$. Let $m = \lfloor n/2 \rfloor$ and set $G_n = \mathrm{Sym}(2)^m$ if m is even, $G_n = \mathrm{Sym}(2)^{m-1} \times \mathrm{Sym}(3)$ if m is odd. If $n \geq 8$, then $e(G_n) - m$ increases with n and $\lim_{n\to\infty} e(G) - m = \kappa^*$, that is κ^* is best possible.

Section 2.2. [82, 108] In this section we investigate the following question for a finite group G. Assume that G has a family $H_1, \ldots, H_t$ of subgroups whose indices have no common divisor and such that $e(H_i) \leq d$ for every $1 \leq i \leq d$. Is it true that $e(G)$ can be bounded in term of d? To head towards this question we analyzed some invariants related to $e(G)$, such as

$$\nu(G) := \min\left\{ k \in \mathbb{N} \;\middle|\; P_G(k) \geq \frac{1}{e} \right\} \quad \text{and} \quad \mathcal{M}(G) := \sup_{n\geq 2} \frac{\log m_n(G)}{\log n}$$

where e is the Nepero number, n is a natural number and $m_n(G)$ is the number of maximal subgroups of G with index n. (Henceforth log denote the logarithm in base 2). As it was noted in [96, Propositions 1.1, 1.2], $e(G)$, $\nu(G)$, and $\mathcal{M}(G)$ are related in the following way:

$$\begin{gathered} \frac{1}{e} \cdot e(G) \leq \nu(G) \leq \frac{e}{e-1} \cdot e(G) \\ (\mathcal{M}(G) - 3.5) \cdot \frac{e-1}{e} \leq e(G) \leq (\mathcal{M}(G) + 2.02) \cdot e. \end{gathered} \tag{0.0.1}$$

However the estimation in (0.0.1) leaves open the question whether $|\mathcal{M}(G) - e(G)|$ could be arbitrarily large. In this section, we observed that the arguments used in [96] can be improved and the following result can be obtained:

$$\lceil \mathcal{M}(G) \rceil - 4 \leq e(G) \leq \lceil \mathcal{M}(G) \rceil + 3. \tag{0.0.2}$$

Using (0.0.1) we proved that if G is a finite soluble group having, for every $p \in \pi(G)$, a subgroup G_p such that p does not divide $|G : G_p|$ and $\nu(G_p) \leq d$, then $\nu(G) \leq d + 7$. Here, by means of (0.0.2) we were able to obtain the result we aimed for. Let G be a finite soluble group. Assume that for every prime p dividing $|G|$, there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $e(G_p) \leq \rho$. Then $e(G) \leq \rho + 9$.

A natural question is whether there is an analogous of the previous theorem for arbitrary finite groups. To prove such a result, we would need to deduce a bound on the number of maximal subgroups of G of a given index from the following hypothesis.
For every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $\nu(G_p) \leq d$.

The difficult part is to find an efficient estimation on the numbers of the maximal subgroups M of G such that the socle of G/M_G is a nonabelian group. We think that it could be possible to use for this purpose the assumption $\nu(G_2) \leq d$. An evidence that this could work is that, in [98], it is showed that the number of such maximal subgroups having index n can be bounded in terms of the smallest cardinality of a generating set of a Sylow 2-subgroup of G. We would need a similar result, using a subgroup of odd index instead of a Sylow 2-subgroup.

Whether the role of a 2-Sylow subgroup can be played by an arbitrary subgroup of odd index is a problem regarding a more wide class of groups. Let us explain how a similar question also arises in the context of profinite groups. We proved that, if G is a finitely generated profinite group and if the 2-Sylow subgroups of G are finitely generated, then G is PFG. We do not know whether the previous result remains true if we only assume that there is a closed subgroup of G which is of odd index and PFG. Therefore, the " profinite version" of our problem, that is
Is it true that if a finitely generated profinite group G contains a PFG closed subgroup of odd index, then G is PFG?
is still open.

Section 2.3. [107] Let G be a transitive subgroup of $\mathrm{Sym}(n)$. Let $\mathrm{P}_{\mathcal{T}}(G, t)$ be the probability that t randomly chosen elements of G generate a transitive subgroup of G. We denote by $e_{\mathcal{T}}(G)$ the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of G is found. In this subsection we prove that, for every natural number $n \geq 3$, then

$$P_{\mathcal{T}}(\mathrm{Sym}(n), t) - P_{\mathcal{T}}(\mathrm{Alt}(n), t) = \frac{(-1)^{n+1}(n-1)!(2^t - 1)}{(n!)^t}, \tag{0.0.3}$$

$$e_{\mathcal{T}}(\mathrm{Sym}(n)) - e_{\mathcal{T}}(\mathrm{Alt}(n)) = \frac{(-1)^{n+1} n!(n-1)!}{(n! - 1)(n! - 2)}. \tag{0.0.4}$$

Observe that $e_{\mathcal{T}}(\mathrm{Sym}(n)) - e_{\mathcal{T}}(\mathrm{Alt}(n))$ tends to zero when n tends to infinity, and it is positive if n is odd and negative otherwise. Further, we prove that, for $n \geq 3$, the following hold

1. If n is odd, then $\frac{3}{2} = e_{\mathcal{T}}(\mathrm{Alt}(3)) \leq e_{\mathcal{T}}(\mathrm{Alt}(n)) < 2$.
2. If n is even, then $2 < e_{\mathcal{T}}(\mathrm{Alt}(n)) \leq e_{\mathcal{T}}(\mathrm{Alt}(4)) = \frac{394}{165} \sim 2.3879$.

Moreover, $\lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Alt}(n)) = 2$.

Section 2.4 [113] Let p a prime divisors of the order of G, let $d_p(G)$, be the minimal size of a generating set of a Sylow p-subgroup of G. If G is a finite nilpotent group, then $m(G) = \sum_{p\in\pi(G)} d_p(G)$. For simplicity, we let

$$\delta(G) := \sum_{p\in\pi(G)} d_p(G).$$

In a private communication to Lucchini, Keith Dennis has conjectured that $m(G) \leq \delta(G)$, for every finite group G. We proved that this is true for soluble groups. Despite this, Dennis' conjecture is false if G is a symmetric group. Indeed studying the asymptotic behavior of the function $\delta(\mathrm{Sym}(n))$, (see Subsection 2.4.4), we showed that $\delta(\mathrm{Sym}(n)) = \log_e 2 \cdot n + o(n)$ for every $n \geq 2$. Since $m(\mathrm{Sym}(n)) = n - 1$ by [163], the difference $m(\mathrm{Sym}(n)) - \delta(\mathrm{Sym}(n))$ goes to infinity with n and the inequality $m(\mathrm{Sym}(n)) \leq \delta(\mathrm{Sym}(n))$ is satisfied by only finitely many values of n. We show by elementary means that, for every positive real number $\eta > 1$, there exists a constant c_η such that $m(\mathrm{Sym}(n)) = n - 1 \leq c_\eta(\delta(\mathrm{Sym}(n))^\eta$, for every $n \in \mathbb{N}$. This motivates the following conjecture, which can be seen as a natural generalization of Dennis' conjecture.

Conjecture 1. *There exist two constants c and η such that $m(G) \leq c \cdot \delta(G)^\eta$ for every finite group G.*

A crucial step towards a proof of Conjecture 1 is the following theorem proved in this section. If G is a finite group and there are two constants $\sigma \geq 1$ and $\eta \geq 2$ such that $m(X) - m(X/S) \leq \sigma \cdot |\pi(S)|^\eta$, for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$, then $m(G) \leq \sigma \cdot \delta(G)^\eta$.

Hence we reduces Conjecture 1 to the following conjecture on finite almost simple groups.

Conjecture 2. *There exist two constants σ and η such that $m(X, \operatorname{soc} X) \leq \sigma \cdot |\pi(\operatorname{soc} X)|^\eta$, for every finite almost simple group X.*

Conjecture 2 holds true, with $\eta = 2$, when $\operatorname{soc} X$ is an alternating group or a sporadic simple group. Hence, we deduce that there exists a constant σ such that, if G has no composition factor of Lie type, then $m(G) \leq \sigma\delta(G)^2$. We observe that Conjecture 2 holds true when $G \in \{\mathrm{PSL}(2,q), \mathrm{SO}(3,q), \mathrm{SU}(3,q)\}$. These partial results lead us to conjecture that, if $\operatorname{soc}(X)$ is a group of Lie type of rank n over the field with $q = p^r$ elements, then $m(X) - m(X/\operatorname{soc} X)$ is polynomially bounded in terms of n and $\tilde{\pi}(r)$. If this were true, then Conjecture 2 would also be true.

Section 2.5 [110] The proof of the theorem of Tarski above mentionad relies on a clever but elementary counting argument which implies also the following result: for every k with $d(G) \leq k < m(G)$ there exists a minimal generating set $\{g_1, \ldots, g_k\}$ with the property that there are $1 \leq i \leq k$ and x_1, x_2 in G such that $\tilde{\omega} := \{g_1, \ldots, g_{i-1}, x_1, x_2, g_{i+1}, \ldots, g_k\}$ is again a minimal generating set of G. Moreover x_1, x_2 can be chosen with the extra property that $g_i = x_1x_2$. Let $\omega := \{g_1, \ldots, g_k\}$ be a minimal generating set of G with $k < m(G)$. We say that $\omega = (g_1, \ldots, g_k)$ is *extendible* if there exist $1 \leq i \leq k$ and x_1, x_2 in G such that $\tilde{\omega} := \{g_1, \ldots, g_{i-1}, x_1, x_2, g_{i+1}, \ldots, g_k\}$ is a minimal generating set of G. In this case we say that $\tilde{\omega}$ is an *immediate descendant* of ω. Furthermore, if $g_i = x_1x_2$, then we say that $\tilde{\omega}$ is a *strong immediate descendant* of ω. More in general, a minimal generating set ω^* of cardinality t (with $t > k$) *is a (strong) descendant* of ω if there exists a sequence $\omega_0, \omega_1, \ldots, \omega_{t-k}$ where $\omega_0 = \omega$, $\omega^* = \omega_{t-k}$ and ω_j is a (strong) immediate descendant of ω_{j-1} for every $1 \leq j \leq t - k$. Finally we say that ω is *(strongly) totally extendible* if it has a (strong) descendant of cardinality $m(G)$.

There exist minimal generating sets that are not totally extendible. For example, let $G = \mathrm{Sym}(4)$ and consider $g_1 = (1,2,3,4)$ and $g_2 = (1,3,2,4)$. Clearly $G = \langle g_1, g_2\rangle$. Assume, by contradiction, that there exists x_1 and x_2 such that $\{x_1, x_2, g_i\}$ is a minimal generating set of G, with $j \in \{1,2\}$. For $i \in \{1,2\}$, we have that $\langle x_i, g_j\rangle$ is a proper subgroup of G containing g_j, but this implies $x_i \in N_G(\langle g_j\rangle)$: as a consequence $\langle g_j\rangle$ is normal in $G = \langle x_1, x_2, g_j\rangle$, but this is false. Therefore $\{g_1, g_2\}$ is not extendible. One can ask whether in a finite group G there exists at least one generating set of cardinality $d(G)$ which is totally extendible. We prove in this subsection that this happens for finite soluble groups.

We now say that G *has the extension property* if every minimal generating set of G whose cardinality is strictly less than $m(G)$ has an immediate descendant. In this section, we investigated the structure of the finite groups satisfying the extension property. In the case of finite nilpotent groups, a complete description can be easily obtained: a finite nilpotent group G has the extension property if and only if either G is a p-group or G is cyclic and $|\pi(G)| = 2$. Here, we characterize the finite soluble groups with the extension property. In particular we proved that, a finite soluble group satisfies the extension property if and only if one of the following occurs:

1. $d(G) = m(G)$.
2. $G/\operatorname{Frat} G = V \rtimes H$ where V is an irreducible H-module, $d(H) = m(H) = 2$ and whenever $\{h_1, h_2\}$ is a generating set of H, then there exists $i \in \{1, 2\}$ such that $C_V(h_i) = \{0\}$. In this case $d(G) = 2$ and $m(G) = 3$.
3. G is cyclic and $|\pi(G)| = 2$.

We deduce that, if G is finite soluble group with the extension property, then $|\pi(G)| \leq 3$ and $m(G) \leq d(G) + 1$. Let H be the dicyclic group of order 12. This group has an action on the 2-dimensional vector space V over the field with 13 elements and this action is irreducible and fixed-point-free: we may then consider the semidirect product $G = V \rtimes H$. Hence the bound $|\pi(G)| \leq 3$ is best possible.

Problems in permutation groups

The theory of permutation groups is an old subject, stretching all the way back to the origin of group theory, with a long tradition and many applications. The modern notion of permutation groups is extremely flexible and used thorough the maths. We focus on finite permutation groups, which continues to be a very active area of current research. The concept of primitive permutation group is central in permutation groups, since these groups can be viewed as the basic building blocks of all permutation groups. Being a very powerful tool for studying finite primitive permutation groups the O'Nan-Scott Theorem is an essential result in this context. This theorem describe the structure finite primitive permutation and the action in terms of the socle of the group, and usually it can be used to reduce a general problem to a much more specific problem concerning almost simple groups. Already from this consideration it appears evident that the Classification of finite simple group has revolutioned the study of finite permutation groups.

In the 19th century, a problem that attracted a lot of attention was that of bounding the order of a finite primitive permutation group. One of the earliest results in this direction is a theorem of Bochert [17] from 1889, which states that if G is a primitive permutation group of degree n not containing the alternating group $\operatorname{Alt}(n)$, then $b(G) \leq n/2$.

Let G be a permutation group on Ω. A subset $\mathcal{B}$ of Ω is a *base* for G if the pointwise stabilizer $G_{(\mathcal{B})}$ is trivial. The *base size* of G, $b(G)$, is the minimal cardinality of a base for G. Since the elements of G are uniquely determined by their effect on a base, then $|G| \leq |\Omega|^{b(G)}$. So one can find an upper bound on the order of a permutation group by bounding the minimal base size. The permutation group G is *large base* if there exist integers m and $r \geq 1$ such that $\operatorname{Alt}(m)^r \trianglelefteq G \leq \operatorname{Sym}(m) \operatorname{wr} \operatorname{Sym}(r)$, where the action of $\operatorname{Sym}(m)$ is on k-element subsets of $\{1, \ldots, m\}$ and the wreath product acts with product action. Note that this includes the natural action of $\operatorname{Alt}(n)$ and $\operatorname{Sym}(n)$. Using the Classification of Finite Simple Groups and building on earlier work by Cameron [31], Liebeck proved that if G is not large base primitive permutation group of degree n, then $b(G) \leq 9 \log n$. Having interesting connections to other areas of mathematics, such as representation theory and graph theory, the concept of bases is crucial in permutation groups. Moreover, since the permutation groups can be

seen as prototype to understand and model the different types of symmetry, the importance of estimation on the base size can be mainly traced to the fact that the concept of bases is an essential tool to capture these symmetries in a more affordable way.

Cameron in [30] proposed one other estimation in the theory of permutation groups. Precisely, if G is a transitive permutation group of degree n, he asked for a polynomial estimation, in terms of n, of the number of maximal system of imprimitivity of G. This question extends naturally to the following question of Wall. In 1961, Wall [160] has conjectured that the number of maximal subgroups of a finite group G is less than the group order $|G|$. Wall himself proved the conjecture under the additional hypothesis that G is soluble. Nearly half a century later, Liebeck, Pyber and Shalev proved [95, Theorem 1.3] a polynomial version of Wall's conjecture: there exists an absolute constant c such that, every finite group G has at most $c|G|^{3/2}$ maximal subgroups. Wall's conjecture was disproved in 2012 by the participants of an AIM workshop, see [63]. (To see how the Question of Cameron extends naturally the question of Wall see Chapter 3)

Now, we briefly describe the motivation for this question. In [2], it was proved that for a finite transitive permutation group G on Ω then: for any map a of rank 2, (that is, one whose image has cardinality 2), the semigroup $\langle G, a\rangle \setminus G$ is idempotent-generated if and only if for every orbit $\mathcal{O}$ of G on 2-sets of Ω, and every maximal block of imprimitivity B for G acting on $\mathcal{O}$, the graph with vertex set Ω and edge set $\mathcal{O} \setminus B$ is connected. Since there are exponentially many maps of rank 2, there are only a linear number of orbits $\mathcal{O}$ of G on 2-sets of Ω, and connectedness is very fast to check a positive answer to the question of Cameron would reveal that the above characterization in combinatorial terms is more convenient in terms of involved calculation.

Moving a bit far, we consider a different problem. Let G be a finite group, let H be a subgroup of G, and let $\mathcal{O}_G(H) := \{K \mid K \text{ subgroup of } G \text{ with } H \leq K\}$ be the set of subgroups of G containing H. This is called the *overgroup lattice* of H in G. Detailed information on the overgroups of a primitive subgroups of G was obtained independently by Aschbacher [5, 6] and Liebeck, Praeger and Saxl [93, 140].

The problem of determining whether every finite lattice is isomorphic to some $\mathcal{O}_G(H)$ for a finite group G arose originally in universal algebra with the work of Pálfy-Pudlák [132]. In 1938, Ore proved that for a finite group G and a subgroup H of G such that the overgroup lattice $\mathcal{O}_G(H)$ is distributive, then there exists a coset Hg generating G [127, Theorem 7]. In [130], Palcoux obtained a dual version of Ore's theorem. More precisely he proved that if $\mathcal{O}_G(H)$ is distributive, then there exists an irreducible complex representation V of G such that $G_{(V^H)} = H$ (where V^H is the H-fixed points subspace of V). In [131] it was proved that for any subgroup $H \subset G$, if the *dual Euler totient*

$$\hat{\varphi}(H, G) := \sum_{K \in \mathcal{O}_G(H)} \mu(H, K)|G : K|,$$

is nonzero, then there is an irreducible complex representation V such that $G_{(V^H)} = H$. So the dual Ore's theorem appears as a natural consequence of the following conjecture.

Conjecture 3. [13, Conjecture 1.5] *If $\mathcal{O}_G(H)$ is Boolean, then $\hat{\varphi}(H, G)$ is nonzero.*

A first step to attack Conjecture 3 could be to prove the case where G is a finite simple group, hence as a preliminary aim one should try to classify the inclusions $H \subset G$ when G is finite simple group and $\mathcal{O}_G(H)$ Boolean. We briefly say what was known in this direction until some moths ago. In [13, Example 4.21] it is noticed that if H is the Borel subgroup of a BN-pair structure (of rank ℓ) on G, then $\mathcal{O}_G(H)$ is Boolean (of rank ℓ). Moreover if G is a finite simple group of Lie type (over a finite field of characteristic p) then its absolute value

$\hat{\varphi}(H,G)$ is the p-contribution in the order of G, which is at least $p^{\frac{1}{2}\ell(\ell+1)}$. Finally, Shareshian suggested examples of boolean $\mathcal{O}_G(H)$ of any rank when G is the alternating group, involving stabilizers of non-trivial regular partitions, as shown in [8] for the rank 2.

In Chapter 3 we discuss some recent results in the theory of permutation groups regarding the themes briefly introduced above and based on joint works with A. Lucchini, P. Spiga, S. Palcoaux, and C. M. Roney-Dougal [112, 111, 122]. Precisely, this chapter is organized as follows.

Section 3.1 [122] In this Section we prove that if G is primitive and not large base, then $b(G) \leq \max\{7, \lceil \log n \rceil + 1\}$. Furthermore, we show that there are infinitely many primitive groups G that are not large base for which $b(G) > \log n + 1$, so our bound is optimal.

Section 3.2 [112] In this section we show that there exists a constant a such that, for every subgroup H of a finite group G, the number of maximal subgroups of G containing H is bounded above by $a|G:H|^{3/2}$. In particular, a transitive permutation group of degree n has at most $an^{3/2}$ maximal systems of imprimitivity. When G is soluble we prove a much stronger bound, that is, the number of maximal subgroups of G containing H is at most $|G:H|-1$.

Section 3.3 [111] This Section provides a classification of the subgroups H of G such that $\mathcal{O}_G(H)$ is Boolean of rank at least 3, when G is a finite alternating or symmetric group. We proved that, besides some sporadic examples and some twisted versions, there are two different types of such lattices. One type arises by taking stabilizers of chains of regular partitions, and the other type arises by taking stabilizers of chains of regular product structures. As an application, we prove in this case Conjecture 3 related to the dual Ore's theorem above mentioned.

Asymptotic enumeration of Cayley graphs

A graph Γ is an ordered pair (V,E) with V a finite non-empty set of vertices, and E a set of unordered pairs from V, representing the edges. An automorphism of a graph is a permutation on V that preserves the set E. Let R be a group and let S be an inverse-closed subset of R. The Cayley graph $\Gamma(R,S)$ with connection set S, is the graph with $V=R$ and $\{r,t\} \in E$ if and only if $tr^{-1} \in S$. When $\Gamma(R,S)$ is a Cayley graph, the group R acts regularly on the vertices as a group of graph automorphisms. A graphical regular representations, GRR for short, for R is therefore a Cayley graph on R that admits no other automorphisms. The problem of finding graphical regular representations (GRRs) for groups has a long history. Mathematicians have studied graphs with specified automorphism groups at least as far back as the 1930s, and in the 1970s there were many papers devoted to the topic of finding GRRs. The main thrust of much of the work through the 1970s was to determine which groups admit GRRs. This question was ultimately answered by Godsil. He showed that, except 13 small groups, a group has graphical regular representation if and only if it is neither a generalised dicyclic group nor an abelian group of exponent greater than 2. A corresponding result for digraphical regular representation (DRR) by Babai was much simpler, requiring no excluded families and finding only 5 exceptional small groups. Babai and Godsil conjectured that, if R is not generalised dicyclic nor abelian of exponent greater than 2, then for almost all inverse-closed subsets S of R, $\Gamma(R,S)$ is a GRR. In this Chapter, we investigate the following more specific formulation of the Babai and Godsil conjecture:

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : S = S^{-1},\ \mathrm{Aut}(\Gamma(R,S)) = R\}|}{2^{\mathbf{c}(R)}} : R \text{ admits a GRR and } |R| = r \right\} = 1,$$

where $2^{\mathbf{c}(R)}$ is the number of inverse-closed subsets of R. The corresponding result for Cayley digraphs (which does not require any families of groups to be excluded) was proved by Morris and Spiga in [120]. The strategy used in [120] to prove that almost every Cayley digraph is a DRR, involved three major pieces. Similarly to the results about existence of GRRs and DRRs, the requirement that a connection set for a graph must be inverse-closed creates complications that make the proof of the Babai-Godsil conjecture more difficult for graphs than for digraphs. Hence it makes sense to divide the proof of the Babai-Godsil conjecture for graph into the main pieces that were used to prove the DRR result, and attempt to show each of these pieces for GRRs. The first piece of the proof of the Babai-Godsil conjecture for graphs, showing that there are not many Cayley graphs admitting graph automorphisms that are also group automorphisms (unless the group is generalised dicyclic or abelian of exponent greater than 2) was accomplished by Spiga in [154]. In this Chapter, based on joint work with J. Morris and P. Spiga [119], we try to accomplish the second pieces of the proof, that is we show that the number of Cayley graphs on R that admit nontrivial graph automorphisms that fix the vertex 1 and normalise some proper nontrivial normal subgroup N of R, is vanishingly small as a proportion of all Cayley graphs on R.

As in the work on DRRs, this problem naturally divides into the cases where the normal subgroup N is "large" or "small" relative to $|R|$. Furthermore in the case of graphs, it emerges that we also need to consider separately graph automorphisms that fix or invert every element of the group. This chapter is organized as follows.

Section 4.1 In this section we deal with graph automorphisms that fix or invert every element of the group. This piece of our work applies whether or not R admits any proper nontrivial normal subgroup.

Section 4.2 In this Section we prove that if R is a finite group and N is a non-identity proper normal subgroup of R, then

$$|\{S \subseteq R \mid S = S^{-1},\, R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R),\, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1\}| \leq 2^{\mathbf{c}(R) - \frac{|N|}{96} + 2\log_2|R| + (\log_2|R|)^2 + 3}.$$

Moreover, if R is neither abelian of exponent greater than 2 nor generalised dicyclic, we may drop the condition "$R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$" in the definition of the set.

Section 4.3 In this Section we show that if R is a finite group and N is a non-identity proper normal subgroup of R, then

$$|\{S \subseteq R \mid S = S^{-1},\, R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R),\, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1, f \text{ fixes each } N\text{-orbit setwise}\}| \leq 2^{\mathbf{c}(R) - \frac{|R|}{192|N|} + (\log_2|R|)^2 + 3}.$$

Moreover, if R is neither abelian of exponent greater than 2 nor generalised dicyclic, we may drop the condition "$R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$" in the definition of the set.

Contents

Chapter 1

Preliminaries

1.1 Group action

The definitions and results in this section are well known and we refer to [32], [48] as main references. Let G be a group, and suppose that G acts on a set Ω. We will always assume that Ω is finite, and we say that the degree of G is the size of Ω. Unless otherwise specified we normally write ωg or ω^g for the image of $\omega \in \Omega$ under $g \in G$. The *stabiliser* of $\omega \in \Omega$, denoted by G_ω is the subgroup of G consisting of those elements that fix ω. The orbit of $\omega \in \Omega$ is $\omega^G := \{\omega^g \mid g \in G\}$. Then the orbit-stabiliser theorem asserts that, for a finite group G, $|G| = |G_\omega||\omega^G|$ for all $\omega \in \Omega$. The action of G is *transitive* if for every $\omega_1, \omega_2 \in \Omega$ there exists $g \in G$ for which $\omega_1^g = \omega_2$, that is $\omega^G = \Omega$ for any $\omega \in \Omega$. If there exists $\omega \in \Omega$ such that $G_\omega = 1$, then ω^G is a *regular orbit* of G. When this occurs, by the orbit-stabiliser theorem $|G| = |\omega^G|$. The action is *faithful* if the identity of G is the only element of G fixing every element of Ω. The group G is a *permutation group* on Ω if G acts faithfully on Ω.

The *setwise stabiliser* of $\Gamma \subseteq \Omega$, denoted by G_Γ is the subgroup of G consisting of the elements $g \in G$ for which $\Gamma^g = \Gamma$ where $\Gamma^g := \{\gamma^g \mid \gamma \in \Gamma\}$. The *pointwise stabiliser* of $\Gamma \subseteq \Omega$, denoted by $G_{(\Gamma)}$ is the subgroup of G consisting of the elements $g \in G$ for which $\gamma^g = \gamma$ for any $\gamma \in \Gamma$. The set of fixed points in Ω of $g \in G$ is denoted by $\mathrm{fix}_\Omega(g)$. A permutation with no fixed points is *fixed-point-free*. The permutation groups $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\Gamma)$ are *permutation isomorphic* if there exist an isomorphism $\psi : G \to H$ and a bijection $\varphi : \Omega \to \Gamma$ such that $(\omega^g)^\varphi = (\omega^\varphi)^{(g^\psi)}$ for all $\omega \in \Omega$ and $g \in G$. If H is a subgroup of G, then we denote the left coset space by $G \setminus H$. Then a transitive action of G on Ω is permutation isomorphic to the action of G by left multiplication on $G \setminus G_\omega$ for any $\omega \in \Omega$.

Let G be a transitive permutation group on Ω. A non-empty subset B of Ω is a *block of imprimitivity* if, for every $g \in G$, either $B \cap B^g = \varnothing$ or $B = B^g$. Each translate B^g is also a block, and we say that $\{B^g \mid g \in G\}$ is a *block system* or a *system of imprimitivity* (this is a partition of Ω). The singleton $\{\omega\} \subseteq \Omega$, and the whole Ω are blocks of imprimitivity; these are called *trivial blocks*, and any other block is *nontrivial*. The group $G \leq \mathrm{Sym}(\Omega)$ is *imprimitive* if admits a nontrivial block of imprimitivity on Ω. Accordingly, G is primitive if it admits only the trivial blocks. The notion of primitivity in permutation group theory has a correspondence with abstract group theory. The relation arises from the following easy result.

Proposition 1.1.1. *Let G be a transitive group on Ω. Then, G is primitive if and only if G_ω is a maximal subgroup for some $\omega \in \Omega$.*

Let $G \leq \mathrm{Sym}(\Omega)$ be an imprimitive permutation group. Let $\Sigma = \{B^g \mid g \in G\}$ be a system of imprimitivity. Note that G acts transitively on Σ, that is, the induced permutation group $G^\Sigma \leq \mathrm{Sym}(\Sigma)$ is transitive. The system of imprimitivity Σ is *maximal* if G^Σ is primitive.

1.2 Crowns

The concept of a crown was introduced by Gaschütz in [56] for finite soluble groups, where he analyses the structure of the chief factors of a soluble group G as G-modules. Later this notion has been generalized to all finite groups (see for example [74], [84], and [43]).

In this section we start setting some notation by reviewing some basic results on G-groups, on monolithic primitive groups and on crowns. For the first part we follow [43], for the second part we follow [74] and for the third part we follow [11, Chapter 1] and [43].

Given a group G and a subgroup M we denote by

$$\mathrm{core}_G(M) = M_G := \bigcap_{g \in G} M^g$$

the *core* of M in G.

An *abstract* group L is said to be *primitive* if it has a maximal subgroup with trivial core. Note that this definition for primitivity is equivalent to that given in the previous section. The *socle* (that is, the subgroup generated by the minimal normal subgroups) of a primitive group L, $\mathrm{soc}(L)$, is either a minimal normal subgroup, or the direct product of two non-abelian minimal normal subgroups. A primitive group L is said to be *monolithic* if the first case occurs, that is, $\mathrm{soc}(L)$ is a minimal normal subgroup of L and hence (necessarily) L has a unique minimal normal subgroup. The primitive group L is of *type I* (respectively *type II*) if it is monolithic and $\mathrm{soc}(L)$ is abelian (respectively non-abelian). Whilst L is of *type III* if $\mathrm{soc}(L)$ is direct product of two non-abelian minimal normal subgroups.

Let L be a monolithic primitive group and let $A := \mathrm{soc}(L)$. For each positive integer k, let L^k be the k-fold direct product of L. The *crown-based power* of L of size k is the subgroup L_k of L^k defined by

$$L_k := \{(l_1, \dots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \pmod{A}\}.$$

Equivalently, if we denote by $\mathrm{diag}(L^k)$ the diagonal subgroup of L^k, then $L_k = A^k \mathrm{diag}(L^k)$.

Lemma 1.2.1. *Let M be a normal subgroup of a crown-based power L_k with socle N^k. Then either $M \leq N^k$ or $N^k \leq M$.*

Proof. For each $i \in \{1, \dots, k\}$, we write $N_i := \{(n_1, \dots, n_k) \in N^k \mid n_j = 1, \forall j \in \{1, \dots, k\} \setminus \{i\}\}$. In particular, $N = N_1 \times \cdots \times N_k$.

Let M be a normal subgroup of the crown based power L_k with socle N^k and with $M \not\leq N^k$. Let $m \in M \setminus N^k$. For each $i \in \{1, \dots, k\}$, since M does not centralize N_i, we deduce $1 \neq [M, N_i] \leq M \cap N_i$. As N_i is one of the minimal normal subgroups of L_k, we must have $N_i \leq M$. Therefore, $N^k = N_1 \times \cdots \times N_k \leq M$. □

Given a group G, a *G-group* is a group A together with a group homomorphism $\theta : G \to \mathrm{Aut}(A)$. If no ambiguity is possible, for simplicity, we write a^g for the image of $a \in A$ under the automorphism $\theta(g)$. Given a G-group A, we have the corresponding *semi-direct product* $A \rtimes_\theta G$ (or simply $A \rtimes G$ when θ is clear from the context), where the multiplication is given by

$$g_1 a_1 \cdot g_2 a_2 = g_1 g_2 a_1^{g_2} a_2,$$

for every $a_1, a_2 \in A$ and for every $g_1, g_2 \in G$. A G-group A is said to be *irreducible* if G leaves invariant no non-identity proper normal subgroup of A.

Two G-groups A and B are said to be *G-isomorphic*, and we write $A \cong_G B$, if there exists an isomorphism $\varphi : A \to B$ such that

$$(a^g)^\varphi = (a^\varphi)^g,$$

for every $a \in A$ and for every $g \in G$. Similarly, we say that A and B are *G-equivalent* ,and we write $A \sim_G B$, if there exist two isomorphisms $\varphi : A \to B$ and $\Phi : A \rtimes G \to B \rtimes G$ such that the following diagram commutes.

$$\begin{array}{ccccccccc} 1 & \hookrightarrow & A & \hookrightarrow & A \rtimes G & \twoheadrightarrow & G & \to & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \hookrightarrow & B & \hookrightarrow & B \rtimes G & \twoheadrightarrow & G & \to & 1 \end{array}$$

Being "G-equivalent" is an equivalence relation among G-groups coarser than the "G-isomorphic" equivalence relation, that is, two G-isomorphic G-groups are necessarily G-equivalent. (Indeed, if A and B are G-isomorphic via $\varphi : A \to B$, then they are G-equivalent via $\Phi : A \rtimes G \to B \rtimes G$ defined by $(ag)^\Phi := a^\varphi g$.)

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

Lemma 1.2.2. *Let A, B be two G-groups. They are G-equivalent if and only if there exists a 1-cocycle $\beta \in Z^1(G, B)$ such that $A \cong_G B_\beta$.*

Proof. If $A \sim_G B$ via $\varphi : A \to B$ and $\Phi : A \rtimes G \to B \rtimes G$, we define $\beta \in Z^1(G, B)$ by $g^\beta := g^{-1} g^\Phi$. Conversely, if $\beta \in Z^1(G, B)$ via $\varphi : A \to B_\beta$, we define Φ by setting $(ag)^\Phi = a^\varphi g g^\beta$. □

If A is a G-group denote by $C_G(A)$ the centralizer of A in G, that is

$$C_G(A) := \{g \in G \mid a^g = a \,, \forall a \in A\}.$$

Note for A, B two G-isomorphic groups then $C_G(A) = C_G(B)$.

Let $A = B$ be a non-abelian simple groups, and let $G := A \times B$ acts on $A \times \{1\}$ and on $\{1\} \times B$ by conjugation. Then $C_G(A \times \{1\}) = \{1\} \times B$, and $C_G(\{1\} \times B) = A \times \{1\}$, in particular $A \times \{1\} \ncong \{1\} \times B$ are not G-isomorphic. But defiyning

$$\begin{array}{ll} \varphi : A \times \{1\} \to \{1\} \times B, & (a, 1) \mapsto (1, a) \\ \Phi : (A \times \{1\}) \rtimes G \to (\{1\} \times B) \rtimes G & (a, 1)(x, y) \mapsto (x, y)(1, y^{-1} x a) \\ \beta : G \to \{1\} \times B, & (x, y) \mapsto (1, y^{-1} x) \end{array}$$

we get that $\beta \in Z^1(G, \{1\} \times B)$, and so $A \times \{1\} \cong_G (\{1\} \times B)_\beta$. That is, $A \times \{1\} \sim_G \{1\} \times B$.

Let G be a group and let $A := X/Y$ be a chief factor of G, where X and Y are normal subgroups of G. Clearly, the action by conjugation of G endows A with the structure of G-group and, in fact, A is an irreducible G-group. On the set of chief factors, the G-equivalence relation is easily described. Indeed, it is proved in [74, Proposition 1.4] that two chief factors A and B of G are G-equivalent if and only if either

- A and B are G-isomorphic, or
- there exists a maximal subgroup M of G such that $G/\mathrm{core}_G(M)$ has two minimal normal subgroups N_1 and N_2 G-isomorphic to A and B respectively.

(The example in the previous paragraph witnesses that the second possibility does arise.) From this, it follows that, for every monolithic primitive group L and for every $k \in \mathbb{N}$, the minimal normal subgroups of the crown-based power L_k are all L_k-equivalent.

Let X and Y be normal subgroups of G with $A = X/Y$ a chief factor of G. Recall that a *complement* U to A in G is a subgroup U of G such that

$$G = UX \text{ and } Y = U \cap X.$$

Further, recall that $A = X/Y$ is a *Frattini chief factor* if X/Y is contained in the Frattini subgroup of G/Y; this is equivalent to saying that A is abelian and there is no complement to A in G. The number $\delta_G(A)$ of non-Frattini chief factors G-equivalent to A in any chief series of G does not depend on the series and hence $\delta_G(A)$ is a well-defined integer depending only on the chief factor A.

We denote by L_A the *monolithic primitive group associated* to A, that is,

$$L_A := \begin{cases} A \rtimes (G/C_G(A)) & \text{if } A \text{ is abelian,} \\ G/C_G(A) & \text{otherwise.} \end{cases}$$

If A is a non-Frattini chief factor of G, then L_A is a homomorphic image of G. More precisely, there exists a normal subgroup N of G such that

$$G/N \cong L_A \text{ and } \operatorname{soc}(G/N) \sim_G A.$$

Consider now the collection $\mathcal{N}_A$ of all normal subgroups N of G with $G/N \cong L_A$ and $\operatorname{soc}(G/N) \sim_G A$: the intersection

$$R_G(A) := \bigcap_{N \in \mathcal{N}_A} N$$

has the property that $G/R_G(A)$ is isomorphic to the crown-based power $(L_A)_{\delta_G(A)}$, that is, $G/R_G(A) \cong (L_A)_{\delta_G(A)}$.

The socle $I_G(A)/R_G(A)$ of $G/R_G(A)$ is called the *A-crown* of G and it is a direct product of $\delta_G(A)$ minimal normal subgroups all G-equivalent to A (where we set $\delta_G(A) = 0$ when $R_G(A) = I_G(A)$). If $\delta_G(A) \geq 2$ then any two different minimal normal subgroups of $G/R_G(A)$ have a common complement, which is a maximal subgroup of $G/R_G(A)$. Every chief series of G contains exactly $\delta_G(A)$ non-Frattini chief factors G-equivalent to A. In particular, in a chief series passing through $R_G(A)$ and $I_G(A)$, the unique non-Frattini chief factors G-equivalent to A are those between $R_G(A)$ and $I_G(A)$. If H/K is a non-Frattini chief factor of G then $H/K \sim_G A$ if and only if $KR_G(A) \leq HR_G(A) \leq I_G(A)$.

We conclude this preliminary section with some technical lemmas.

Lemma 1.2.3. [11, Lemma 1.3.6] *Let G be a finite group with trivial Frattini subgroup. There exists a chief factor A of G and a non-identity normal subgroup D of G with $I_G(A) = R_G(A) \times D$.*

Lemma 1.2.4. [43, Proposition 11] *Let G be a finite group with trivial Frattini subgroup, let $I_G(A), R_G(A)$ and D be as in the statement of Lemma 1.2.3 and let K be a subgroup of G. If $G = KD = KR_G(A)$, then $G = K$.*

Note that

$$I_G(A) := \{g \in G \mid g \text{ induces an inner automorphism in } A\},$$

and for $A = X/Y$, we get that $I_G(A) = XC_G(A)$. In particular, when A is abelian, then $I_G(A) = C_G(A)$. Now, the following corollary is immediate.

Corollary 1.2.5. *Let G be a finite soluble group with trivial Frattini subgroup. There exists a crown $C_G(A)/R_G(A)$ and a non-identity normal subgroup D of G such that $C_G(A) = R_G(A) \times D$. Moreover, when $K \leq G$ is such that $G = KD = KR_G(A)$, then $G = K$.*

Lemma 1.2.6. *If G is not nilpotent, then we can assume that the irreducible G-module A in the statement of Corollary 1.2.5 is a non-trivial G-module.*

Proof. Let U be a trivial G-module. Since $\operatorname{Frat} G = 1$, U has a complement, say H, in G. Since the action of G on U is trivial, then $G = H \times U$. Now, there exists a crown $C_H(B)/R_H(B)$ and a non trivial normal subgroup W of H such that $C_H(B) = R_H(B) \times W$. However we have $C_G(B) = C_H(B) \times U$ and $R_G(B) = R_H(B) \times U$, hence $C_G(B) = R_G(B) \times W$. This means that we may consider B in place of U. It is possible that also B is a trivial G-module. In that case we can take a complement K of $U \times W$ in G and repeat the previous argument. Continuing in this way, either G is abelian or we obtain a non-trivial irreducible G-module satisfying our statement of G. □

1.3 Zsigmondy primes

We state some useful results on the primitive prime divisors.

Definition 1.3.1. Let a and n be positive integers. A prime number p is called a *primitive prime divisor* of $a^n - 1$ if p divides $a^n - 1$ and p does not divide $a^e - 1$ for every integer $1 \leq e \leq n - 1$. We denote an arbitrary primitive prime divisors of $a^n - 1$ by a_n.

Theorem 1.3.2 (Zsigmondy's Theorem [164])**.** *Let a and n be integers bigger than 1. There exists a primitive prime divisor of $a^n - 1$ except in one of the following cases:*

1. *$n = 2$, $a = 2^s - 1$ (i.e. a is a Mersenne prime), and $s \geq 2$.*
2. *$n = 6$, $a = 2$.*

Lemma 1.3.3. [80, Proposition 5.2.15] $a_n \equiv 1 \mod n$.

1.4 Finite simple groups

The classification of finite simple groups is as follows, and for this we refer to [40].

Theorem 1.4.1. *A finite simple group is isomorphic to one of the following.*

1. *A cyclic group C_p of prime order.*
2. *An alternating group $\mathrm{Alt}(n)$ of degree n at least 5.*
3. *A simple group of Lie type.*
4. *One of 26 sporadic simple groups.*

The proof of this is spread throughout hundreds of papers. We shall use this result throughout this thesis, and CFSG will mean "Classification of the Finite Simple Groups".

1.5 The O'Nan-Scott Theorem

The modern key for analysing a finite primitive permutation group L is to study the *socle* N of L. The socle of an arbitrary finite group is isomorphic to the non-trivial direct product of simple groups; moreover, for finite primitive groups these simple groups are pairwise isomorphic. The O'Nan-Scott theorem describes in details the embedding of N in L and collects some useful information about the action of L. This theorem was stated independently by O'Nan and Scott in the preliminary proceedings of the Santa Cruz Conference on Finite Groups in 1979. Only Scott's version made it into the final Proceedings [151]. Later, Aschbacher pointed out the existence of another class of groups erroneously excluded in the original version of the O'Nan-Scott Theorem. In [92], Liebeck, Praeger and Saxl gave a self-contained proof, precisely five types of primitive groups are defined (depending on the group-

Table 1.1: The primitive permutation groups.

Type		Description
I	(HA)	Affine-type: $G = V \rtimes G_0 \leq AGL(V)$, $G_0 \leq GL(V)$ irreducible
II	(AS)	Almost simple: $T \leq G \leq \mathrm{Aut}(T)$
III(a)(i)	(SD)	Diagonal-type: $T^k \leq G \leq T^k.(\mathrm{Out}(T) \times P), P \leq \mathrm{Sym}(k)$ primitive
III(a)(ii)	(HS)	Diagonal-type: $T^2 \leq G \leq T^2.\mathrm{Out}(T)$
III(b)(i)	(PA)	Product-type: $G \leq H\mathrm{wr}P$, H primitive of type II, $P \leq \mathrm{Sym}(k)$ transitive
III(b)(ii)	(CD)	Product-type: $G \leq H\mathrm{wr}P$, H primitive of type III(a)(i), $P \leq \mathrm{Sym}(k)$ transitive
III(b)(iii)	(HC)	Product-type: $G \leq H\mathrm{wr}P$, H primitive of type III(a)(ii), $P \leq \mathrm{Sym}(k)$ transitive
III(c)	(TW)	Twisted wreath product

and action-structure of the socle), namely the *Affine-type* (HA), the *Almost Simple* (AS), the *Diagonal-type*, the *Product-type*, and the *Twisted Wreath product*, and it is shown that every primitive group belongs to exactly one of these types.

In [140] this division into types is refined further, namely the Diagonal-type is partitioned in *Holomorphic simple* (HS), and *Simple Diagonal* (SD), and the Product-type is partitioned into *Holomorphic compound* (HC), *Compound Diagonal* (CD), and *Product action* (PA).

Table 1.1 providing a rough description of the families of primitive groups that arise. In Table 1.1, V is a vector space over a field $\mathbb{F}_p$ of prime order, T denotes a nonabelian simple group, and T^k is the direct product of k copies of T.

In what follows, when we refer to the O'Nan and Scott theorem, we will explicitly state if we use the version presented in [92] or that in [140] depending on the occurrence.

Chapter 2

Generation of groups

From now on, if we do not say differently, G will be a finite group. We say that a subset X of G *is a generating set* for G if every element of G can be express as a product of elements of $X \cup X^{-1}$. In this case, we write $G = \langle X \rangle$, or $G = \langle x_1, \ldots, x_t \rangle$ when $X = \{x_1, \ldots, x_t\}$. The elements of X are called *generators* of G, and we used to say that G *is generated by* X or that X *generates* G. A group is said *finitely generated* if there exists a finite set that generates it. Evidently, a finite group is finitely generated. Let

$$d(G) := \min\{|S| \mid G = \langle S \rangle\}$$

be the minimal number of generators for G. We will say that G is *d-generated* if $d(G)$ is at most d.

The invariant $d(G)$ has been deeply studied for many groups G. Gaschütz [55] gave a formula to compute the minimal number of generators of a finite soluble group in terms of certain 'local' and 'global' parameters associated to a chief series of the group. On the other side, it follows from the CFSG that every finite simple group can be generated by just two of its elements ([156], [7]). For example, it is easy to show that

$$\mathrm{Alt}(n) = \begin{cases} \langle (1,2,3), (1,2,\ldots,n) \rangle & \text{if } n \text{ is even} \\ \langle (1,2,3), (2,3,\ldots,n) \rangle & \text{if } n \text{ is odd.} \end{cases}$$

For a finite group G, and a positive integer k, we define

$$P_G(k) = \frac{|\{(g_1, \ldots, g_k) \in G^k \mid \langle g_1, \ldots, g_k \rangle = G\}|}{|G|^k}$$

to be the probability that k randomly chosen elements of G generate G. Since every finite simple group is 2-generated, then $P_G(2) > 0$ for all finite simple groups G. So, arises naturally the idea to investigate the asymptotic behavior of $P_G(2)$ with respect to $|G|$. The problem has a very early origin. Indeed, in 1882, Netto conjectured that almost all pairs of elements of $\mathrm{Alt}(n)$ generate the whole group (see [123, page 90]). In probabilistic terms, Netto's conjecture can be states as: $P_{\mathrm{Alt}(n)}(2) \to 1$ as $n \to \infty$. This conjecture was proved by Dixon [47] in 1967. In fact, Dixon proved more, showing that $P_{\mathrm{Alt}(n)}(2) > 1 - \frac{8}{(\log_e \log_e n)^2}$ for sufficiently large n. In the same paper, Dixon conjectured that all finite simple groups are strongly 2-generated in the sense of Netto. In other words, he conjetured that for every finite simple group G, then $P_G(2) \to 1$ as $|G| \to \infty$. The conjecture was proved for classical groups by Kantor and Lubotzky in [77], and for exceptional groups of Lie type by Liebeck and Shalev in [91]. The proof is based on the following observation.

Lemma 2.0.1. *Let G be a finite group, and let $m_n(G)$ be the number of index n maximal subgroups of G. Then*

$$1 - P_G(k) \leq \sum_{n \geq 2} \frac{m_n(G)}{n^k}. \tag{2.0.1}$$

Proof. Observe that if $x_1, \ldots, x_k$ do not generate G, then they lie in a maximal subgroup M of G. Given M, the probability that this happens (for random $x_1, \ldots, x_k$) is $\frac{|M|^k}{|G|^k} = \frac{1}{|G:M|^k}$. Hence

$$1 - P_G(k) \leq \sum_{\substack{M < G \\ max}} \frac{1}{|G:M|^k} = \sum_{n \geq 2} \frac{m_n(G)}{n^k}.$$

□

Now, studying the maximal subgroups of a finite simple group of Lie type G, by using powerful results on the subgroup structure of these groups, such as Aschbacher's theorem [4] for classical groups, one can show that $1 - P_G(2)$ tends to 0 as $|G|$ tends to infinity. Therefore $P_G(2) \to 1$ as $|G| \to \infty$ and Dixon's conjecture follows.

This probabilistic argument shows that every sufficiently large finite simple group of Lie type is 2-generated, without explicitly construct a pair of generators. This highlights that, in the context of generation of groups, a central role is played by probabilistic methods. Let us introduce more precisely the general setting.

Let G be a nontrivial finite group and let $x = (x_n)_{n \in \mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables. We may define a random variable τ_G by

$$\tau_G := \min\{n \geq 1 \mid \langle x_1, \ldots, x_n \rangle = G\}.$$

We denote by $e(G)$ the expectation $\mathrm{E}(\tau_G)$ of this random variable. Hence, $e(G)$ is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. Clearly $\tau_G > n$ if and only if $\langle x_1, \ldots, x_n \rangle$ is a proper subgroup of G. Hence we get that

$$P(\tau_G > n) = 1 - P_G(n). \tag{2.0.2}$$

Therefore,

$$\begin{aligned} e(G) &= \sum_{n \geq 1} n P_G(\tau_G = n) = \sum_{n \geq 1} \left(\sum_{m \geq n} P_G(\tau_G = m) \right) \\ &= \sum_{n \geq 1} P_G(\tau_G \geq n) = \sum_{n \geq 0} P_G(\tau_G > n) = \sum_{n \geq 0} (1 - P_G(n)). \end{aligned} \tag{2.0.3}$$

Let us consider some examples. Let $G = C_p$ is a cyclic group of prime order p, then τ_G is a geometric random variable with parameter $\frac{p-1}{p}$, so $e(C_p) = \frac{p}{p-1}$. If $G = D_{2p}$ is the dihedral group of order $2p$, with p an odd prime: then $\langle g_1, \ldots, g_k \rangle = G$ if and only if there exist $1 \leq i < j \leq n$ such that $g_i \neq 1$ and $g_j \notin \langle g_i \rangle$. We may think that we are repeating independent trials (choices of an element from G in a uniform way). The number of trials needed to obtain a nontrivial element x of G is a geometric random variable with parameter $\frac{2p-1}{2p}$: its expectation is equal to $E_0 = \frac{2p-1}{2p}$. With probability $p_1 = \frac{p}{2p-1}$, the nontrivial element x has order 2: in this case the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-2}{2p}$ and expectation $E_1 = \frac{2p}{2p-2}$. On the other hand, with probability $p_2 = \frac{p-1}{2p-1}$, the nontrivial element x has order p: here, the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with parameter $\frac{2p-p}{2p}$ and expectation $E_2 = \frac{2p}{2p-p}$. This implies

$$e(D_{2p}) = E_0 + p_1 E_1 + p_2 E_2 = 2 + \frac{2p^2}{(2p-1)(2p-2)}.$$

It appears evident from the second example that, when we consider a group G with a richer subgroup structure, the computation of $e(G)$ became more complicated. When the subgroup structure of G is clear, the results proved in [64] and [103] became very appealing. Indeed, in [64], respectively in [103] it was showed that $P_G(t)$, respectively $e(G)$ can be computed only by using knowledge about the subgroup structure of the group G. More precisely, defining the *Möbius function on the subgroup lattice of* G by setting

$$\mu_G(G) = 1 \text{ and } \mu_G(H) = -\sum_{H<K\leq G} \mu_G(K), \ \forall H < G,$$

then

$$P_G(t) = \sum_{H\leq G} \frac{\mu_G(H)}{|G:H|^t}, \tag{2.0.4}$$

$$e(G) = -\sum_{H<G} \frac{\mu_G(H)|G|}{|G|-|H|}. \tag{2.0.5}$$

Here, arises naturally to asks how $d(G)$ and $e(G)$ are related. Surely $d(G) \leq e(G)$. But, more in general, what we can say about $e(G) - d(G)$? Pomerance [137] studied the question for the abelian groups. He showed that if G is an abelian group, then $e(G) \leq d(G) + \sigma$ where the constant $\sigma \sim 2.1185$ is explicitly described in terms of the Riemann zeta function and is the best possible. Since $e(G) = e\left(G/\operatorname{Frat}(G)\right)$ and, when G is a nilpotent group, $G/\operatorname{Frat}(G)$ is abelian, then the Pomerance's result is true also for finite nilpotent group. Whilst Kantor and Lubotzky proved that $e(G) - d(G)$ is unbounded in general. Indeed, in [77], they showed that for every positive real number ϵ and every positive integer k there exists a 2-generated finite group $G_{\epsilon,k}$ with $P_{G_{\epsilon,k}}(t) \leq \epsilon$ for every $t \leq k$. Hence, by (2.0.3),

$$e(G_{\epsilon,k}) \geq \sum_{0\leq t\leq k} (1 - P_{G_{\epsilon,k}}(t)) \geq (k+1)(1-\epsilon),$$

and consequently

$$e(G_{\epsilon,k}) - d(G_{\epsilon,k}) \geq (k+1)(1-\epsilon) - 2.$$

Others key estimation on $e(G)$ can be found in [44] and [96].

At this point, we investigate how some hypotheses on the number of generators of subgroups of a specific family of subgroups of G impact on $e(G)$. One of the first step towards this investigation was to prove a probabilistic version of the following theorem, independently proved by Guralnick [60] and Lucchini [100] in 1989.

Theorem 2.0.2. *Let G be a finite group with all the Sylow subgroups d-generated. Then $d(G) \leq d + 1$.*

Precisely we proved the following theorem which improves a result in [99].

Theorem 2.0.3. [109, Theorem 1.1] *Let G be a finite group. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + \kappa$ where κ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context. Approximately, κ equals 2.752394.*

This bound can be further improved under some additional assumptions on G. For example, we proved that if all the Sylow subgroups of G can be generated by d elements and G is not soluble, then $e(G) \leq d + 2.750065$ (Proposition 2.1.7). A stronger result holds if $|G|$ is odd.

Theorem 2.0.4. [109, Theorem 1.2] *Let G be a finite group of odd order. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq d + \tilde{\kappa}$ with $\tilde{\kappa} \sim 2.148668$.*

In this case the constant $\tilde{\kappa}$ is probably not best possible. In particular, a precise estimation would require a complete knowledge of the distribution of the Fermat primes.

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements (see [83]), so Theorem 2.0.3 has the following consequence: if G is a permutation group of degree n, then $e(G) \leq \lfloor n/2 \rfloor + \kappa$. However this bound is not best possible and a better result can be obtained.

Theorem 2.0.5. [109, Corollary 1.3] *If G is a permutation group of degree n, then either $G = \mathrm{Sym}(3)$ and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \kappa^*$ with $\kappa^* \sim 1.606695$.*

The number κ^* is best possible. Let $m = \lfloor n/2 \rfloor$ and set $G_n = \mathrm{Sym}(2)^m$ if m is even, $G_n = \mathrm{Sym}(2)^{m-1} \times \mathrm{Sym}(3)$ if m is odd. If $n \geq 8$, then $e(G_n) - m$ increases with n and $\lim_{n\to\infty} e(G) - m = \kappa^*$.

We discuss the details of the proofs of Theorems 2.0.3, 2.0.4, 2.0.5 in Section 2.1.

In 1991, Kovács and Sim proved that if a finite soluble group G has a family of d-generator subgroups whose indices have no common divisor, then G can be generated by $d+1$ elements (see [82, Theorem 2]). The hypotheses on the family on d-generated subgroups is coarser than that in Theorem 2.0.2. So, motivated by the result in Theorem 2.0.3, we searched for a probabilistic version of the result of Kovács and Sim mentioned above. In order to move in this direction let consider the following invariant, introduced by Pak:

$$\nu(G) = \min\left\{ k \in \mathbb{N} \;\middle|\; P_G(k) \geq \frac{1}{e} \right\},$$

where e is the Nepero number. As it was noticed by Pak (see for example [96, Proposition 1.1]), $e(G)$ and $\nu(G)$ are related in the following way:

$$\frac{1}{e} \cdot e(G) \leq \nu(G) \leq \frac{e}{e-1} \cdot e(G). \tag{2.0.6}$$

Now, assume that a finite soluble group G has a family $H_1, \ldots, H_t$ of subgroups whose indices have no common divisor and such that $\nu(H_i) \leq d$ for every $1 \leq i \leq d$. Is it true that $\nu(G)$ can be bounded in term of d? We proved that the answer is affirmative.

Theorem 2.0.6. [106, Theorem 1] *Let G be a finite soluble group. Assume that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $\nu(G_p) \leq d$. Then $\nu(G) \leq d + 7$.*

As customary, we denoted by $\pi(G)$ the set of prime divisors of the order of G.

To be more coherent with the statement of Theorem 2.0.3, we aimed to replaced in the statement of Theorem 2.0.6 the invariants $\nu(G)$ and $\nu(G_p)$ with $e(G)$ and $e(G_p)$. In order to do so, we need to introduce another invariant related to both $e(G)$ and $\nu(G)$. For $n \in \mathbb{N}$, let

$$\mathcal{M}(G) = \sup_{n \geq 2} \frac{\log m_n(G)}{\log n}$$

where we recall that $m_n(G)$ is the number of maximal subgroups of G with index n. (In this thesis, log will denote the logarithm to base 2, unless otherwise indicated.)

Actually $\mathcal{M}(G)$ is the "polynomial degree" of the rate of growth of $m_n(G)$. This rate has been studied for finite and profinite groups by Mann, Shalev, Borovik, Jaikin-Zapirain, Liebeck, Pyber and more recently by Ballester-Bolinches, Esteban-Romero, Jiménez-Seral and Hangyang Meng (see [18], [75], [114], [115], [12]). It is roughly equal to $\nu(G)$, indeed the following holds true (see [96, Proposition 1.2]):

$$\mathcal{M}(G) - 3.5 \leq \nu(G) \leq \mathcal{M}(G) + 2.02. \tag{2.0.7}$$

The estimation for $e(G)$ given by Lubotzky is obtained combining (2.0.6) and (2.0.7):

$$(\mathcal{M}(G) - 3.5) \cdot \frac{e-1}{e} \leq e(G) \leq (\mathcal{M}(G) + 2.02) \cdot e. \tag{2.0.8}$$

The proof of Theorem 2.0.6 relies on (2.0.7), to be precise it depend on the fact that $|\mathcal{M}(G) - \nu(G)|$ is bounded above by a constant. However the estimation in (2.0.8) leaves open the question whether $|\mathcal{M}(G) - e(G)|$ could be arbitrarily large. We observed that the arguments used in [96] can be improved and the following result can be obtained.

Theorem 2.0.7. [108, Theorem 1.1] *Let G be a finite group. Then*

$$\lceil \mathcal{M}(G) \rceil - 4 \leq e(G) \leq \lceil \mathcal{M}(G) \rceil + 3.$$

With this theorem we were able to obtain the result we aimed for:

Theorem 2.0.8. [108, Theorem 1.5] *Let G be a finite soluble group. Assume that for every prime p dividing $|G|$, there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $e(G_p) \leq \rho$. Then $e(G) \leq \rho + 9$.*

We proved Theorem 2.0.6, Theorem 2.0.7, and Theorem 2.0.8 in Section 2.2.

Observe that the proofs of the results we have seen so far, depend implicitly on the CFSG. More precisely the proof of Theorem 2.0.3, 2.0.6, 2.0.7 require the following result proved by Pyber.

Theorem 2.0.9. [96, Theorem 1.3] *There exists a constant b such that for every finite group G and every $n \geq 2$, G has at most n^b core-free maximal subgroups of index n. In fact, $b = 2$ will do.*

While the proof of Corollary 2.0.5 uses a bound on the chief length of a permutation group of degree n (see Proposition 2.1.13).

A generalization of the theorem (above mentioned) of Kovács and Sim to arbitrary finite group is given in [101]: if a finite group G has a family of d-generator subgroups whose indices have no common divisor, then G can be generated by $d+2$ elements. So a natural question is whether there is an analogous of Theorem 2.0.6 for arbitrary finite groups. This is a difficult question. Denote by $\Lambda_p(G)$, or respectively $\Lambda_{\text{nonab}}(G)$, the set of the maximal subgroups M of G with the property that the socle of G/M_G is an abelian p-group, or respectively a nonabelian group. Assume that for every $p \in \pi(G)$ there exists $G_p \leq G$ such that p does not divide $|G : G_p|$ and $\nu(G_p) \leq d$. In order to prove an analogous of Theorem 2.0.6 we would need to deduce from this hypothesis a bound on the number of maximal subgroups of G of a given index. Imitating the arguments of the proof of Theorem 2.0.6, the assumption $\nu(G_p) \leq d$ can be used to estimate the number of maximal subgroups in $\Lambda_p(G)$ in terms of d, but it remains the problem of getting an efficient estimation of the number of the maximal subgroups in $\Lambda_{\text{nonab}}(G)$. We think that it could be possible to use for this purpose the assumption $\nu(G_2) \leq d$. An evidence that this could work is that, in [98], it is showed that the number of maximal subgroups in $\Lambda_{\text{nonab}}(G)$ of index n in G can be bounded in terms of $d_2(G)$ the smallest cardinality of a generating set of a Sylow 2-subgroup of G. We would need a similar result, using a subgroup of odd index instead of a Sylow 2-subgroup.

Whether the role of a 2-Sylow subgroup can be played by an arbitrary subgroup of odd index is a problem regarding a more wide class of groups. Let us explain how a similar question also arises in the context of profinite groups. (Recall that a topological group G is profinite if it is Hausdorff, compact, and totally totally disconnected.)

Being a compact topological group, a profinite group G, can be seen as a probability space. If we denote by μ the normalized Haar measure on G, so that $\mu(G) = 1$, the probability that k random elements generate (topologically) G is defined as

$$P_G(k) = \mu(\{(x_1, \dots, x_k) \in G^k | \langle x_1, \dots, x_k \rangle = G\}),$$

where μ denotes also the product measure on G^k. A profinite group G is said to be *positively finitely generated*, PFG for short, if $P_G(k)$ is positive for some natural number k. Not all finitely generated profinite groups are PFG (for example if $\hat{F}_d$ is the free profinite group of rank $d \geq 2$ then $P_{\hat{F}_d}(t) = 0$ for every $t \geq d$, see for example [77]). It is not difficult to prove the following (see Subsection 2.2.5)

Proposition 2.0.10. [106, Proposition 1.3] *Let G be a finitely generated profinite group. If the 2-Sylow subgroups of G are finitely generated, then G is PFG.*

We do not know whether the previous result remains true if we only assume that there is a closed subgroup of G which is of odd index and PFG. Therefore, the " profinite version" of our problem, that is

Is it true that if a finitely generated profinite group G contains a PFG closed subgroup of odd index, then G is PFG?

is still open.

Finally, observe that the definition of $e(G)$ can be extended to the case of a (topologically) finitely generated profinite group G. As it is proved for example in [100, Section 6],

$$e(G) = \sup_{N \in \mathcal{N}} e(G/N),$$

where $\mathcal{N}$ is the set of the open normal subgroups of G. This implies that Theorems 2.0.3, 2.0.7 still hold if G is a finitely generated profinite group. A profinite group G is said to have *polynomial maximal subgroup growth* if there exist some constant α and σ such that $m_n(G) \leq \alpha n^\sigma$ for all n. Note that the profinite version of Theorem 2.0.7 can be considered as a quantitative version of the celebrated result of Mann and Shalev [115], saying that a profinite group is PFG if and only if it has polynomial maximal subgroup growth.

Now, we analyze a different question in the context of random generation.

Question 1. Let $n \in \mathbb{N}$. Suppose that there are two boxes, one is blue and one is red. The balls in the blue box correspond to the elements of $\mathrm{Sym}(n)$, the balls in the red box correspond to the elements of $\mathrm{Alt}(n)$. We choose one of the boxes, and then we extract balls from the chosen box, with replacement, until a transitive permutation group of degree n is generated. In order to minimize the number of extractions, is it better to choose the red box or the blue one?

Let us formalize this question. Let G be a subgroup of $\mathrm{Sym}(n)$. Let $\mathrm{P}_{\mathcal{T}}(G, t)$ be the probability that t randomly chosen elements of G generate a transitive subgroup of G. Let $G \leq \mathrm{Sym}(n)$ and let $x = (x_m)_{m \in \mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables. We may define a random variable $\tau_{G,n}$ by setting

$$\tau_{G,n} = \min\{t \geq 1 | \, \langle x_1, \dots, x_t \rangle \text{ is a transitive subgroup of G}\}.$$

We denote by $e_{\mathcal{T}}(G)$ the expectation of the random variable $\tau_{G,n}$. Hence $e_{\mathcal{T}}(G)$ is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of G is found. With arguments similar to that used for τ_G, in Subsection 2.3.1, we proved that

$$P(\tau_{G,n} > t) = 1 - P_{\mathcal{T}}(G, t) \quad \text{and} \quad e_{\mathcal{T}}(G) = \sum_{t \geq 0} (1 - P_{\mathcal{T}}(G, t)). \tag{2.0.9}$$

The case $G = \mathrm{Sym}(n)$ has been studied in [46] and [103]. Let Π_n be the set of partitions of n, that is, the set of decreasing sequences of natural numbers whose sum is n, and let Π_n^* be the set of partitions of n into at least two parts. Given $\omega = (n_1, \dots, n_k) \in \Pi_n$ with

$$n_1 = \cdots = n_{k_1} > n_{k_1+1} = \cdots = n_{k_1+k_2} > \cdots > n_{k_1+\cdots+k_{r-1}+1} = \cdots = n_{k_1+\cdots+k_r},$$

and $k_1 + \cdots + k_r = k$, we define

$$\mu(\omega) := (-1)^{k-1}(k-1)!, \quad \iota(\omega) := \frac{n!}{n_1! \dots n_k!}, \quad \nu(\omega) := k_1! k_2! \dots k_r!.$$

It turns out (see [103, Theorem 9] and [46, Proposition 2.1]) that for every $n \geq 2$,

$$\begin{aligned} P_{\mathcal{T}}(\mathrm{Sym}(n), t) &= \sum_{\omega \in \Pi_n} \frac{\mu(\omega)\iota(\omega)}{\nu(\omega)\iota(\omega)^t} \\ e_{\mathcal{T}}(\mathrm{Sym}(n)) &= -\sum_{\omega \in \Pi_n^*} \frac{\mu(\omega)\iota(\omega)^2}{\nu(\omega)(\iota(\omega)-1)}. \end{aligned} \tag{2.0.10}$$

We are interested in the case $G = \mathrm{Alt}(n)$. Since $\mathrm{Alt}(2) = \{1\}$ there are no possibilities to find a transitive subgroup of $\mathrm{Alt}(2)$, so we study the problem for $n \geq 3$. Let $n = 3$. The unique transitive subgroup of $\mathrm{Alt}(3)$ is $\mathrm{Alt}(3)$ itself, therefore

$$P(\tau_{\mathrm{Alt}(3),3} = t) = 1 - \frac{1}{3^t}, \quad \text{and} \quad e_{\mathcal{T}}(\mathrm{Alt}(3)) = \sum_{t \geq 0} \frac{1}{3^t} = \frac{3}{2}.$$

Whilst, (2.0.10) yield

$$P(\tau_{\mathrm{Sym}(3),3} = t) = 1 - \frac{3}{3^t} + \frac{2}{6^t}, \quad \text{and} \quad e_{\mathcal{T}}(\mathrm{Sym}(3)) = \frac{21}{10}.$$

Hence if $n = 3$ to find a transitive subgroup, it is more convenient to search in the alternating group.

Let us analyze the case $n = 4$. The transitive subgroups of $\mathrm{Alt}(4)$ are the noncyclic subgroups. Note that $H = \langle x_1, \dots, x_t \rangle$ is a transitive subgroup of $\mathrm{Alt}(n)$ if and only if there exist $1 \leq i < j \leq t$ such that $x_i \neq 1$ and $x_j \notin \langle x_i \rangle$. The numbers of trials needed to obtain $x \in \mathrm{Alt}(4) \setminus \{1\}$ is a geometric random variable with expectation $E_0 = \frac{12}{11}$. With probability $p_1 = \frac{3}{11}$ the element x has order 2. In this case, the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with expectation $E_1 = \frac{12}{10}$. On the other hand, with probability $p_2 = \frac{8}{11}$ the element x has order 3. In this second case, the number of trials needed to find an element $y \notin \langle x \rangle$ is a geometric random variable with expectation $E_2 = \frac{12}{9}$. Summing up we get that

$$e_{\mathcal{T}}(\mathrm{Alt}(4)) = E_0 + p_1 E_1 + p_2 E_2 = \frac{394}{165}.$$

Whilst, (2.0.10) yield

$$e_{\mathcal{T}}(\mathrm{Sym}(4)) = \frac{7982}{3795}.$$

Therefore, to have a transitive subgroup it is more convenient to search in $\mathrm{Sym}(4)$. The previous examples suggest us that the answer to the Question 1 depends on the parity of n. We confirmed this proving the following result.

Theorem 2.0.11. [107, Theorem 1.1, Theorem 2.4] *For every natural number $n \geq 3$, then*

$$P_{\mathcal{T}}(\mathrm{Sym}(n), t) - P_{\mathcal{T}}(\mathrm{Alt}(n), t) = \frac{(-1)^{n+1}(n-1)!(2^t - 1)}{(n!)^t}, \tag{2.0.11}$$

$$e_{\mathcal{T}}(\mathrm{Sym}(n)) - e_{\mathcal{T}}(\mathrm{Alt}(n)) = \frac{(-1)^{n+1} n!(n-1)!}{(n!-1)(n!-2)}. \tag{2.0.12}$$

Observe that $e_{\mathcal{T}}(\mathrm{Sym}(n)) - e_{\mathcal{T}}(\mathrm{Alt}(n))$ tends to zero when n tends to infinity, but it is positive if n is odd and negative otherwise. To explain this behaviour notice that, if $G \leq \mathrm{Sym}(n)$, then $P_{\mathcal{T}}(G, 1)$ the probability that one randomly chosen element g in G generates a transitive subgroup of $\mathrm{Sym}(n)$, coincide with the probability that g is a n-cycle: in particular

$$P_{\mathcal{T}}(\mathrm{Sym}(n), 1) = \frac{1}{n} \quad \text{and} \quad P_{\mathcal{T}}(\mathrm{Alt}(n), 1) = \begin{cases} \frac{2}{n}, & \text{if } n \text{ is odd} \\ 0, & \text{if } n \text{ is even.} \end{cases}$$

The details of the proof of Theorem 2.0.11 are discussed in Subsection 2.3.2. In [103, Section 5], it is proved that $\lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Sym}(n)) = 2$ and

$$2 = e_{\mathcal{T}}(\mathrm{Sym}(2)) \leq e_{\mathcal{T}}(\mathrm{Sym}(n)) \leq e_{\mathcal{T}}(\mathrm{Sym}(4)) = \frac{7982}{3795} \sim 2.1033.$$

A similar result can be obtained in the alternating case.

Theorem 2.0.12. [107, Theorem 1.2] *Assume that* $n \geq 3$.

1. *If* n *is odd, then* $\frac{3}{2} = e_{\mathcal{T}}(\mathrm{Alt}(3)) \leq e_{\mathcal{T}}(\mathrm{Alt}(n)) < 2$.
2. *If* n *is even, then* $2 < e_{\mathcal{T}}(\mathrm{Alt}(n)) \leq e_{\mathcal{T}}(\mathrm{Alt}(4)) = \frac{394}{165} \sim 2.3879$.

Moreover $\lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Alt}(n)) = 2$.

The proof of Theorem 2.0.12 is in Subsection 2.3.3.

Here, we pass from the theory of random generation to a question regarding the theory of minimal generation. A generating set X of a finite group G is said to be *minimal* (or *independent*) if no proper subset of X generates G. We denote by $m(G)$ the largest size of a minimal generating set of G. First steps toward investigating $m(G)$ have been taken in the context of permutation groups. An exhaustive investigation has been done for finite symmetric groups [34, 163], proving that $m(\mathrm{Sym}(n)) = n-1$ and giving a complete description of the independent generating sets of $\mathrm{Sym}(n)$ having cardinality $n-1$. Partial results for some families of simple groups are in [152]: it turns out that already in the case $G = \mathrm{PSL}(2, q)$, the precise value of $m(G)$ is quite difficult to obtain. Moreover, Apisa and Klopsch [1] proposed a natural "classification problem": given a non-negative integer c, characterize all finite groups G such that $m(G) - d(G) \leq c$, where $d(G)$ is the minimal size of a generating set of G. In particular, they classified the finite groups for which the equality $m(G) = d(G)$ holds. During the same period Lucchini started in [104, 105] a systematic investigation of how $m(G)$ can be estimated for an arbitrary finite group G.

Minded the result obtained in Theorem 2.0.2, one may ask whether a similar result holds also for $m(G)$. More precisely, denote by $d_p(G)$ the minimal number of generators of a Sylow p-subgroup of G. Is it possible to bound $m(G)$ as a function of the numbers $d_p(G)$, with p running through the prime divisors of the order of G?

It can be easily seen that, if G is a finite nilpotent group, then $m(G) = \sum_{p\in\pi(G)} d_p(G)$ (see Proposition 2.4.1 for details). For simplicity, we let

$$\delta(G) := \sum_{p\in\pi(G)} d_p(G).$$

In a private communication to Lucchini, Keith Dennis has conjectured that $m(G) \leq \delta(G)$, for every finite group G. This conjecture is true for soluble groups.

Theorem 2.0.13. [113, Theorem 1.1] *Let* G *be a finite soluble group. Then* $m(G) \leq \delta(G)$.

Despite Theorem 2.0.13, Dennis' conjecture is false if G is a symmetric group. We studied the asymptotic behaviour of the function $\delta(\mathrm{Sym}(n))$ (see Subsection 2.4.4). In particular, the following theorem holds true.

Theorem 2.0.14. [113, Theorem 5.1] *For every $n \geq 2$, we have $\delta(\mathrm{Sym}(n)) = \log_e 2 \cdot n + o(n)$.*

(See Subsection 2.4.4 for a proof of Theorem 2.0.14.) Since $m(\mathrm{Sym}(n)) = n - 1$ by [163], the difference $m(\mathrm{Sym}(n)) - \delta(\mathrm{Sym}(n))$ goes to infinity with n and the inequality $m(\mathrm{Sym}(n)) \leq \delta(\mathrm{Sym}(n))$ is satisfied by only finitely many values of n. Indeed, using the explicit upper bound on $\delta(\mathrm{Sym}(n))$ in Theorem 2.4.10 and some calculations, we have

$$\begin{aligned}
&\delta(\mathrm{Sym}(n)) = n - 1 \text{ if and only if } n \in \{1, 2, 3, 4, 5, 8, 10, 11, 16, 17, 18, 19, 25, 30, 31\},\\
&\delta(\mathrm{Sym}(n)) = n \text{ if and only if } n \in \{6, 7, 12, 13, 20, 26, 42, 43, 48\},\\
&\delta(\mathrm{Sym}(n)) = n + 1 \text{ if and only if } n \in \{14, 21, 44, 45\},\\
&\delta(\mathrm{Sym}(n)) = n + 2 \text{ if and only if } n \in \{15, 22, 23, 24, 46, 47\}.
\end{aligned}$$

For all the other values of n, we have $\delta(\mathrm{Sym}(n)) < n - 1 = m(\mathrm{Sym}(n))$.

The proof of Theorem 2.4.10 is rather technical and uses some explicit bounds on the prime counting function. However, in Lemma 2.4.8 we showed by elementary means that, for every positive real number $\eta > 1$, there exists a constant c_η such that $m(\mathrm{Sym}(n)) = n - 1 \leq c_\eta(\delta(\mathrm{Sym}(n))^\eta$, for every $n \in \mathbb{N}$.

This motivates the following conjecture, which can be seen as a natural generalization of Dennis' conjecture.

Conjecture 4. *There exist two constants c and η such that $m(G) \leq c \cdot \delta(G)^\eta$ for every finite group G.*

Given a normal subgroup N of a finite group G, we let

$$m(G, N) = m(G) - m(G/N).$$

The following theorem is a crucial result towards a proof of Conjecture 4.

Theorem 2.0.15. [113, Theorem 1.4] *Let G be a finite group. Assume that there exist two constants $\sigma \geq 1$ and $\eta \geq 2$ such that $m(X, S) \leq \sigma \cdot |\pi(S)|^\eta$, for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$. Then $m(G) \leq \sigma \cdot \delta(G)^\eta$.*

Observe that Theorem 2.0.15 reduces Conjecture 4 to the following conjecture on finite almost simple groups.

Conjecture 5. *There exist two constants σ and η such that $m(X, \operatorname{soc} X) \leq \sigma \cdot |\pi(\operatorname{soc} X)|^\eta$, for every finite almost simple group X.*

Conjecture 5 holds true, with $\eta = 2$, when $\operatorname{soc} X$ is an alternating group or a sporadic simple group (Lemma 2.4.9). Therefore, we have the following corollary.

Corollary 2.0.16. [113, Corollary 1.6] *There exists a constant σ such that, if G has no composition factor of Lie type, then $m(G) \leq \sigma\delta(G)^2$.*

Very little is known about $m(G)$ when G is an almost simple group with socle a simple group of Lie type. Saxl and Whiston in [152] proved that, if $G = \mathrm{PSL}(2, q)$ with $q = p^r$ and with p a prime number, then $m(G) \leq \max(6, \tilde{\pi}(r) + 2)$ where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r. It follows from Zsigmondy's Theorem that $\tilde{\pi}(r) \leq \tilde{\pi}(q + 1) \leq |\pi(\mathrm{PSL}(2, q))|$. Therefore Conjecture 5 holds true when $G = \mathrm{PSL}(2, q)$. In his PhD thesis [78], P. J. Keen found a good upper bound for $m(\mathrm{SL}(3, q))$, when $q = p^r$ and p is odd. In

preparation for this, he also investigated the sizes of independent sets in $\mathrm{SO}(3,q)$ and $\mathrm{SU}(3,q)$, getting in all the cases a linear bound in terms of $\tilde{\pi}(r)$. These partial results lead us to conjecture that, if $\mathrm{soc}(X)$ is a group of Lie type of rank n over the field with $q = p^r$ elements, then $m(X, \mathrm{soc}\, X)$ is polynomially bounded in terms of n and $\tilde{\pi}(r)$. If this were true, then Conjecture 5 would also be true.

The proofs of Theorem 2.0.15 and Corollary 2.0.16 are in Subsection 2.4.3. These proofs require two preliminary results, one concerning the prime divisors of the order of a finite non-abelian simple group and the other about permutation groups, proved respectively in Subections 2.4.1 and 2.4.2.

We have seen that the minimal and the maximal size of a minimal generating set of a finite group G has been well studied for many groups G. So arises naturally to ask what it is known on the (not necessarily minimal or maximal) size of a minimal generating set of G. A nice result in universal algebra, due to Tarski and known with the name of Tarski irredundant basis theorem (see for example [29, Theorem 4.4]), implies that G contains an independent generating set of cardinality k, for every positive integer $d(G) \leq k \leq m(G)$.

The proof of this theorem relies on a clever but elementary counting argument which implies also the following result: for every k with $d(G) \leq k < m(G)$ there exists a minimal generating set $\{g_1, \ldots, g_k\}$ with the property that there are $1 \leq i \leq k$ and x_1, x_2 in G such that $\tilde{\omega} := \{g_1, \ldots, g_{i-1}, x_1, x_2, g_{i+1}, \ldots, g_k\}$ is again a minimal generating set of G. Moreover x_1, x_2 can be chosen with the extra property that $g_i = x_1 x_2$.

Now, we introduce some definitions to conclude this chapter with some results in this direction. Let $\omega := \{g_1, \ldots, g_k\}$ be a minimal generating set of G with $k < m(G)$. We say that $\omega = (g_1, \ldots, g_k)$ is *extendible* if there exist $1 \leq i \leq k$ and x_1, x_2 in G such that $\tilde{\omega} := \{g_1, \ldots, g_{i-1}, x_1, x_2, g_{i+1}, \ldots, g_k\}$ is a minimal generating set of G. In this case we say that $\tilde{\omega}$ is an *immediate descendant* of ω. Furthermore, if $g_i = x_1 x_2$, then we say that $\tilde{\omega}$ is a *strong immediate descendant* of ω. More in general, a minimal generating set ω^* of cardinality t (with $t > k$) *is a (strong) descendant* of ω if there exists a sequence $\omega_0, \omega_1, \ldots, \omega_{t-k}$ where $\omega_0 = \omega$, $\omega^* = \omega_{t-k}$ and ω_j is a (strong) immediate descendant of ω_{j-1} for every $1 \leq j \leq t-k$. Finally we say that ω is *(strongly) totally extendible* if it has a (strong) descendant of cardinality $m(G)$.

There exist minimal generating sets that are not totally extendible. For example, let $G = \mathrm{Sym}(4)$ and consider $g_1 = (1,2,3,4)$ and $g_2 = (1,3,2,4)$. Clearly $G = \langle g_1, g_2 \rangle$. Assume, by contradiction, that there exists x_1 and x_2 such that $\{x_1, x_2, g_i\}$ is a minimal generating set of G, with $j \in \{1,2\}$. For $i \in \{1,2\}$, we have that $\langle x_i, g_j \rangle$ is a proper subgroup of G containing g_j, but this implies $x_i \in N_G(\langle g_j \rangle)$: as a consequence $\langle g_j \rangle$ is normal in $G = \langle x_1, x_2, g_j \rangle$, but this is false. Therefore $\{g_1, g_2\}$ is not extendible. One can ask whether in a finite group G there exists at least one generating set of cardinality $d(G)$ which is totally extendible. We prove that this happens for finite soluble groups.

Theorem 2.0.17. [110, Theorem 1.1] *Let G be a finite soluble group. Then there exists a strongly totally extendible generating set of cardinality $d(G)$.*

We now say that G *has the extension property* if every minimal generating set of G whose cardinality is strictly less than $m(G)$ has an immediate descendant. In [110], we investigated the structure of the finite groups satisfying the extension property. In the case of finite nilpotent groups, a complete description can be easily obtained: a finite nilpotent G has the extension property if and only if either G is a p-group or G is cyclic and $|\pi(G)| = 2$ (see Proposition 2.5.3). There are also non nilpotent groups with the extension property, for example the groups G with the property that $d(G) = m(G)$ (classified in [1, Theorem 1.6]). There exist also non nilpotent groups that satisfy the extension property but not the equality $d(G) = m(G)$. Consider for example the semidirect product $G = V \rtimes Q$, where Q is the

quaternion group, V is an elementary abelian group of order 9 and the action of Q on V is obtained by identifying Q with a Sylow 2-subgroup of $\mathrm{SL}(2,3)$. We have $d(G) = 2$, $m(G) = 3$. Moreover, if $G = \langle x_1, x_2 \rangle$, then $|x_1| = |x_2| = 4$, and consequently there exists $v \in V$ such that $\langle x_1^v, x_2 \rangle$ is a Sylow 2-subgroup of G. Hence $\{x_1^v, x_2, [v, x_1]\}$ is an immediate descendant of $\{x_1, x_2\}$, and G has the extension property. We obtained a complete description of the finite soluble groups with the extension property. In particular we proved the following statement.

Theorem 2.0.18. [113, Theorem 1.2] *A finite soluble group satisfies the extension property if and only if one of the following occurs:*

1. $d(G) = m(G)$.
2. $G/\operatorname{Frat} G = V \rtimes H$ *where* V *is an irreducible* H*-module,* $d(H) = m(H) = 2$ *and whenever* $\{h_1, h_2\}$ *is a generating set of* H*, then there exists* $i \in \{1, 2\}$ *such that* $C_V(h_i) = \{0\}$*. In this case* $d(G) = 2$ *and* $m(G) = 3$*.*
3. G *is cyclic and* $|\pi(G)| = 2$*.*

By [1, Theorem 1.5], if $d(G) = m(G)$, then $\pi(G) \leq 2$, so we immediately deduce the following corollary.

Corollary 2.0.19. [113, Corollary 1.3] *If* G *is finite soluble group with the extension property, then* $|\pi(G)| \leq 3$ *and* $m(G) \leq d(G) + 1$*.*

The bound $|\pi(G)| \leq 3$ in the previous corollary is best possible. Let H be the dicyclic group of order 12. This group has an action on the 2-dimensional vector space V over the field with 13 elements and this action is irreducible and fixed-point-free: we may then consider the semidirect product $G = V \rtimes H$.

From the proofs of Theorem 2.0.18 and Proposition 2.5.3, we readily deduce the following.

Corollary 2.0.20. [113, Corollary 1.4] *If a finite soluble group* G *satisfies the extension property, then it also satisfies the strong extension property.*

To prove Theorems 2.0.17, 2.0.18 other than heavily use the concept of crowns, we proved some Lemmas in linear algebra (see Subsections 2.5.2, 2.5.3).

2.1 A probabilistic version of a theorem of Guralnick and Lucchini

2.1.1 Preliminaries

Let G be a finite group and use the following notations:

- For a given prime p, $d_p(G)$ is the smallest cardinality of a generating set of a Sylow p-subgroup of G.
- For a given prime p and a positive integer t, $\alpha_{p,t}(G)$ is the number of complemented factors of order p^t in a chief series of G.
- For a given prime p, $\alpha_p(G) = \sum_t \alpha_{p,t}(G)$ is the number of complemented factors of p-power order in a chief series of G.
- $\beta(G)$ is the number of nonabelian factors in a chief series of G.

Lemma 2.1.1. *For every finite group G, we have:*

1. $\alpha_p(G) \leq d_p(G)$.
2. $\alpha_2(G) + \beta(G) \leq d_2(G)$.
3. *If* $\beta(G) \neq 0$, *then* $\beta(G) \leq d_2(G) - 1$.
4. *If* $\alpha_{2,1}(G) = 0$, *then* $\alpha_2(G) + \beta(G) \leq d_2(G) - 1$.
5. *If* $\alpha_{p,1}(G) = 0$, *then* $\alpha_p(G) \leq d_p(G) - 1$.

Proof. (1), (2) and (3) are proved in [99, Lemma 4]. Now assume that no complemented chief factor of G has order 2 and let $r = \alpha_2(G) + \beta(G)$. There exists a sequence $X_r \leq Y_r \leq \cdots \leq X_1 \leq Y_1$ of normal subgroups of G such that, for every $1 \leq i \leq r$, Y_i/X_i is a complemented chief factor of G of even order. Notice that $\beta(G/Y_1) = \alpha_2(G/Y_1) = 0$, hence G/Y_1 is a finite soluble group all of whose complemented chief factors have odd order, but then G/Y_1 has odd order and consequently $d_2(G) = d_2(Y_1)$. Moreover, as in the proof of [99, Lemma 4], $d_2(Y_1) \geq d_2(Y_1/X_1) + r - 1$. Since $|Y_1/X_1| \neq 2$ and the Sylow 2-subgroups of a finite nonabelian simple cannot be cyclic [144, 10.1.9], we deduce $d_2(Y_1/X_1) \geq 2$ and consequently $d_2(G) = d_2(Y_1) \geq r + 1$. This proves (4). The proof of (5) is similar. □

Using the notations introduced in [96, Section 2], we say that a maximal subgroup M of G is of type A if $\mathrm{soc}(G/\mathrm{Core}_G(M))$ is abelian, of type B otherwise, and we denote by $m_n^A(G)$ (respectively $m_n^B(G)$) the number of maximal subgroups of G of type A (respectively B) of index n. Given $t \in \mathbb{N}$ and $p \in \pi(G)$, define

$$\mu^*(G,t) = \sum_{k \geq t} \left(\sum_{n \geq 5} \frac{m_n^B(G)}{n^k} \right), \quad \mu_p(G,t) = \sum_{k \geq t} \left(\sum_{n \geq 1} \frac{m_{p^n}^A(G)}{p^{nk}} \right).$$

Lemma 2.1.2. *Let $t \in \mathbb{N}$. Then $e(G) \leq t + \mu^*(G,t) + \sum_{p \in \pi(G)} \mu_p(G,t)$.*

Proof. By (2.0.3) and (2.0.1),

$$e(G) \leq t + \sum_{n \geq t} (1 - P_G(n)) \leq t + \sum_{k \geq t} \left(\sum_{n \geq 2} \frac{m_n(G)}{n^k} \right). \quad \square$$

Lemma 2.1.3. *Let $t \in \mathbb{N}$. If $\beta(G) = 0$, then $\mu^*(G,t) = 0$. If $t \geq \beta(G) + 3$, then*

$$\mu^*(G,t) \leq \frac{\beta(G)(\beta(G)+1)}{2 \cdot 5^{t-4}} \cdot \frac{1}{4}.$$

Proof. The result follows from [99, Lemma 8] and its proof. In those proofs were used Theorem 2.0.9; this explain the implicit dependence on CFSG of our results.

□

Lemma 2.1.4. *Let $t \in \mathbb{N}$ and $p \in \pi(G)$. If $\alpha_p(G) = 0$, then $\mu_p(G,t) = 0$.*

1. *If $\alpha_2(G) \leq t-1$ and $\alpha_{2,u}(G) \leq t-2$ for every $u > 1$, then*

$$\mu_2(G,t) \leq \frac{1}{2^{t-\alpha_2(G)-1}}.$$

2. *Let p be an odd prime. If $\alpha_p(G) \leq t-2$ then*

$$\mu_p(G,t) \leq \frac{1}{p^{t-\alpha_p(G)-2}} \frac{1}{(p-1)^2}.$$

Proof. The result follows from [99, Lemma 7] and its proof.

□

Let G be a finite soluble group and let $\mathcal{A}$ be a set of representatives for the irreducible G-modules that are G-isomorphic to some complemented chief factor of G. For every $A \in \mathcal{A}$, let δ_A be the number of complemented factors G-isomorphic to A in a chief series of G, $q_A = |\operatorname{End}_G(A)|$, $r_A = \dim_{\operatorname{End}_G(A)}(A)$, $\zeta_A = 0$ if A is a trivial G-module, $\zeta_A = 1$ otherwise. Moreover, for every $l \in \mathbb{N}$, let $Q_{A,l}(s)$ be the Dirichlet polynomial defined by

$$Q_{A,l}(s) = 1 - \frac{q_A^{l+r_A \cdot \zeta_A}}{q_A^{r_A \cdot s}}.$$

By [55, Satz 1], for every positive integer k we have

$$P_G(k) = \prod_{A \in \mathcal{A}} \left(\prod_{0 \leq l \leq \delta_A - 1} Q_{A,l}(k) \right). \tag{2.1.1}$$

For every prime p dividing $|G|$, let $\mathcal{A}_p$ be the subset of $\mathcal{A}$ consisting of the irreducible G-modules having order a power of p and let

$$P_{G,p}(k) = \prod_{A \in \mathcal{A}_p} \left(\prod_{0 \leq l \leq \delta_A - 1} Q_{A,l}(k) \right). \tag{2.1.2}$$

Definition 2.1.5. *For every prime p and every positive integer α let*

$$C_{p,\alpha}(s) = \prod_{0 \leq i \leq \alpha - 1} \left(1 - \frac{p^i}{p^s}\right), \quad D_{p,\alpha}(s) = \prod_{1 \leq i \leq \alpha} \left(1 - \frac{p^i}{p^s}\right).$$

Lemma 2.1.6. *Let G be a finite soluble group and let k be a positive integer.*

1. *If $d_p(G) \leq d$, then $P_{G,p}(k) \geq D_{p,d}(k)$.*
2. *If p divides $|G/G'|$, then $P_{G,p}(k) \geq C_{p,d}(k)$.*
3. *If $\alpha_{p,1}(G) = 0$, then $P_{G,p}(k) \geq C_{p,d}(k)$.*

4. If $d_2(G) \leq d$, then $P_{G,2}(k) \geq C_{2,d}(k)$.

Proof. Suppose that $\mathcal{A}_p = \{A_1, \ldots, A_t\}$ and let $q_i = q_{A_i}$, $r_i = r_{A_i}$, $\zeta_i = \zeta_{A_i}$ and $\delta_i = \delta_{A_i}$. Recall that

$$P_{G,p}(k) = \prod_{\substack{1 \leq i \leq t \\ 0 \leq l \leq \delta_i - 1}} Q_{A_i,l}(k). \tag{2.1.3}$$

By Lemma 2.1.1, $\delta_1 + \delta_2 + \cdots + \delta_t = \alpha_p(G) \leq d_p(G)$, hence the number of factors $Q_{A_i,l}(k)$ in (2.1.3) is at most $d_p(G)$. We order these factors in such a way that $Q_{A_i,u}(k)$ precedes $Q_{A_j,v}(k)$ if either $i < j$ or $i = j$ and $u < v$. Moreover we order the elements of $\mathcal{A}_p$ in such a way that A_1 is the trivial G-module if p divides $|G/G'|$.
1) Since $D_{p,d}(k) = 0$ if $k \leq d$, we may take $k > d$. To show that $P_{G,p}(k) \geq D_{p,d}(k)$, it is sufficient to show that the j-th factor $Q_j(k) = Q_{A_i,l}(k)$ of $P_{G,p}(k)$ is greater than the j-th factor

$$D_j(k) = 1 - \frac{p^j}{p^k}$$

of $D_{p,d}(k)$. If $j \leq \delta_1$ then $Q_j(k) = Q_{A_1,l}(k)$ with $l = j - 1$. If $j > \delta_1$ then $Q_j(k) = Q_{A_i,l}(k)$ for some $i \in \{2, \ldots, t\}$ and $l \in \{0, \ldots, \delta_i - 1\}$, thus

$$j = \delta_1 + \delta_2 + \cdots + \delta_{i-1} + l + 1 \geq l + 2.$$

In any case,

$$q_i^{r_i\zeta_i} q_i^l \leq q_i^{r_i(l+1)} \leq q_i^{r_i j}.$$

We have $q_i = p^{n_i}$ for some $n_i \in \mathbb{N}$. Since $j \leq d < k$, we deduce that

$$\frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \leq \frac{q_i^{r_i j}}{q_i^{r_i k}} = \left(\frac{p^j}{p^k}\right)^{r_i n_i} \leq \frac{p^j}{p^k}.$$

But then

$$Q_j(k) = 1 - \frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \geq 1 - \frac{p^j}{p^k} = D_j(k).$$

2) Since $C_{p,d}(k) = 0$ if $k < d$, we may take $k \geq d$. To show that $P_{G,p}(k) \geq C_{p,d}(k)$, it is sufficient to show that the j-th factor $Q_j(k) = Q_{A_i,l}(k)$ of $P_{G,p}(k)$ is greater than the j-th factor

$$C_j(k) = 1 - \frac{p^{j-1}}{p^k}$$

of $C_{p,d}(k)$. If $i = 1$, then, by the way in which we ordered the elements of $\mathcal{A}_p$, we have $Q_j(k) = C_j(k)$. Otherwise, as we have seen in the proof of (1), $l + 2 \leq j$ so $r_i\zeta_i + l \leq r_i + j - 2 \leq r_i(j-1)$. Since $j \leq d \leq k$, we deduce that

$$\frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \leq \frac{q_i^{r_i(j-1)}}{q_i^{r_i k}} \leq \frac{p^{j-1}}{p^k} \quad \text{and} \quad Q_j(k) = 1 - \frac{q_i^{r_i\zeta_i} q_i^l}{q_i^{r_i k}} \geq 1 - \frac{p^{j-1}}{p^k} = C_j(k).$$

3) Assume that no complemented chief factor of G has order p. By (5) of Lemma 2.1.1, $\alpha_p(G) \leq d_p(G) - 1 \leq d - 1$. But then, in the factorization of $P_{G,p}(k)$ described in (2.1.3) the number of factors is at most $d - 1$ and, arguing as in the proof of (1), we conclude $P_{G,p}(k) \geq D_{p,d-1}(k) \geq C_{p,d}(k)$
4) We may assume $\alpha_2(G) \neq 0$ (otherwise $P_{G,2}(k) = 1$). Since $\alpha_{2,1}(G) \neq 0$ if and only if 2 divides $|G/G'|$, the conclusion follows from (2) and (3).

□

2.1.2 Proof of Theorem 2.0.3

Proposition 2.1.7. *Let G be a finite group. If all the Sylow subgroups of G can be generated by d elements and G is not soluble, then*

$$e(G) \leq d + \kappa^* \quad \text{with} \quad \kappa^* \leq 2.750065.$$

Proof. Let $\beta = \beta(G)$. Since G is not soluble, $\beta > 0$, hence by (2) and (3) of Lemma 2.1.1, we have $1 \leq \beta \leq d_2(G) - 1 \leq d - 1$ and $\alpha_2(G) \leq d_2(G) - \beta \leq d - 1$. We distinguish two cases:
a) $\beta < d - 1$. By Lemma 2.1.2, 2.1.3 and 2.1.4 and using a rather precise approximation of $\sum_p (p-1)^{-2}$ given in [38], we conclude

$$\begin{aligned} e(G) &\leq d + 2 + \mu^*(G, d+2) + \mu_2(G, d+2) + \sum_{p>2} \mu_p(G, d+2) \\ &\leq d + 2 + \frac{1}{20} + \frac{1}{4} + \sum_{p>2} \frac{1}{(p-1)^2} \leq d + 2.675065. \end{aligned}$$

b) $\beta = d - 1$. By (2) and (4) of Lemma 2.1.1, either $\alpha_2(G) = 0$ or $\alpha_2(G) = \alpha_{2,1}(G) = 1$. In the first case $\mu_2(G, d+2) = 0$, in the second case $m_2^A(G) = 1$ and consequently

$$\mu_2(G, d+2) = \sum_{k \geq d+2} \frac{m_2^A(G)}{2^k} \leq \sum_{k \geq d+2} \frac{1}{2^k} \leq \sum_{k \geq 4} \frac{1}{2^k} \leq \frac{1}{8}.$$

By Lemma 2.1.2, 2.1.3 and 2.1.4, we conclude

$$\begin{aligned} e(G) &\leq d + 2 + \mu^*(G, d+2) + \mu_2(G, d+2) + \sum_{p>2} \mu_p(G, d+2) \\ &\leq d + 2 + \frac{1}{4} + \frac{1}{8} + \sum_{p>2} \frac{1}{(p-1)^2} \leq d + 2.750065. \end{aligned}$$

□

The previous proposition reduces the proof of Theorem 2.0.3 to the particular case when G is soluble. To deal with this case, we are going to introduce, for every positive integer d and every set of primes π, a supersoluble group $H_{\pi,d}$ all of whose Sylow subgroups are d-generated and with the property that $e(G) \leq e(H_{\pi,d})$ whenever G is soluble, $\pi(G) \subseteq \pi$ and the Sylow subgroups of G are d-generated.

Definition 2.1.8. *Let π be a finite set of prime numbers with $2 \in \pi$, and let d be a positive integer. We define $H_{\pi,d}$ as the semidirect product of A with $\langle y, z_1, \ldots, z_{d-1} \rangle$, where A is isomorphic to $\prod_{p \in \pi \setminus \{2\}} C_p^d$ and $\langle y, z_1, \ldots, z_{d-1} \rangle$ is isomorphic to C_2^d and acts on A via $x^y = x^{-1}$, $x^{z_i} = x$ for all $x \in A$ and $1 \leq i \leq d-1$. Thus*

$$H_{\pi,d} \cong \left(\left(\prod_{p \in \pi \setminus \{2\}} C_p^d \right) \rtimes C_2 \right) \times C_2^{d-1}.$$

Theorem 2.1.9. *Let G be a finite soluble group. If all the Sylow subgroups of G can be generated by d elements, then $e(G) \leq e(H_{\pi,d})$, where $\pi = \pi(G) \cup \{2\}$.*

Proof. Let $H = H_{\pi,d}$, $p \in \pi$ and $k \in \mathbb{N}$. Let $\mathcal{A}$ be a set of representatives for the irreducible H-modules that are H-isomorphic to some complemented chief factor of H and let $\mathcal{A}_p$ be the subset of $\mathcal{A}$ consisting of the irreducible H-modules having order a power of p. For every $p \in \pi$, $\mathcal{A}_p$ contains a unique element A_p. Moreover $|A_p| = p$, $\delta_{A_p} = d$ and $\zeta_{A_p} = 1$ if $p \neq 2$, while $\zeta_{A_2} = 0$. Hence, by (2.1.2), $P_{H,p}(k) = D_{p,d}(k)$ if $p \neq 2$, while $P_{H,2}(k) = C_{2,d}(k)$. By Lemma 2.1.6, $P_{G,p}(k) \geq P_{H,p}(k)$ for every $p \in \pi(G)$. This implies

$$P_G(k) = \prod_{p \in \pi(G)} P_{G,p}(k) \geq \prod_{p \in \pi} P_{H,p}(k) = P_H(G)$$

and consequently $e(G) = \sum_{k \geq 0} (1 - P_G(k)) \leq \sum_{k \geq 0} (1 - P_H(k)) = e(H)$.

□

Definition 2.1.10. *Let π be a finite set of prime numbers with $2 \in \pi$, and let d be a positive integer. We set $e_d = \sup_\pi e(H_{\pi,d})$ and $\kappa = \sup_d(e_d - d)$.*

Let $\pi^* = \pi \setminus \{2\}$. Since $P_{H_{\pi,d}}(k) = 0$ for all $k \leq d$ we have

$$\begin{aligned} e(H_{\pi,d}) &= \sum_{k\geq 0}\Big(1 - P_{H_{\pi,d}}(k)\Big) = d + 1 + \sum_{k\geq d+1}\left(1 - C_{2,d}(k)\prod_{p\in\pi^*} D_{p,d}(k)\right) \\ &= d + 1 + \sum_{k\geq d+1}\left(1 - \prod_{1\leq i\leq d}\left(1 - \frac{2^{i-1}}{2^k}\right)\prod_{p\in\pi^*}\prod_{1\leq i\leq d}\left(1 - \frac{p^i}{p^k}\right)\right) \\ &= d + 1 + \sum_{t\geq 0}\left(1 - \prod_{1\leq i\leq d}\left(1 - \frac{2^{i-1}}{2^{t+(d+1)}}\right)\prod_{p\in\pi^*}\prod_{1\leq i\leq d}\left(1 - \frac{p^i}{p^{t+(d+1)}}\right)\right). \end{aligned}$$

We immediately deduce that $e(H_{\pi,d}) - d$ increases as d increases. Moreover we have

$$\begin{aligned} e_d - d &= \sup_\pi\,(e(H_{\pi,d}) - d) \\ &= 1 + \sum_{k\geq d+1}\left(1 - \frac{(1-\frac{1}{2^k})}{(1-\frac{2^d}{2^k})}\prod_p\prod_{1\leq i\leq d}\left(1 - \frac{p^i}{p^k}\right)\right). \end{aligned}$$

For $k = d+1$ the double product tends to 0, while for $k \geq d+2$ it tends to $\prod_{1\leq i\leq d}\zeta(k-i)^{-1}$, where ζ denotes the Riemann zeta function. Hence we get

$$\begin{aligned} e_d - d &= 2 + \sum_{k\geq d+2}\left(1 - \frac{(1-\frac{1}{2^k})}{(1-\frac{2^d}{2^k})}\prod_{1\leq i\leq d}\zeta(k-i)^{-1}\right) \\ &= 2 + \sum_{j\geq 1}\left(1 - \frac{(1-\frac{1}{2^{j+(d+1)}})}{(1-\frac{1}{2^{j+1}})}\prod_{1\leq l\leq d}\zeta(j+l)^{-1}\right) \\ &= 2 + \sum_{j\geq 1}\left(1 - \left(\frac{2^{j+1}-2^{-d}}{2^{j+1}-1}\right)\prod_{1+j\leq n\leq d+j}\zeta(n)^{-1}\right). \end{aligned}$$

Let $c = \prod_{2\leq n\leq\infty}\zeta(n)^{-1}$. Since $e_d - d$ increases as d grows, we get

$$\begin{aligned} \kappa &= \lim_{d\to\infty} e_d - d \\ &= 2 + \left(1 - \left(\frac{2^2}{2^2-1}\right)c\right) + \sum_{j\geq 2}\left(1 - \left(\frac{2^{j+1}}{2^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right) \\ &= 2 + \left(1 - \frac{4}{3}\cdot c\right) + \sum_{j\geq 2}\left(1 - \left(1 + \frac{1}{2^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right). \end{aligned}$$

Using the computer algebra system **PARI/GP** [133], we get

$$\kappa = 2 + \left(1 - \frac{4}{3}\cdot c\right) + \sum_{j\geq 2}\left(1 - \left(1 + \frac{1}{2^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right) \sim 2.752395.$$

Combining this result with Proposition 2.1.7 and Theorem 2.1.9, we obtain the proof of Theorem 2.0.3.

2.1.3 Proof of Theorem 2.0.4

To prove Theorem 2.0.4 we need prove the preliminar result below.

Theorem 2.1.11. *Let G be a finite soluble group. There exists a finite supersoluble group H such that*

1. $\pi(H) = \pi(G)$,
2. $P_G(k) \geq P_H(k)$ *for all* $k \in \mathbb{N}$,
3. $d_p(G) \geq d_p(H)$ *for all* $p \in \pi(G)$,
4. $\pi(G/G') \subseteq \pi(H/H')$.

Proof. Let $\pi(G) = \{p_1, \ldots, p_n\}$ with $p_1 \leq \cdots \leq p_n$. For $i \in \{1, \ldots, n\}$, set $\pi_i = \{p_1, \ldots, p_i\}$. We will prove, by induction on i, that for every $i \in \{1, \ldots, n\}$ there exists a supersoluble group H_i such that $\pi(H_i) = \pi_i$ and, for every $j \leq i$,

1. $P_{H_i,p_j}(k) \leq P_{G,p_j}(k)$ for all $k \in \mathbb{N}$,
2. $d_{p_j}(H_i) \leq d_{p_j}(G)$,
3. if C_{p_j} is an epimorphic image of G, then C_{p_j} is an epimorphic image of H_i,
4. $\pi_i \cap \pi(G/G') \subseteq \pi(H_i/H_i')$.

Assume that H_i has been constructed and set $p = p_{i+1}$ and $d_p = d_p(G)$. We distinguish two different cases:
1) Either p divides $|G/G'|$ or G contains no complemented chief factor of order p. We consider the direct product $H_{i+1} = H_i \times C_p^{d_p}$. Clearly $P_{H_{i+1},p_j}(k) = P_{H_i,p_j}(k) \leq P_{G,p_j}(k)$ if $j \leq i$. Moreover, by (2) and (3) of Lemma 2.1.6, $P_{H_{i+1},p}(k) = C_{p,d_p}(k) \leq P_{G,p}(k)$.
2) p does not divide $|G/G'|$ but G contains a complemented chief factor which is isomorphic to a nontrivial G-module, say A, of order p. In this case $G/C_G(A)$ is a nontrivial cyclic group whose order divides $p-1$. Let q be a prime divisor of $|G/C_G(A)|$ (it must be $q = p_j$ for some $j \leq i$). Since q divides $|G/G'|$, we have that q divides also $|H_i/H_i'|$, hence there exists a normal subgroup N of H_i with $H_i/N \cong C_q$ and a nontrivial action of H_i on C_p with kernel N. We use this action to construct the supersoluble group $H_{i+1} = C_p^{d_p} \rtimes H_i$. Clearly $P_{H_{i+1},p_j}(k) = P_{H_i,p_j}(k) \leq P_{G,p_j}(k)$ if $j \leq i$. Moreover, by (1) of Lemma 2.1.6, $P_{H_{i+1},p}(k) = D_{p,d_p}(k) \leq P_{G,p}(k)$.

We conclude the proof, noticing that $H = H_n$ satisfies the requests in our statement. □

Proof of Theorem 2.0.4. Let $\pi = \pi(G)$. By Theorem 2.1.11, there exists a supersoluble group H such that $\pi(H) = \pi$, $d_p(H) \leq d$ for every $p \in \pi$ and $P_G(k) \geq P_H(k)$ for every $k \in \mathbb{N}$. In particular $e(G) = \sum_{k\geq 0}(1 - P_G(k)) \leq \sum_{k\geq 0}(1 - P_H(k)) = e(H)$.

Since H is supersoluble, if A is H-isomorphic to a chief factor of H, then $|A| = p$ for some $p \in \pi$ and $H/C_H(A)$ is a cyclic group of order dividing $p-1$. If p is a Fermat prime, then $H/C_H(A)$ is a 2-group and, since $|H|$ is odd, we must have $H = C_H(A)$. This implies that if $p \in \pi$ is a Fermat prime, then $P_{H,p}(k) = C_{p,d_p(H)}(k) \geq C_{p,d}(k)$. For all the other primes in π, by (1) of Lemma 2.1.6 we have $P_{H,p}(k) \geq D_{p,d}(k)$. Therefore, denoting by Λ the set of the Fermat primes and by Δ the set of the remaining odd primes, we get

$$P_H(k) = \prod_{p\in\pi} P_{H,p}(k) \geq \prod_{p\in\Lambda} C_{p,d}(k) \prod_{p\in\Delta} D_{p,d}(k).$$

It follows that

$$\begin{aligned} e(H) &= \sum_{k\geq 0}(1-P_H(k)) \\ &\leq \sum_{k\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^k}\right)\prod_{\substack{p\in\Delta\\ p\neq 2}}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^k}\right)\right) \\ &= d+1+\sum_{k\geq d+1}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^k}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^k}\right)\right) \\ &= d+1+\sum_{t\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^{t+(d+1)}}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+(d+1)}}\right)\right). \end{aligned}$$

Let

$$\tilde{\kappa}_d=\sum_{t\geq 0}\left(1-\prod_{p\in\Lambda}\prod_{1\leq i\leq d}\left(1-\frac{p^{i-1}}{p^{t+(d+1)}}\right)\prod_{p\in\Delta}\prod_{1\leq i\leq d}\left(1-\frac{p^i}{p^{t+(d+1)}}\right)\right)+1.$$

It can be easily check that $\tilde{\kappa}_d$ increases as d increases. Let

$$b=\prod_{1\leq n\leq\infty}\left(1-\frac{1}{2^n}\right)^{-1},\qquad c=\prod_{2\leq n\leq\infty}\zeta(n)^{-1}$$

and let $\Lambda^*=\{3,\ 5,\ 17,\ 257,\ 65537\}$ be the set of the known Fermat primes. Similar computations to the ones in the final part of Subsection 2.1.2 lead to the conclusion

$$\begin{aligned} \tilde{\kappa}_d &\leq 3-\frac{b\cdot c}{2}\prod_{p\in\Lambda}\frac{p^2}{p^2-1}+\sum_{j\geq 2}\left(1-b\prod_{1\leq n\leq j}\left(1-\frac{1}{2^n}\right)\prod_{p\in\Lambda}\left(1+\frac{1}{p^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right) \\ &\leq 3-\frac{b\cdot c}{2}\prod_{p\in\Lambda^*}\frac{p^2}{p^2-1}+\sum_{j\geq 2}\left(1-b\prod_{1\leq n\leq j}\left(1-\frac{1}{2^n}\right)\prod_{p\in\Lambda^*}\left(1+\frac{1}{p^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right). \end{aligned}$$

Let

$$\tilde{\kappa}=3-\frac{b\cdot c}{2}\prod_{p\in\Lambda^*}\frac{p^2}{p^2-1}+\sum_{j\geq 2}\left(1-b\prod_{1\leq n\leq j}\left(1-\frac{1}{2^n}\right)\prod_{p\in\Lambda^*}\left(1+\frac{1}{p^{j+1}-1}\right)c\prod_{2\leq n\leq j}\zeta(n)\right).$$

With the help of **PARI/GP**, we get that $\tilde{\kappa}\sim 2.148668$. □

2.1.4 Proof of Theorem 2.0.5

It follows some necessary preliminary results.

Theorem 2.1.12. *[83, Corollary] If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p\rfloor$ elements.*

Theorem 2.1.13. *[116, Theorem 10.0.5] The chief length of a permutation group of degree n is at most $n-1$.*

Lemma 2.1.14. *If $G\leq\mathrm{Sym}(n)$ and $n\geq 8$, then $\beta(G)\leq\lfloor n/2\rfloor-3$.*

Proof. Let $R(G)$ be the soluble radical of G. By [69, Theorem 2] $G/R(G)$ has a faithful permutation representation of degree at most n, so we may assume that $R(G)=1$. In particular $\mathrm{soc}(G)=S_1\times\cdots\times S_r$ where $S_1,\ldots,S_r$ are nonabelian simple groups and, by [51, Theorem 3.1], $n\geq 5r$. Let $K=N_G(S_1)\cap\cdots\cap N_G(S_r)$. We have that $K/\mathrm{soc}(G)$ is soluble and that $G/K\leq\mathrm{Sym}(r)$, so by Theorem 2.1.13, $\beta(G/K)\leq r-1$ (and indeed $\beta(G/K)=0$ if $r\leq 4$). But then $\beta(G)\leq 2r-1\leq 2\lfloor n/5\rfloor-1$ if $r\geq 5$, $\beta(G)\leq r\leq\lfloor n/5\rfloor$ otherwise. □

Lemma 2.1.15. *Suppose that $G \leq \mathrm{Sym}(n)$ with $n \geq 8$. If G is not soluble, then*

$$e(G) \leq \lfloor n/2 \rfloor + 1.533823.$$

Proof. Let $m = \lfloor n/2 \rfloor$. By Theorem 2.1.12, $d_2(G) \leq m$. Since G is not soluble, we must have $\beta(G) \geq 1$. By Lemma 2.1.14, $\beta(G) \leq m-3$, hence, by Lemma 2.1.3, $\mu^*(G,m) \leq 1/4$. By (2) and (4) of Lemma 2.1.1, $\alpha_2(G) \leq m-1$ and $\alpha_{2,u}(G) \leq m-2$ for every $u > 1$, hence, by Lemma 2.1.4, $\mu_2(G,m) \leq 1$. If $p \geq 5$, then, by Theorem 2.1.12, $m - \alpha_p(G) \geq m - d_p(G) \geq m - \lfloor n/5 \rfloor \geq 3$ so, by Lemma 2.1.4, $\mu_p(G,m) \leq (p(p-1)^2)^{-1}$. Since $n \geq 8$ we have $m - \alpha_3(G) \geq m - \lfloor n/3 \rfloor \geq 2$ if $n \neq 9$. On the other hand, it can be easily checked that $\alpha_3(G) \leq 2$ for every non-soluble subgroup G of $\mathrm{Sym}(9)$, so $m - \alpha_3(G) \geq 2$ also when $n = 9$. But then, again by Lemma 2.1.4, $\mu_3(G,m) \leq 1/4$. It follows that

$$\begin{aligned} e(G) &\leq m + \mu^*(G,m) + \mu_2(G,m) + \mu_3(G,m) + \sum_{p>3} \mu_p(G,m) \\ &\leq m + \frac{1}{4} + 1 + \frac{1}{4} + \sum_{p \geq 5} \frac{1}{p(p-1)^2} \leq m + \frac{3}{2} + \sum_{n \geq 5} \frac{1}{n(n-1)^2} \leq m + 1.533823. \end{aligned}$$ □

Lemma 2.1.16. *Suppose that $G \leq \mathrm{Sym}(n)$ with $n \geq 8$. If G is soluble and $\alpha_{2,1}(G) < \lfloor n/2 \rfloor$, then*

$$e(G) \leq \lfloor n/2 \rfloor + 1.533823.$$

Proof. Let $\alpha = \alpha_{2,1}(G)$, $\alpha^* = \sum_{i>1} \alpha_{2,i}(G)$ and $m = \lfloor n/2 \rfloor$. Notice that $\alpha^* \leq m-1$ by Lemma 2.1.1 (4). Set

$$\mu_{2,1}(G,t) = \sum_{k \geq t} \frac{m_2^A(G)}{2^k}, \quad \mu_{2,2}(G,t) = \sum_{k \geq t} \left(\sum_{n \geq 2} \frac{m_{2^n}^A(G)}{2^{nk}} \right).$$

We distinguish two cases:
a) $\alpha_{2,u}(G) < m-1$ for every $u \geq 2$. Since $m_2^A(G) = 2^\alpha - 1$, we have

$$\mu_{2,1}(G,m) \leq \sum_{k \geq m} \frac{2^\alpha}{2^k} = \frac{1}{2^{m-\alpha-1}} \leq 1.$$

Moreover, arguing as in the proof of [99, Lemma 7], we deduce that

$$\mu_{2,2}(G,m) \leq \frac{1}{2^{m-\alpha^*-1}} \leq 1.$$

Notice that if $\alpha = m-1$, then $\alpha^* \leq 1$ and consequently $\mu_{2,2}(G,m) \leq 2^{2-m} \leq 1/4$. Similarly, if $\alpha^* = m-1$, then $\alpha \leq 1$ and $\mu_{2,1}(G,m) \leq 2^{2-m} \leq 1/4$. If follows that $\mu_2(G,m) = \mu_{2,1}(G,m) + \mu_{2,2}(G,m) \leq 5/4$. Except in the case when $n = 9$ and $\alpha_3(G) = 3$, arguing as toward the end of the proof of Lemma 2.1.15, we conclude that

$$\begin{aligned} e(G) &\leq m + \mu_2(G,m) + \mu_3(G,m) + \sum_{p>3} \mu_p(G,m) \\ &\leq m + \frac{5}{4} + \frac{1}{4} + \sum_{p \geq 5} \frac{1}{p(p-1)^2} \leq m + 1.533823. \end{aligned}$$

It remains to deal with the case when G is a soluble subgroup of $\mathrm{Sym}(9)$ with $\alpha_3(G) = 3$. This occurs only if G is contained in the wreath product $\mathrm{Sym}(3) \mathrm{wr} \mathrm{Sym}(3)$. In particular $\alpha_2(G) \leq 3$. If $\alpha_2(G) \leq 2$, then, by Lemma 2.1.4,

$$e(G) \leq 5 + \mu_2(G,5) + \mu_3(G,5) \leq 5 + \frac{1}{4} + \frac{1}{4} = 5.5.$$

We have $\alpha_2(G) = \alpha_3(G) = 3$ only in two cases:

$$\mathrm{Sym}(3) \times \mathrm{Sym}(3) \times \mathrm{Sym}\,3,\ \langle (1,2,3),(4,5,6),(1,4)(2,5)(3,6),(1,2)(4,5)\rangle \times \mathrm{Sym}(3).$$

In this two cases, G contains exactly 16 maximal subgroups, 7 of index 2 and 9 of index 3. But then

$$e(G) \leq 4 + \sum_{k\geq 4} \frac{m_2(G)}{2^k} + \sum_{k\geq 4} \frac{m_3(G)}{3^k} = 4 + \sum_{k\geq 4} \frac{7}{2^k} + \sum_{k\geq 4} \frac{9}{3^k} = 4 + \frac{7}{8} + \frac{1}{6} \sim 5.041667.$$

b) $\alpha_{2,u}(G) = m - 1$ for some $u \geq 2$. In this case $m_2^A(G) \leq 1$, so

$$\mu_{2,1}(G, m+1) \leq \sum_{k\geq m+1} \frac{1}{2^k} = \frac{1}{2^m} \leq \frac{1}{16}.$$

Moreover, by [99, Lemma 5], $m_{2^u}^A(G) \leq 2^{u\alpha_{2,t}(G)+u}$, hence

$$\begin{aligned}\mu_{2,2}(G, m+1) &= \sum_{k\geq m+1} \left(\sum_{n\geq 2} \frac{m_{2^n}^A(G)}{2^{nk}} \right) = \sum_{k\geq m+1} \frac{m_{2^u}^A(G)}{2^{uk}} \leq \sum_{k\geq m+1} \frac{2^{u\alpha_{2,t}(G)+u}}{2^{uk}} \\ &\leq \sum_{k\geq m+1} \frac{2^{um}}{2^{uk}} = \frac{1}{2^u - 1} \leq \frac{1}{3}.\end{aligned}$$

If $p \geq 5$, then $m - \alpha_p(G) \geq 3$ so, by Lemma 2.1.4, $\mu_p(G, m+1) \leq (p(p-1))^{-2}$. Moreover $m - \alpha_3(G) \geq 2$ (notice that there is no subgroup of Sym(9) with $\alpha_3(G) = 3$ and $\alpha_{2,u}(G) = 3$ for some $u \geq 2$), so, again by Lemma 2.1.4, $\mu_3(G, m+1) \leq 1/12$. It follows that

$$\begin{aligned}e(G) &\leq m+1 + \mu_{2,1}(G, m+1) + \mu_{2,2}(G, m+1) + \mu_3(G, m+1) + \sum_{p>3} \mu_p(G, m+1) \\ &\leq m+1+\frac{1}{16}+\frac{1}{3}+\frac{1}{12}+\sum_{p\geq 5} \frac{1}{p^2(p-1)^2} \leq \frac{71}{48}+\sum_{n\geq 5} \frac{1}{n^2(n-1)^2} \leq m+1.484316. \quad \square\end{aligned}$$

When $G \leq \mathrm{Sym}(n)$ and $n \leq 7$, the precise value of $e(G)$ can be computed by **GAP** [53] using the formula (2.0.4). The crucial information is gathered in the following lemma.

Lemma 2.1.17. *Suppose that $G \leq \mathrm{Sym}(n)$ with $n \leq 7$. Either $e(G) \leq \lfloor n/2 \rfloor + 1$ or one of the following cases occurs:*

1. $G \cong \mathrm{Sym}(3)$, $n = 3$, $e(G) = 29/10$;
2. $G \cong C_2 \times C_2$, $n = 4$, $e(G) = 10/3$;
3. $G \cong D_8$, $n = 4$, $e(G) = 10/3$;
4. $G \cong C_2 \times \mathrm{Sym}(3)$, $n = 5$, $e(G) = 1181/330$;
5. $G \cong C_2 \times C_2 \times C_2$, $n = 6$, $e(G) = 94/21$;
6. $G \cong C_2 \times D_8$, $n = 6$, $e(G) = 94/21$;
7. $G \cong C_2 \times C_2 \times \mathrm{Sym}(3)$, $n = 7$, $e(G) = 241789/53130$;
8. $G \cong D_8 \times \mathrm{Sym}(3)$, $n = 7$, $e(G) = 241789/53130$.

Theorem 2.1.18. *Let G be a permutation group of degree $n \neq 3$. If $\alpha_{2,1}(G) = \lfloor n/2 \rfloor$, then $e(G) \leq \lfloor n/2 \rfloor + \nu$, with $\nu \sim 1.606695$.*

Proof. Let $m = \lfloor n/2 \rfloor$. We have that $\alpha_{2,1}(G) = m$ if and only if C_2^m is an epimorphic image of G. If C_2^m is an epimorphic image of G, then, by the main theorem in [**?**], the group G is the direct product of its transitive constituents and each constituent is one of the following: Sym(2), of degree 2, Sym(3), of degree 3, $C_2 \times C_2$, D_8, of degree 4, and the central product $D_8 \circ D_8$, of degree 8. Consequently:

$$G/\operatorname{Frat}(G) \simeq \begin{cases} C_2^m & \text{if } n = 2m, \\ C_2^{m-1} \times \operatorname{Sym}(3) & \text{if } n = 2m+1. \end{cases}$$

And so, by 2.1.1),

$$P_G(k) = P_{G/\operatorname{Frat}(G)}(k) = \prod_{0 \le i \le m-1} \left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{n-2m}.$$

Setting $\eta = 0$ if n is even, $\eta = 1$ otherwise, we have

$$\begin{aligned} e(G) &= \sum_{k \ge 0} (1 - P_G(k)) \le \sum_{k \ge 0} \left(1 - \prod_{0 \le i \le m-1} \left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{\eta}\right) \\ &= m + \sum_{k \ge m} \left(1 - \prod_{0 \le i \le m-1} \left(1 - \frac{2^i}{2^k}\right)\left(1 - \frac{3}{3^k}\right)^{\eta}\right) \\ &= m + \sum_{j \ge 0} \left(1 - \prod_{1 \le l \le m} \left(1 - \frac{1}{2^{j+l}}\right)\left(1 - \frac{3}{3^{j+m}}\right)^{\eta}\right). \end{aligned}$$

Set

$$\omega_{m,\eta} = \sum_{j \ge 0} \left(1 - \prod_{1 \le l \le m} \left(1 - \frac{1}{2^{j+l}}\right)\left(1 - \frac{3}{3^{j+m}}\right)^{\eta}\right).$$

Clearly $\omega_{m,0}$ increase with m. On the other hand, if $m \ge 4$ and $j \ge 0$ then

$$\left(1 - \frac{1}{2^{j+m+1}}\right)\left(1 - \frac{3}{3^{j+m+1}}\right) \le \left(1 - \frac{3}{3^{j+m}}\right)$$

and so $\omega_{m,1} \le \omega_{m+1,1}$ if $m \ge 4$. Moreover

$$\lim_{m \to \infty} \omega_{m,1} = \lim_{m \to \infty} \omega_{m,0} \sim 1.606695.$$

But then $e(G) \le m + 1.606695$ whenever $m \ge 4$. The value of $e(G)$ when n is small is given by the following table (that indicates also how fast $e(G) - m$ tends to 1.606695).

n	$e(G)$
2	2
3	$\frac{29}{10} = 2.900000$
4	$\frac{10}{3} \sim 3.333334$
5	$\frac{1181}{330} \sim 3.578788$
6	$\frac{94}{21} \sim 4.476191$
7	$\frac{241789}{53130} \sim 4.550894$
8	$\frac{194}{35} \sim 5.542857$
9	$\frac{4633553}{832370} \sim 5.566699$
10	$\frac{7134}{1085} \sim 6.575115$
11	$\frac{3227369181}{490265930} \sim 6.582895$
12	$\frac{74126}{9765} \sim 7.590988$
13	$\frac{6399598043131}{842767133670} \sim 7.593554$
14	$\frac{10663922}{1240155} \sim 8.598862$
15	$\frac{70505670417749503}{8198607229768494} \sim 8.599713$

From the information contained in this table, we deduce that $e(G) \leq m + 1.606695$, except when $G = \mathrm{Sym}(3)$. □

Combining Lemmas 2.1.15, 2.1.16, 2.1.17, and Theorem 2.1.18, we obtain the proof of Theorem 2.0.5.

2.2 A probabilistic version of a theorem of Kovács and Sim

2.2.1 Peliminaries

Let G be a soluble group. If M is a maximal subgroup of G, clearly $\mathrm{soc}(M/M_G)$ is a chief factor of G and, being G soluble, it is abelian. Further, M/M_G is a complement of $\mathrm{soc}(M/M_G)$ in G. Let $\mathcal{A}(G)$ be a set of representatives of the irreducible G-modules that are G-isomorphic to some chief factor of G having a complement and, for every $V \in \mathcal{A}(G)$, let $\Sigma_V(G)$ be the set of maximal subgroups M of G with $\mathrm{soc}(G/M_G) \cong_G V$. Recall form Section 1.2 that the V-crown of G, $\mathrm{soc}(G/R_G(V)) = I_G(V)/R_G(V) = C_G(V)/R_G(V)$, is G-isomorphic to a direct product of $\delta_G(V)$ copies of V. Further, we recall that $\delta_G(V)$ (the V-rank of G) coincides with the number of complemented factors in any chief series of G that are G-isomorphic to V. In particular $G/R_G(V) \cong V^{\delta_G(V)} \rtimes H$, with $H \cong G/C_G(V)$. Now, set $q_G(V) = |\operatorname{End}_G V|$, $\epsilon_G(V) = 0$ if V is a trivial G-module, and $\epsilon_G(V) = 1$ otherwise. We have that

$$|\Sigma_V(G)| = \frac{\left(q_G(V)^{\delta_G(V)} - 1\right)|V|^{\epsilon_G(V)}}{q_G(V) - 1} \tag{2.2.1}$$

(see [56]).

For a finite soluble group X, denote by $\Sigma_p(X)$ denotes the set of the maximal subgroups of G whose index is a p-power. Now, let $\mathcal{A}_p(G)$ be the set of the irreducible G-modules $V \in \mathcal{A}(G)$ whose order is a p-power, and let H be a subgroup of G containing a Sylow

p-subgroup of G. We want to compare $\Sigma_p(G)$ and $\Sigma_p(H)$. Fix $V \in \mathcal{A}_p(G)$, let $\delta = \delta_G(V)$, $q = q_G(V)$, $R = R_G(V)$. Moreover set $\overline{G} = G/R$ and $\overline{H} = HR/R$. We have

$$\overline{G} \cong V^\delta \rtimes X \text{ with } X \leq \operatorname{Aut} V.$$

Since $\overline{H}$ contains a Sylow p-subgroup of $\overline{G}$, $V^\delta \leq \overline{H}$ and, by the Dedeking law,

$$\overline{H} = \overline{G} \cap \overline{H} = V^\delta X \cap \overline{H} = V^\delta (X \cap \overline{H}),$$

hence

$$\overline{H} \cong V^\delta \rtimes Y \text{ with } Y = X \cap \overline{H}.$$

Now let U be an irreducible H-module that can be obtained as an H-epimorphic image of V (viewed as an H-module) and define

$$\Omega_U := \{Z \leq_H V \mid V/Z \cong_H U\}, \quad J_U := \bigcap_{Z \in \Omega_U} Z.$$

There exists $t \in \mathbb{N}$ such that $V/J_U \cong_H U^t$ and $\delta^* := \delta_H(U) \geq t \cdot \delta$. Notice that if $Z \in \Omega_U$ and $\alpha \in F = \operatorname{End}_G V$, then $Z^{\alpha h} = Z^{h\alpha} = Z^\alpha$ for every $h \in H$, i.e. $Z^\alpha \leq_H V$. Moreover, if $\alpha \neq 0$, then the map

$$V/Z \to V/Z^\alpha$$
$$v + Z \mapsto v^\alpha + Z^\alpha$$

is an H-isomorphism, so $V/Z \cong_H V/Z^\alpha$ and $Z^\alpha \in \Omega_U$. It follows that J_U is F-invariant and there is a ring homomorphism

$$F \to \operatorname{End}_H(V/J_U) \cong \operatorname{End}_H(U^t) \cong M_{t\times t}(\operatorname{End}_H U).$$

Let $r = |\operatorname{End}_H U|$ and suppose $F^* = \langle a \rangle$. We have that $\langle a \rangle \leq \mathrm{GL}(t, r)$ and this implies $|a| \leq r^t - 1$. In particular

$$q \leq r^t. \tag{2.2.2}$$

Notice that

$$|\Sigma_U(H)| = \frac{r^{\delta^*} - 1}{r - 1}|U|^{\epsilon_U} \geq \frac{r^{t\cdot\delta} - 1}{r - 1}|U|^{\epsilon_U} + \frac{r^b - 1}{r - 1}|U|^{\epsilon_U} \tag{2.2.3}$$

where $b := \delta^* - t \cdot \delta$. Set

$$\mu_V := |\Sigma_V(G)|, \quad \mu_{V,U} := \frac{r^{t\cdot\delta} - 1}{r - 1}|U|^{\epsilon_U}.$$

We have

$$\frac{\mu_V}{|V|} = \frac{(q^\delta - 1)|V|^{\epsilon_V}}{(q - 1)|V|} \leq \frac{q^\delta - 1}{q - 1} \leq q^\delta - 1 \leq r^{\delta\cdot t} - 1 \leq \frac{(r^{t\cdot\delta} - 1)|U|}{r - 1} \leq |U|\mu_{V,U}. \tag{2.2.4}$$

2.2.2 Proof of Theorem 2.0.6

Lemma 2.2.1. *Let G be a finite soluble group, and let $n \geq 2$. Then G has at most n core-free maximal subgroups of index n.*

Proof. We can assume that there exists M a core-free maximal subgroup of G of index n. Hence G is a monolithic primitive group of type I. That is, G has a unique minimal normal subgroup N. Clearly $NM = G$, and since N is abelian and minimal normal in G, then $N \cap M = \{1\}$. Now, the number of core-free maximal subgroups of index n is equal to the number of complements of N in G. Since all core-free maximal subgroups of a primitive soluble group are conjugate ([70, II, 3.2 and 3.3]), the number of complements of N in G is equal to $|G : N_G(M)|$, that is the number of conjugates of M in G. Evidently $|G : N_G(M)| \leq |G : M| = n$, as required.

□

Lemma 2.2.2. *If G is a finite soluble group, then $\mathcal{M}(G) \leq \nu(G) + 2.5$.*

Proof. By [96, Proposition 1.2], there exists a constant γ such that $\mathcal{M}(G) \leq \nu(G)+\gamma$ for every finite group G (see 2.0.7 for the explicit value of γ). From the proof of [96, Proposition 1.2], it turns out that $\gamma \leq b+\log e$, where b must be chosen such that, for every finite group X and every $n \geq 2$, X has at most n^b core-free maximal subgroups of index n. As it is noticed in [96], from Theorem 2.0.9, it is sufficient take $b = 2$. However, by Lemma 2.2.1 every finite soluble group X and every $n \geq 2$, X has at most n core-free maximal subgroups of index n. So in the soluble case, we can take $b = 1$ and consequently $\mathcal{M}(G) \leq \nu(G) + 1 + \log e \leq \nu(G) + 2.5$. □

Proof of Theorem 2.0.6. Set

$$a_G(t) = \sum_{n\geq 2} \frac{m_n(G)}{n^t}, \quad a_{G,p}(t) = \sum_{u\geq 1} \frac{m_{p^u}(G)}{p^{u\cdot t}}, \quad b_p(t) = \sum_{u\geq 1} \frac{m_{p^u}(G_p)}{p^{u\cdot t}}.$$

For every $V \in \mathcal{A}_p(G)$, let $U \in \mathcal{A}_p(G_p)$ be an irreducible G_p-module that can be obtained as a G_p-epimorphic image of V. By 2.2.4), for $t \geq 1$, we have

$$a_{G,p}(t) = \sum_{V\in\mathcal{A}_p(G)} \frac{\mu_V}{|V|^t} \leq \sum_{V\in\mathcal{A}_p(G)} \frac{|U|\mu_{V,U}}{|V|^{t-1}} \leq \sum_{V\in\mathcal{A}_p(G)} \frac{\mu_{V,U}}{|U|^{t-2}} \leq b_p(t-2).$$

By Lemma 2.2.2,

$$\mathcal{M}(G_p) \leq \mathcal{V}(G_p) + \gamma \leq d + 2.5 = c.$$

It follows that

$$\frac{\log(m_{p^u}(G_p))}{\log(p^u)} \leq c,$$

and consequently

$$m_{p^u}(G_p) \leq p^{u\cdot c}.$$

We deduce

$$a_G(t) = \sum_p a_{G,p}(t) \leq \sum_p b_p(t-2) \leq \sum_n \frac{n^c}{n^{t-2}}.$$

It follows that

$$1 - P_G(t) \leq \sum_{M \underset{max}{<} G} \frac{1}{|G:M|^t} \leq \sum_{n\geq 2} \frac{m_n(G)}{n^t} = a_G(t) \leq \sum_{n\geq 2} n^{c+2-t}.$$

Thus, if $t \geq c + 4.02$, we deduce that

$$1 - P_G(t) \leq \sum_{n=2}^{\infty} \frac{1}{n^{2.02}} = \zeta(2.02) - 1$$

which is smaller than $\frac{e-1}{e}$. □

2.2.3 Proof of Theorem 2.0.7

For a real number $\eta \geq 1$, let us define

$$\nu_\eta(G) = \min\left\{ k \in \mathbb{N} \;\middle|\; P_G(k) \geq \frac{1}{\eta} \right\}.$$

The argument used by Lubotzky to bound $\nu(G) = \nu_e(G)$, can be adapted to bound $\nu_\eta(G)$, for an arbitrarily value of η. The proof is essentially the same, but for the sake of clarity, we prefer to give the details.

Lemma 2.2.3. $\nu_\eta(G) \geq \mathcal{M}(G) - b - \log\eta \geq \mathcal{M}(G) - 2 - \log\eta$.

Proof. Let $\{N_i\}$ be an enumeration of all cores of maximal subgroups of G (each core occuring only once). For each N_i choose a maximal subgroup M_i whose core is N_i. Let $C_n(G)$ be the number of the maximal subgroups of index n obtained in this way. The events M_i^k in G^k are pairwise independent and from the quantitative version of the Borel-Cantelli lemma (see appendix A.1), one deduces that

$$\sum_{n=2}^{\infty} C_n(G)n^{-k} \leq \frac{1}{P_k(G)}$$

and in particular,

$$C_n(G) \leq \frac{n^k}{P_k(G)}.$$

Taking $k = \mathcal{V}_\eta(G)$ we get that

$$C_n(G) \leq \eta \cdot n^{\mathcal{V}_\eta(G)}.$$

Now, Theorem 2.0.9 implies that

$$m_n(G) \leq C_n(G)n^b.$$

Hence, $m_n(G) \leq \eta \cdot n^{\mathcal{V}_\eta(G)+b}$. It follows that

$$\mathcal{M}(G) = \sup_{n\geq 2} \frac{\log m_n(G)}{\log n} \leq \mathcal{V}_\eta(G) + b + \log\eta. \quad \square$$

The proof of Theorem 2.0.7 follows combining the following two Lemmas.

Lemma 2.2.4. $\lceil \mathcal{M}(G) \rceil - 4 \leq e(G)$.

Proof. By Lemma 2.2.3, for every positive integer i, we have

$$\mathcal{V}_{2^i}(G) \geq \mathcal{M}(G) - b - \log(2^i) \geq \mathcal{M}(G) - 2 - i.$$

In particular if $k = \lceil \mathcal{M}(G) \rceil - 3 - i$, then $P_G(k) < 2^{-i}$. Let $m = \lceil \mathcal{M}(G) \rceil$. It follows from 2.0.3) that

$$\begin{aligned} e(G) &\geq \sum_{0\leq k\leq m-4} (1 - P_G(k)) \geq \sum_{0\leq k\leq m-4} \left(1 - 2^{k-(m-3)}\right) \\ &= m - 3 - \sum_{1\leq j\leq m-3} 2^{-j} \geq m - 3 - \sum_{j\geq 1} 2^{-j} = m - 4, \quad \square \end{aligned}$$

as required.

Lemma 2.2.5. $e(G) \leq \lceil \mathcal{M}(G) \rceil + 3$.

Proof. Let $m = \lceil \mathcal{M}(G) \rceil$ and $k = m + t$ with t a positive integer. As it is noticed in [97, (11,6)] we have

$$1 - P_G(k) \leq \sum_{n\geq 2} \frac{m_n(G)}{n^k} \leq \sum_{n\geq 2} \frac{n^{\mathcal{M}(G)}}{n^k} \leq \sum_{n\geq 2} \frac{n^m}{n^k} \leq \sum_{n\geq 2} \frac{1}{n^t}.$$

Hence

$$\begin{aligned} e(G) &= \sum_{k\geq 0}(1 - P_G(k)) \leq m + 2 + \sum_{k\geq m+2} (1 - P_G(k)) \\ &\leq m + 2 + \sum_{u\geq 2} \left(\sum_{n\geq 2} n^{-u} \right) = m + 2 + \left(\sum_{n\geq 2} \left(\sum_{u\geq 2} n^{-u} \right) \right) \\ &= m + 2 + \sum_{n\geq 2} \frac{n}{n^2(n-1)} = m + 2 + \left(\sum_{n\geq 1} \frac{1}{n(n+1)} \right) = m + 3. \end{aligned}$$

$\square$

Corollary 2.2.6. *If G is a finite soluble group, then*

$$\lceil \mathcal{M}(G) \rceil - 3 \leq e(G) \leq \lceil \mathcal{M}(G) \rceil + 3.$$

Proof. By Lemma 2.2.1, in Lemma 2.2.4, we are allowed to take $b = 1$. □

2.2.4 Proof of Theorem 2.0.8

Lemma 2.2.7. *Let G be a finite soluble group. There exists a prime divisor p of the order of G and a positive integer a such that $m_{p^a}(G) = p^{a \cdot \mathcal{M}(G)}$. If H is a subgroup of G containing a Sylow p-subgroup of G, then $\mathcal{M}(G) \leq \mathcal{M}(H) + 3$.*

Proof. Let $m = \mathcal{M}(G)$. Since the maximal subgroups of G have prime-power indices, there exists a prime divisor p of the order of G and a positive integer a such that $m_{p^a}(G) = p^{a \cdot m}$. Let H be a subgroup of G containing a Sylow p-subgroup of G and let $\mu = \mathcal{M}(H)$. It follows from 2.2.4 that

$$p^{a \cdot m} = m_{p^a}(G) \leq \sum_{b \leq a} p^{a+b} m_{p^b}(H) \leq \sum_{b \leq a} p^{a+b} p^{b \cdot \mu} \leq p^{3 \cdot a + \mu \cdot a},$$

hence $m \leq 3 + \mu$. □

Proof of Theorem 2.0.8. By Lemma 2.2.7, there exists a prime divisor p of G, such that $\mathcal{M}(G) \leq \mathcal{M}(G_p) + 3$. But then we deduce from Corollary 2.2.6, that $e(G) \leq \lceil \mathcal{M}(G) \rceil + 3 \leq \lceil \mathcal{M}(G_p) \rceil + 6 \leq e(G_p) + 9$. □

2.2.5 Proof of Proposition 2.0.10

Let $h = d_2(G)$ be the smallest cardinaly of a (topologically) generating set of a 2-Sylow subgroup of G. By Lemma 2.1.1(3) (indeed a consequence of the Tate's p-nilpotency criterion [70, page 431]), for every open normal subgroup N of G, a chief series of G/N contains at most $h-1$ non-abelian factors. This implies that G is virtually pro-soluble, and consequently G is PFG by [114, Theorem 10]. This concludes our proof.

2.3 Comparing the expected number of random elements from the symmetric and the alternating groups needed to generate a transitive subgroup

2.3.1 Preliminaries

Let $\Lambda = (X, \leq)$ be a finite poset. Recall that the Möbius function μ_Λ on the poset Λ is the unique function $\mu_\Lambda : X \times X \to \mathbb{Z}$, satisfying $\mu(x, y) = 0$ unless $x \leq y$ and the recursion formula

$$\sum_{x \leq y \leq z} \mu_\Lambda(y, z) = \begin{cases} 1 & \text{if } x = z, \\ 0 & \text{otherwise.} \end{cases}$$

Let $G \leq \mathrm{Sym}(n)$. Recall that, if $x = (x_m)_{m \in \mathbb{N}}$ is a sequence of independent, uniformly distributed G-valued random variables, then

$$\tau_{G,n} = \min\{t \geq 1 | \langle x_1, \ldots, x_t \rangle \text{ is a transitive subgroup of } G\} \in [0, +\infty].$$

Notice that $\tau_{G,n} > t$ if and only if $\langle x_1, \dots, x_t \rangle$ is not a transitive subgroup of G, so we have that

$$P(\tau_{G,n} > t) = 1 - P_{\mathcal{T}}(G, t).$$

Recalling that $e_{\mathcal{T}}(G)$ is the expectation of the random variable $\tau_{G,n}$, we get that

$$\begin{aligned} e_{\mathcal{T}}(G) &= \sum_{t \geq 1} tP(\tau_{G,n} = t) = \sum_{t \geq 1} \left(\sum_{m \geq t} P(\tau_{G,n} = m) \right) \\ &= \sum_{t \geq 1} P(\tau_{G,n} \geq t) = \sum_{t \geq 0} P(\tau_{G,n} > t) = \sum_{t \geq 0} (1 - P_{\mathcal{T}}(G, t)). \end{aligned} \tag{2.3.1}$$

Let $\mathcal{X}_G$ be the set of intransitive subgroups of G, let $\mathcal{I}_G$ be the set of subgroups of G that can be obtained as the intersection of maximal element in the poset $\mathcal{X}_G$, and let $\mathcal{J}_G = \mathcal{I}_G \cup \{G\}$. In [46] it was proved that

$$P_{\mathcal{T}}(G, t) = \sum_{H \in \mathcal{J}_G} \frac{\mu_{\mathcal{T},G}(H, G)}{|G : H|^t},$$

where $\mu_{\mathcal{T},G}$ denotes the Möbius function on the lattice $\mathcal{L}_{\mathcal{T}}(G) = \mathcal{X}_G \cup \{G\}$. So, in order to compute the function $P_{\mathcal{T}}(G, t)$ it is necessary to have information about the subgroups in $\mathcal{J}_G$. Let $\mathcal{P}_n$ be the poset of partitions of $\{1, \dots, n\}$ ordered by refinement. The maximum $\hat{1}$ of $\mathcal{P}_n$ is $\{\{1, \dots, n\}\}$ and the minimum $\hat{0}$ is $\{\{1\}, \dots, \{n\}\}$. The orbit lattice of G is defined as follows

$$\mathcal{P}_n(G) = \{\sigma \in \mathcal{P}_n \mid \text{the orbits of some } H \leq G \text{ are the parts of } \sigma\}.$$

If $\sigma = \{\Omega_1, \dots, \Omega_k\} \in \mathcal{P}_n$, then we define

$$G(\sigma) = (\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_k)) \cap G.$$

If $\sigma \in \mathcal{P}_n(G)$, then $G(\sigma)$ is the maximal element in the lattice of those subgroups of G whose orbits are precisely the parts of σ. Notice that $H \in \mathcal{J}_G$ if and only if there exists $\sigma \in \mathcal{P}_n(G)$ with $H = G(\sigma)$; moreover $\mu_{\mathcal{X}}(G(\sigma), G) = \mu_{\mathcal{P}_n(G)}(\sigma, \hat{1})$, so

$$P_{\mathcal{T}}(G, t) = \sum_{\sigma \in \mathcal{P}_n(G)} \frac{\mu_{\mathcal{P}_n(G)}(\sigma, \hat{1})}{|G : G(\sigma)|^t}. \tag{2.3.2}$$

2.3.2 Proof of Theorem 2.0.11

From now on, we assume $n \geq 3$, we let $\mathcal{P}_{2,n}$ be the subset of $\mathcal{P}_n$ consisting of the partitions of $\{1, \dots, n\}$ into $n-1$ parts (one of size 2, the others of size 1) and we let $\mathcal{P}^*_{2,n} = \mathcal{P}_{2,n} \cup \{\hat{0}\}$. The following two lemmas are immediate but crucial in our computation.

Lemma 2.3.1. *$\mathcal{P}_n(\mathrm{Sym}(n)) = \mathcal{P}_n$ and $\mathcal{P}_n(\mathrm{Alt}(n)) = \mathcal{P}_n \setminus \mathcal{P}_{2,n}$.*

Lemma 2.3.2. *If $\sigma \in \mathcal{P}_n \setminus \mathcal{P}^*_{2,n}$, then*

1. *$\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\sigma, \hat{1}) = \mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\sigma, \hat{1}) = \mu_{\mathcal{P}_n}(\sigma, \hat{1})$;*
2. *$|\mathrm{Sym}(n) : \mathrm{Sym}(n)(\sigma)| = |\mathrm{Alt}(n) : \mathrm{Alt}(n)(\sigma)|$.*

Lemma 2.3.3. *We have*

1. *$\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\hat{0}, \hat{1}) = (-1)^{n-1}(n-1)!$;*

2. $\mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\hat{0},\hat{1}) = (-1)^{n-1}(n-1)! + \frac{(-1)^{n-2}n!}{2}$.

Proof. We use the following known result (see for example [155], p. 128):

$$\mu_{\mathcal{P}_n}(\{\Omega_1,\dots,\Omega_k\},\hat{1}) = (-1)^{k-1}(k-1)!. \tag{2.3.3}$$

This immediately implies $\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\hat{0},\hat{1}) = \mu_{\mathcal{P}_n}(\hat{0},\hat{1}) = (-1)^{n-1}(n-1)!$. Moreover

$$\begin{aligned}
\mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\hat{0},\hat{1}) =& -\sum_{\sigma\in\mathcal{P}_n(\mathrm{Alt}(n))\setminus\{\hat{0}\}} \mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\sigma,\hat{1}) = -\sum_{\sigma\in\mathcal{P}_n\setminus\mathcal{P}^*_{2,n}} \mu_{\mathcal{P}_n}(\sigma,\hat{1})\\
=& -\sum_{\sigma\in\mathcal{P}_n\setminus\{\hat{0}\}} \mu_{\mathcal{P}_n}(\sigma,\hat{1}) + \sum_{\sigma\in\mathcal{P}_{2,n}} \mu_{\mathcal{P}_n}(\sigma,\hat{1})\\
=&\mu_{\mathcal{P}_n}(\hat{0},\hat{1}) + \sum_{\sigma\in\mathcal{P}_{2,n}} \mu_{\mathcal{P}_n}(\sigma,\hat{1})\\
=&(-1)^{n-1}(n-1)! + \binom{n}{n-2}(-1)^{n-2}(n-2)!\\
=&(-1)^{n-1}(n-1)! + \frac{(-1)^{n-2}n!}{2}. \quad \square
\end{aligned}$$

Proof of 2.0.11) in Theorem 2.0.11. For every $t\in\mathbb{N}$, let

$$\begin{aligned}
\eta_1(n,t) &= \sum_{\sigma\in\mathcal{P}_{2,n}} \frac{\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\sigma,\hat{1})}{|\operatorname{Sym}(n):\operatorname{Sym}(n)(\sigma)|^t} = \binom{n}{2}\frac{(-1)^{n-2}(n-2)!2^t}{(n!)^t} = \frac{(-1)^{n-2}(n!)2^t}{2(n!)^t},\\
\eta_2(n,t) &= \frac{\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\hat{0},\hat{1})}{|\operatorname{Sym}(n):\operatorname{Sym}(n)(\hat{0})|^t} = \frac{(-1)^{n-1}(n-1)!}{(n!)^t},\\
\eta_3(n,t) &= \frac{\mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\hat{0},\hat{1})}{|\operatorname{Alt}(n):\operatorname{Alt}(n)(\hat{0})|^t} = \left((-1)^{n-1}(n-1)! + \frac{(-1)^{n-2}n!}{2}\right)\left(\frac{2}{n!}\right)^t.
\end{aligned}$$

Note that to compute the values of η_1,η_2,η_3 we used 2.3.3) and Lemma 2.5.7.

From 2.3.2), Lemma 2.3.1 and Lemma 2.3.2, we deduce that

$$\begin{aligned}
P_{\mathcal{T}}(\mathrm{Sym}(n),t) =& \sum_{\sigma\in\mathcal{P}_n(\mathrm{Sym}(n))} \frac{\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\sigma,\hat{1})}{|\operatorname{Sym}(n):\operatorname{Sym}(n)(\sigma)|^t}\\
=& \sum_{\sigma\in\mathcal{P}_n(\mathrm{Alt}(n))} \frac{\mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\sigma,\hat{1})}{|\operatorname{Alt}(n):\operatorname{Alt}(n)(\sigma)|^t} + \sum_{\sigma\in\mathcal{P}_{2,n}(\mathrm{Sym}(n))} \frac{\mu_{\mathcal{P}_n}(\sigma,\hat{1})}{|\operatorname{Sym}(n):\operatorname{Sym}(n)(\sigma)|^t}\\
&+ \frac{\mu_{\mathcal{P}_n(\mathrm{Sym}(n))}(\hat{0},\hat{1})}{|\operatorname{Sym}(n):\operatorname{Sym}(n)(\hat{0})|^t} - \frac{\mu_{\mathcal{P}_n(\mathrm{Alt}(n))}(\hat{0},\hat{1})}{|\operatorname{Alt}(n):\operatorname{Alt}(n)(\hat{0})|^t}\\
=& P_{\mathcal{T}}(\mathrm{Alt}(n),t) + \eta_1(n,t) + \eta_2(n,t) - \eta_3(n,t)\\
=& P_{\mathcal{T}}(\mathrm{Alt}(n),t) + \frac{(-1)^n(n-1)!(2^t-1)}{(n!)^t}. \quad \square
\end{aligned}$$

Proof of 2.0.11) in Theorem 2.0.11. Using equation 2.3.1) we obtain that

$$\begin{aligned} e_{\mathcal{T}}(\mathrm{Sym}(n)) - e_{\mathcal{T}}(\mathrm{Alt}(n)) &= \sum_{t\geq 0} (P_{\mathcal{T}}(\mathrm{Alt}(n),t) - P_{\mathcal{T}}(\mathrm{Sym}(n),t)) \\ &= \sum_{t\geq 0} \frac{(-1)^{n+1}(n-1)!(2^t-1)}{(n!)^t} \\ &= (-1)^{n+1}(n-1)! \left(\sum_{t\geq 0} \left(\frac{2}{n!}\right)^t - \sum_{t\geq 0} \left(\frac{1}{n!}\right)^t \right) \\ &= (-1)^{n+1}(n-1)! \left(\frac{n!}{n!-2} - \frac{n!}{n!-1} \right) \\ &= \frac{(-1)^{n+1} n!(n-1)!}{(n!-1)(n!-2)}. \end{aligned}$$

□

2.3.3 Proof of Theorem 2.0.12

Lemma 2.3.4. *Let $\epsilon = 0$ if n is even, $\epsilon = 1$ if n is odd. Then*

$$e_{\mathcal{T}}(\mathrm{Alt}(n)) \leq 2 - \frac{2\epsilon}{n} + \frac{1}{n-1} + \frac{2}{n(n-1)-2} + \frac{3n}{n(n-1)(n-2)-6}.$$

Proof. Since an element of $\mathrm{Alt}(n)$ generates a transitive subgroup if and only if it is a cycle of length n, we have that $P_{\mathcal{T}}(\mathrm{Alt}(n),1) = 2\epsilon/n$. Now, let $t \geq 2$ and let $Y = \langle x_1 \ldots, x_t \rangle \leq \mathrm{Alt}(n)$. If Y is contained in an intransitive maximal subgroup, then Y is contained in a subgroup conjugate to $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$ for some $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$. Let $k \in \{1, \ldots, n-1\}$. The probability that Y is contained in a subgroup conjugate to $\mathrm{Sym}(k) \times \mathrm{Sym}(n-k)$ is bounded by $\binom{n}{k}^{1-t}$. So

$$1 - P_{\mathcal{T}}(\mathrm{Alt}(n),t) \leq \sum_{1\leq k\leq \lfloor \frac{n-1}{2} \rfloor} \binom{n}{k}^{1-t}.$$

Notice that

$$\sum_{3\leq k\leq \lfloor \frac{n-1}{2} \rfloor} \binom{n}{k}^{1-t} \leq \frac{n}{2} \binom{n}{3}^{1-t}.$$

Hence

$$\begin{aligned} e_{\mathcal{T}}(\mathrm{Alt}(n)) &= \sum_{t\geq 0} (1 - P_{\mathcal{T}}(\mathrm{Alt}(n),t)) \\ &= (1 - P_{\mathcal{T}}(\mathrm{Alt}(n),0)) + (1 - P_{\mathcal{T}}(\mathrm{Alt}(n),1)) + \sum_{t\geq 2} (1 - P_{\mathcal{T}}(\mathrm{Alt}(n),t)) \\ &\leq 2 - \frac{2\epsilon}{n} + \sum_{t\geq 2} \left(n^{1-t} + \binom{n}{2}^{1-t} + \frac{n}{2} \binom{n}{3}^{1-t} \right) \\ &= 2 - \frac{2\epsilon}{n} + \frac{1}{n-1} + \frac{1}{\binom{n}{2}-1} + \frac{n}{2} \frac{1}{\binom{n}{3}-1} \\ &= 2 - \frac{2\epsilon}{n} + \frac{1}{n-1} + \frac{2}{n(n-1)-2} + \frac{3n}{n(n-1)(n-2)-6}. \end{aligned}$$

□

Proof of Theorem 2.0.12. Let

$$f(n) = \frac{(-1)^{n+1} n!(n-1)!}{(n!-1)(n!-2)}.$$

In [109, Section 5] it has been proved that $\lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Sym}(n)) = 2$. This implies

$$\lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Alt}(n)) = \lim_{n\to\infty}(e_{\mathcal{T}}(\mathrm{Sym}(n)) - f(n)) = \lim_{n\to\infty} e_{\mathcal{T}}(\mathrm{Sym}(n)) - \lim_{n\to\infty} f(n) = 2.$$

Moreover, again by [109, Section 5], if $n \geq 2$, then

$$2 \leq e_{\mathcal{T}}(\mathrm{Sym}(n)) \leq e_{\mathcal{T}}(\mathrm{Sym}(4)) \sim 2.1033. \tag{2.3.4}$$

The values of $e_{\mathcal{T}}(\mathrm{Alt}(n))$ and $e_{\mathcal{T}}(\mathrm{Sym}(n))$ when $n \in \{3, 4\}$ have been discussed in the introduction. So we may assume $n \geq 5$. Notice that $|f(n)|$ is a decreasing function and that $f(n) < 0$ if n is even, $f(n) > 0$ otherwise.

Assume that n is even:

$$e_{\mathcal{T}}(\mathrm{Alt}(n)) = e_{\mathcal{T}}(\mathrm{Sym}(n)) - f(n) \geq 2 - f(n) > 2,$$
$$e_{\mathcal{T}}(\mathrm{Alt}(n)) = e_{\mathcal{T}}(\mathrm{Sym}(n)) - f(n) \leq e_{\mathcal{T}}(\mathrm{Sym}(4)) - f(4) = e_{\mathcal{T}}(\mathrm{Alt}(4)).$$

Assume that n is odd: it follows immediately from Lemma 2.3.4, that $e_{\mathcal{T}}(\mathrm{Alt}(n)) < 2$ if $n \geq 9$. Moreover

$$e_{\mathcal{T}}(\mathrm{Alt}(5)) = \frac{2205085}{1170324} \sim 1.8842,\ e_{\mathcal{T}}(\mathrm{Alt}(7)) = \frac{1493015628619946854486}{779316363245447358045} \sim 1.9158.$$

Finally

$$e_{\mathcal{T}}(\mathrm{Alt}(n)) = e_{\mathcal{T}}(\mathrm{Sym}(n)) - f(n) \geq 2 - f(5) \geq 2 - \frac{1440}{7021} > \frac{3}{2} = e_{\mathcal{T}}(\mathrm{Alt}(3)). \quad \square$$

2.4 Maximal size of independent generating sets of finite groups

Proposition 2.4.1. *Let G is a finite nilpotent group. Then $m(G) = \sum_{p\in\pi(G)} d_p(G)$*

Proof. Since G is a finite nilpotent group, then $G = P_1 \times \cdots \times P_t$ where $P_1, \ldots, P_t$ are the Sylow subgroups of G. Since P_i is a p_i-group and from [1] $m(P_i) = d(P_i)$, the result follows from the fact $m(G) = m(P_1) + \cdots + m(P_t)$ (see [105]). $\square$

Proof of Theorem 2.0.13. In [104], it is proved that $m(G) = \sum_{p\in\pi(G)} \alpha_p(G)$, where $\alpha_p(G)$ is defined according with the notation of Subsection 2.1.1, Now, Lemma 2.1.1 yields $\alpha_p(G) \leq d_p(G)$. Therefore $m(G) \leq \sum_{p\in\pi(G)} d_p(G) = \delta(G)$. $\square$

2.4.1 A result on the order of a finite simple group

Theorem 2.4.2. *Let S be a simple group of Lie type. There exist two different primes dividing $|S|$ but not $|\mathrm{Out}(S)|$.*

Proof. Let $S = L(q)$ be a simple group of Lie type defined over the field with q elements, where $q = p^t$ and p is a prime number. From Burnside's theorem, $|\pi(S)| \geq 3$. From [67], if $|\pi(S)| = 3$, then

$$S \in \{A_1(5), A_1(7), A_1(8), A_1(17), A_2(9), A_2(3), {}^2A_2(3), {}^2A_3(2)\},$$

and for these groups the theorem holds by a direct inspection. Therefore, for the rest of the proof we may suppose

$$|\pi(S)| \geq 4. \tag{2.4.1}$$

In particular, the result immediately follows when $|\pi(\mathrm{Out}(S))| \leq 2$ and hence we may suppose $|\pi(\mathrm{Out}(S))| \geq 3$.

The order of $L(q)$ has the cyclotomic factorization in terms of q :

$$|L(q)| = \frac{1}{d} q^h \prod_{m \in \Lambda} \Phi_m(q)^{r_m},$$

where $\Phi_m(q)$ is the m-th cyclotomic polynomial and Λ, d, h and r_m are listed in Tables L.1, C.1 and C.2 of [81].

Suppose that $S \neq D_4(q)$ and that S is untwisted. From [143, page 207], if $l \geq 2$ and $m \geq 1$ are integers such that $l_{m \cdot t}$ is a primitive prime divisor of $(l^t)^m - 1$, then $l_{m \cdot t}$ divides $\Phi_m(l^t)$. From this and from Zsigmondy's theorem, we conclude that, except for the six cases listed below, there exist $i, j \in \Lambda$ with $2 \leq i < j$ such that $x := p_{i \cdot t}$ and $y := p_{j \cdot t}$ are distinct primitive prime divisors. In particular, x and y are odd divisors of $|S|$ and are relatively prime to $q - 1$ because $i \geq 2$. Moreover, by Lemma 1.3.3, $x \equiv y \equiv 1 \mod t$ and hence x and y are relatively prime to t. In particular, x and y are our required primes. (The case $S = D_4(q)$ is special in this argument because 3 is (potentially) an odd prime divisor of $|\mathrm{Out}(S)|$ not arising from field automorphisms.)

We are going to analyze the groups for which the existence of x and y is not ensured from the previous argument.

1. $S = A_2(q)$ and q is a Mersenne prime: in this case $|\mathrm{Out}(S)| = 2 \cdot (q - 1, 3)$ is divisible by at most 2 different primes, contradicting $|\pi(\mathrm{Out}(S))| \geq 3$.

2. $S = A_2(4)$: in this case 5 and 7 are the required primes.

3. $S = A_1(q)$: we may assume $t \geq 5$, otherwise $|\pi(\mathrm{Out}S)| \leq 2$. Now, the existence of $x = p_t$ and $y = p_{2 \cdot t}$ is ensured by Zsigmondy's Theorem.

4. $S = B_2(q)$ with q a Mersenne prime: in this case $|\pi(\mathrm{Out}(S))| = 1$, a contradiction.

5. $S = B_2(8)$: in this case 5 and 7 are the requested primes.

6. $S = G_2(q)$ with q a Mersenne prime: in this case $|\pi(\mathrm{Out}(S))| \leq 2$, a contradiction.

It remains to deal with the case $S = D_4(q)$ and with the twisted groups of Lie type.

Suppose $S = D_4(q)$. Since 3 divides $|\mathrm{Out}(S)|$, the previous argument fails exactly when the primitive prime divisor x or y is 3. The existence of $x = p_{2 \cdot t}$, $y = p_{4 \cdot t}$ and $z = p_{6 \cdot t}$ is ensured when $q \notin \{2, 8\}$ and when q is not a Mersenne prime. When $q = 2$, the result follows since $|\mathrm{Out}(S)| = 6$; when $q = 8$, we have that $t = 3$ does not divide y and z; therefore y and z are prime numbers satisfying our statement . When q is a Mersenne prime, if $q \neq 3$, then q and z are prime numbers satisfying our statement; if $q = 3$, then 5 and 7 are prime numbers satisfying our statement.

Assume $S \in \{{}^2B_2(q), {}^2G_2(q), {}^2F_4(q)\}$. In these cases we have $|\mathrm{Out}(S)| = t$, so we may assume that t is not a prime. Since the existence of $x = p_{i \cdot t}$ and $y = p_{j \cdot t}$ is ensured by Zsigmondy's Theorem, for two different elements i and j of Λ, we are done.

If $S = {}^3D_4(q)$ and $q \notin \{2, 8\}$ and q is not a Mersenne prime, then we can take $x = p_{2 \cdot t}$ and $y = p_{6 \cdot t}$ (notice that $|\mathrm{Out}\, S|$ divides $3 \cdot t$). When $q = 2$ or $q = 8$ or q is a Mersenne prime, then $|\mathrm{Out}(S)|$ is divisible only by 3, against our assumption.

If $S = {}^2E_6(q)$, then we can take $x = p_{8 \cdot t}$ and $y = p_{12 \cdot t}$ (notice that $|\mathrm{Out}(S)|$ divides $6 \cdot t$).

If $S = {}^2D_n(q)$, then $|\mathrm{Out}(S)|$ divides $8 \cdot t$. So, when $q = 2$ or when q is a Mersenne prime, the result holds since $|\mathrm{Out}(S)|$ has only one prime divisor. For the remaining cases, we can take $x = p_{4 \cdot t}$ and $y = p_{6 \cdot t}$.

Finally assume$S = {}^2A_n(q)$. In this case $|\mathrm{Out}(S)| = 2 \cdot t \cdot (n+1, q+1)$. If $n \geq 3$ and $q \neq 2$, then we can take $x = p_{4 \cdot t}$ and $y = p_{6 \cdot t}$. When $q = 2$, we have $|\pi(\mathrm{Out}({}^2A_n(2)))| \leq 2$, which is a contradiction. We remain with the case $S = {}^2A_2(q)$. The group $S = {}^2A_2(3)$ was already analyzed, so we can suppose $q \geq 4$. Now $|\mathrm{Out}(S)| = 2 \cdot t \cdot (3, q+1)$, so we may assume $t \neq 1$.

If $(3, q+1) = 1$, we may assume $t \neq 2$ and we can take $x = p_{2\cdot t}$ and $y = p_{6\cdot t}$. Otherwise $(3, q+1) = 3$, so $(3, q-1) = 1$ and in particular $x = p_t \neq 3$. It follows that $x = p_t$ and $y = p_{6\cdot t}$ are the prime we are interested in. □

2.4.2 An auxiliary result

Lemma 2.4.3. *Let Q be a p-group, let P be a permutation p-group with domain Δ and let $n_\Delta(P)$ be the number of orbits of P on Δ. Then*

$$d(Q\mathrm{wr}_\Delta P) = d(P) + n_\Delta(P)d(Q).$$

Proof. Let $\Delta_1, \ldots, \Delta_\ell$ be the orbits of P on Δ.

Replacing Q by $Q/\operatorname{Frat}(Q)$ if necessary, we may suppose that Q is an elementary abelian p-group. Let B be the base group of the wreath product $W := Q\mathrm{wr}_\Delta P$.

Using the fact that B is an abelian normal subgroup of W and standard commutator computations, we get $[W, W] = [B, P][P, P]$. Given $\sigma \in P$ and $f \in B$, we have

$$\begin{aligned}(\sigma f)^p &= \sigma^p f^{\sigma^{p-1}} f^{\sigma^{p-2}} \cdots f^\sigma f \\ &= \sigma^p (f^{\sigma^{p-1}} f^{-1})(f^{\sigma^{p-2}} f^{-1}) \cdots (f^\sigma f^{-1}) \in P^p[B, P]\end{aligned}$$

and hence

$$\operatorname{Frat}(W) = [B, P] \operatorname{Frat}(P). \tag{2.4.2}$$

Consider V, the subspace of B consisting of all functions $g : \Delta \to Q$ with

$$\prod_{\delta \in \Delta_i} g(\delta) = 1, \text{ for every } i \in \{1, \ldots, \ell\}.$$

Given $f \in B$, $\sigma \in P$ and $i \in \{1, \ldots, \ell\}$, we have

$$\begin{aligned}\prod_{\delta \in \Delta_i} [f, \sigma](\delta) &= \prod_{\delta \in \Delta_i} (f^\sigma f^{-1})(\delta) = \prod_{\delta \in \Delta_i} f(\delta^{\sigma^{-1}}) f(\delta)^{-1} = \prod_{\delta \in \Delta_i} f(\delta^{\sigma^{-1}}) \prod_{\delta \in \Delta_i} f(\delta)^{-1} \\ &= \left(\prod_{\delta \in \Delta_i} f(\delta) \right) \left(\prod_{\delta \in \Delta_i} f(\delta) \right)^{-1} = 1.\end{aligned}$$

Hence, $[B, P] \leq V$. For each $i \in \{1, \ldots, \ell\}$, fix $\bar{\delta}_i \in \Delta_i$ and let $g \in V$. For every $i \in \{1, \ldots, \ell\}$ and $\delta \in \Delta_i \setminus \{\bar{\delta}_i\}$, we let $f_\delta : \Delta \to Q$ and $h_\delta : \Delta \to Q$ be the mappings defined by

$$f_\delta(\delta') = \begin{cases} g(\delta) & \text{if } \delta' = \delta, \\ g(\delta)^{-1} & \text{if } \delta' = \bar{\delta}_i, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta, \bar{\delta}_i\}, \end{cases} \qquad h_\delta(\delta') = \begin{cases} g(\delta)^{-1} & \text{if } \delta' = \delta, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta\}. \end{cases}$$

Since $g \in V$, with a computation, we obtain

$$g = \prod_{\delta \in \Delta \setminus \{\bar{\delta}_1, \ldots, \bar{\delta}_\ell\}} f_\delta.$$

For each $i \in \{1, \ldots, \ell\}$ and $\delta \in \Delta_i \setminus \{\bar{\delta}_i\}$, since δ and $\bar{\delta}_i$ are in the same P-orbit, there exists $\sigma \in P$ with $\delta^\sigma = \bar{\delta}_i$. For each $\delta' \in \Delta$, we have

$$[h_\delta, \sigma](\delta') = h_\delta^{-1}(\delta') h_\delta^\sigma(\delta') = h_\delta(\delta')^{-1} h_\delta(\delta'^{\sigma^{-1}}) = \begin{cases} g(\delta) & \text{if } \delta' = \delta, \\ g(\delta)^{-1} & \text{if } \delta' = \bar{\delta}_i, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta, \bar{\delta}_i\}. \end{cases}$$

It follows $f_\delta = [h_\delta, \sigma] \in [B, P]$ and hence $g \in [B, P]$. So, $V \leq [B, P]$. Therefore

$$V = [B, P]. \tag{2.4.3}$$

From (2.4.2), (2.4.3) and from the fact that $|B : V| = |Q|^\ell$, we obtain

$$\begin{aligned} |W : \mathrm{Frat}(W)| &= |BP : V\,\mathrm{Frat}(P)| = |P : \mathrm{Frat}(P)||B : V| = p^{d(P)}|Q|^\ell \\ &= p^{d(P)}p^{d(Q)\ell} = p^{d(P)+n_\Delta(P)d(Q)}. \end{aligned}$$

□

Given a permutation group X on Ω and $\omega \in \Omega$, we let $X_\omega := \{x \in X \mid \omega^x = \omega\}$ the stabilizer of ω in X. Let K be a transitive permutation group on a set Ω and let $\omega \in \Omega$. We define $t_\Omega(K)$ to be the maximum number $t \in \mathbb{N}$ of subgroups $U_1, \ldots, U_t$ of K with

1. $K_\omega = U_1 \cap \cdots \cap U_t$, and
2. $K_\omega \neq \bigcap_{j\in J} U_j$, for each proper subset J of $\{1, \ldots, t\}$.

When (1) and (2) are satisfied (even if t is not necessarily the maximum), we say that $U_1, \ldots, U_t$ are *independent* subgroups of K. Moreover, let S be a finite non-abelian simple group and let us denote by $\pi^*(S)$ the set of primes dividing $|S|$ but not $|\mathrm{Out}(S)|$.

Theorem 2.4.4. *Let K be a transitive permutation group on Ω, let S be a non-abelian simple group and let G be a group with $S\mathrm{wr}_\Omega K \leq G \leq (\mathrm{Aut}\, S)\mathrm{wr}_\Omega K$. Then*

$$\sum_{p\in\pi^*(S)} d_p(G) > t_\Omega(K).$$

Proof. For every $p \in \pi^*(S)$, we have $d_p(G) = d_p(S\mathrm{wr}_\Omega K)$ and hence, without loss of generality, we may assume $G = S\mathrm{wr}_\Omega K$. For simplicity, we write

$$f(S, \Omega, K) := \sum_{p\in\pi^*(S)} d_p(G).$$

We argue by induction on $t := t_\Omega(K)$. When $t = 1$, from Theorem 2.4.2 we deduce

$$f(S, \Omega, K) \geq \pi^*(S) \geq 2 > 1 = t.$$

Suppose then $t > 1$. Let $\omega \in \Omega$ and let $U_1, \ldots, U_t$ be t independent subgroups of K with

$$\bigcap_{i=1}^{t} U_i = K_\omega.$$

For each $i \in \{1, \ldots, t\}$, we define

$\bar{U}_i$ to be the intersection $\bigcap_{j\in\{1,\ldots,t\}\setminus\{i\}} U_j$; (as $K_\omega \leq \bar{U}_i$, the orbit $\omega^{\bar{U}_i} := \{\omega^x \mid x \in \bar{U}_i\}$ is a block of imprimitivity for the action of K on Ω.)

Ω_i to be the system of imprimitivity determined by the block of imprimitivity $\omega^{\bar{U}_i}$;

$\hat{K}_i$ to be the permutation group induced by K on Ω_i; (we also denote by $\sigma_i : K \to \hat{K}_i$ the natural projection, so $\hat{K}_i = \sigma_i(K)$.)

G_i to be the wreath product $G_i := S\mathrm{wr}_{\Omega_i}\hat{K}_i$.

Let $i \in \{1,\dots,t\}$. Since the point stabilizer $\sigma_i(\bar{U}_i)$ of $\omega^{\bar{U}_i} \in \Omega_i$ in $\hat{K}_i$ is defined as the intersection of the $t-1$ independent subgroups $\{\sigma_i(U_j) \mid j \in \{1,\dots,t\} \setminus \{i\}\}$, we have $t_{\Omega_i}(\hat{K}_i) \geq t-1$. Moreover, from our inductive argument, we have

$$\sum_{p\in\pi^*(S)} d_p(G_i) = f(S,\Omega_i,\hat{K}_i) > t_{\Omega_i}(\hat{K}_i) \geq t-1. \tag{2.4.4}$$

For each prime $p \in \pi^*(S)$, let Π_p be a Sylow p-subgroup of S and let P be a Sylow p-subgroup of K. In particular, $\hat{P}_i := \sigma_i(P)$ is a Sylow p-subgroup of $\hat{K}_i$. From Lemma 3.3.7, for every $i \in \{1,\dots,t\}$, we have

$$f(S,\Omega_i,\hat{K}_i) = \sum_{p\in\pi^*(S)} (d(\hat{P}_i) + n_{\Omega_i}(\hat{P}_i)d(\Pi_p)), \tag{2.4.5}$$

where $n_{\Omega_i}(\hat{P}_i) = n_{\Omega_i}(P)$ denotes the number of orbits of P on Ω_i. Observe that $d(P) \geq d(\hat{P}_i)$.

In particular, using (2.4.4) and (2.4.5), we deduce

$$f(S,\Omega,K) > t,$$

unless, for each $i \in \{1,\dots,t\}$ and for each $p \in \pi^*(S)$,

(a) $d(P) = d(\hat{P}_i)$,

(b) $n_\Omega(P) = n_{\Omega_i}(P)$.

In particular, for the rest of the proof we may assume that **(a)** and **(b)** hold.

Since $|\pi^*(S)| \geq 2$, we may choose $p \in \pi^*(S)$ and $i \in \{1,\dots,\ell\}$ such that $|\bar{U}_i : K_\omega|$ is not a power of p. Let $\hat{\delta}_1,\dots,\hat{\delta}_s$ be a set of representatives of the orbits of P on Ω_i, where $s := n_{\Omega_i}(P)$. In other words, this means that

$$\Omega_i = \bigcup_{j=1}^{s} \{\hat{\delta}_j^x \mid x \in P\}$$

and that this union is disjoint. For each $j \in \{1,\dots,s\}$, let $\delta_j \in \hat{\delta}_j$. As $\hat{\delta}_j \subseteq \Omega$ is a block of imprimitivity for the action of K on Ω, the union

$$\bigcup_{j=1}^{s} \{\delta_j^x \mid x \in P\} \subseteq \Omega \tag{2.4.6}$$

is made by pairwise disjoint P-orbits and hence $n_\Omega(P) \geq s = n_{\Omega_i}(P)$. Moreover, $n_\Omega(P) = n_{\Omega_i}(P)$ if and only if the equality in (2.4.6) is attained, which in turn happens, if and only if, for each $j \in \{1,\dots,s\}$, the points in $\hat{\delta}_j \subseteq \Omega$ are in the same P-orbit.

Since we are assuming that $n_\Omega(P) = n_{\Omega_i}(P)$, the previous paragraph shows that the stabilizer $P_{\hat{\delta}_j}$ of the block $\hat{\delta}_j$ is transitive on the points in $\hat{\delta}_j$. Since P is a p-group, we deduce $|\hat{\delta}_j| = |\bar{U}_i : K_\omega|$ is a power of p, contradicting our choice of i and p.

□

2.4.3 Proofs of Theorem 2.0.15 and Corollary 2.0.16

If N is a normal subgroup of a finite group G, we denote by $m(G,N)$ the difference $m(G) - m(G/N)$. In the first part of this section we recall some results proved in [104, 105], estimating the value of $m(G,N)$ when N is a minimal normal subgroup of G.

Lemma 2.4.5. *If N is an abelian minimal normal subgroup of G, then $m(G,N)$ is either 0 or 1 depending on whether $N \leq \mathrm{Frat}(G)$ or not.*

Proof. If follows from [104, Lemma 11 and Lemma 12]. □

Lemma 2.4.6. *Assume that N is a non-abelian minimal normal subgroup of a finite group G. There exist a non-abelian simple group S and a positive integer r such that $N = S_1 \times \cdots \times S_r$, with $S \cong S_i$ for each $1 \leq i \leq r$. Let K be the transitive subgroup of $\mathrm{Sym}(r)$ induced by the conjugacy action of G on the set $\{S_1, \ldots, S_r\}$ of the simple components of N. As in the previous section, let $t(K) := t_{\{1,\ldots,r\}}(K)$ be the largest positive integer t such that the stabilizer in K of a point in $\{1, \ldots, r\}$ can be obtained as an intersection of t independent subgroups. Moreover let X be the subgroup of $\mathrm{Aut}\, S_1$ induced by the conjugation action of $N_G(S_1)$ on the first factor S_1 . Then*

$$m(G, N) \leq m(X, \mathrm{soc}\, X) + t(K).$$

Proof. If follows from [104, Lemma 13] and [105, Theorem 1]. □

Lemma 2.4.7. *Let N be a minimal normal subgroup of a finite group G. If $N \not\leq \mathrm{Frat}(G)$, then $\delta(G) \geq \delta(G/N) + |\pi(N)|$.*

Proof. It suffice to prove that $d_p(G) > d_p(G/N)$ whenever $p \in \pi(N)$. Let $p \in \pi(N)$ and let P be a Sylow p-subgroup of G. When N is abelian, there exists a maximal subgroup H of G such that $G = N \rtimes H$. Hence N is complemented in P^g for some $g \in G$. In particular, $N \not\leq \mathrm{Frat}(P^g)$, and $d_p(G/N) + 1 \leq d_p(G)$. Now, assume that N is non-abelian. If $P \cap N \leq \mathrm{Frat}(P)$, then Tate's Theorem [70, p. 431] shows that N has a normal p-complement. However, this is impossible because N is a direct product of non-abelian simple groups. Thus $P \cap N \not\leq \mathrm{Frat}(P)$, and consequently $d_p(G/N) + 1 \leq d_p(G)$. □

Proof of Theorem 2.0.15. Clearly the statement is true if G is simple. Thus we suppose that S is not a simple group and we proceed by induction on the order of G. We may assume $\mathrm{Frat}(G) = 1$. Let N be a minimal normal subgroup of G. If N is abelian, using Lemma 2.4.7 and the inductive hypotheses, we have

$$m(G) = m(G/N) + 1 \leq \sigma(\delta(G/N))^\eta + 1 \leq \sigma \cdot (\delta(G) - 1)^\eta + 1 \leq \sigma \cdot \delta(G)^\eta.$$

(In the last inequality, we used the fact that $\sigma \geq 1$ and $\eta \geq 2$.) Assume that N is non-abelian. Let K, X and S be as in the statement of Lemma 2.4.6. By Theorem 2.4.4, we have

$$t(K) < \sum_{p \in \pi^*(S)} d_p(G) \leq \delta(G).$$

Combining this with Lemmas 2.4.6 and 2.4.7, we conclude that

$$\begin{aligned} m(G) &\leq m(G/N) + m(X, S) + t(K) \leq \sigma \cdot \delta(G/N)^\eta + \sigma \cdot |\pi(S)|^\eta + \delta(G) \\ &\leq \sigma \cdot \delta(G/N)^\eta + \sigma \cdot |\pi(S)|^\eta + \sigma \cdot \delta(G) \leq \sigma(\delta(G/N)^\eta + |\pi(N)|^\eta + \delta(G)) \\ &\leq \sigma((\delta(G/N)^\eta + (\delta(G) - \delta(G/N))^\eta + \delta(G/N) + (\delta(G) - \delta(G/N))) \\ &\leq \sigma \cdot \delta(G)^\eta. \end{aligned}$$

The last inequality follows from the fact that $x^\eta + y^\eta + x + y \leq (x + y)^\eta$, for every positive integers x and y and for every $\eta \geq 2$. □

In order to prove Corollary 2.0.16, we first need the following lemma.

Lemma 2.4.8. *For every positive real number $\eta > 1$, there exists a constant c_η such that $n \leq c_\eta \pi(n)^\eta$, where $\pi(n)$ is the number of prime numbers less than or equal to n.*

Proof. By [146, Theorem 29], if $n \geq 55$, then $\pi(n) > \frac{n}{\log_e n + 2}$, so if suffices to notice that $\lim_{n\to\infty} \frac{n^{\eta-1}}{(\log_e n+2)^\eta} = \infty$. □

Lemma 2.4.9. *There exists a constant ρ such that, if X is an almost simple group and $S = \mathrm{soc}(X)$ is not a simple group of Lie type, then $m(X,S) \leq \rho \cdot |\pi(S)|^2$.*

Proof. First assume that $S = \mathrm{Alt}(n)$. By [163, Theorem 1], $m(X,S) \leq n-1$. By Lemma 2.4.8, there exists a constant c_2 such that $m(X,S) \leq c_2\pi(n)^2 = c_2 \cdot |\pi(S)|^2$. Clearly there exists a constant c such that $m(X,S) \leq c \cdot |\pi(S)|^2$, for every sporadic simple group S. Taking $\rho = \max\{c, c_2\}$, the result follows. □

Proof of Corollary 2.0.16. It follows from Theorem 2.0.15 and Lemma 2.4.9. □

2.4.4 Estimating $\delta(\mathrm{Sym}(n))$

In this section, we aim to bound, from above and from below, $\delta(\mathrm{Sym}(n))$ as a function of n. By [163, Theorem 1], $m(\mathrm{Sym}(n)) = n-1$ while, by Kalužnin's Theorem, if

$$a_{\ell(p,n)}p^{\ell(p,n)} + a_{\ell(p,n)-1}p^{\ell(p,n)-1} + \cdots + a_1 p + a_0$$

is the p-adic expansion of n, then

$$d_p(\mathrm{Sym}(n)) = a_{\ell(p,n)}\ell(p,n) + a_{\ell(p,n)-1}(\ell(p,n)-1) + \cdots + a_1.$$

In order to make the notation less cumbersome, we set

$$d_p(n) := d_p(\mathrm{Sym}(n)) = a_{\ell(p,n)}\ell(p,n) + a_{\ell(p,n)-1}(\ell(p,n)-1) + \cdots + a_1$$

and

$$\delta(n) := \sum_{p \text{ prime}} d_p(n) = \delta(\mathrm{Sym}(n)).$$

As in the previous sections we denote by $\pi : \mathbb{R} \to \mathbb{N}$ the prime counting function, that is, $\pi(x)$ is the number of prime numbers less than or equal to x. As $d_p(n) \geq 1$ for every prime $p \leq n$, we have

$$\pi(n) \leq \delta(n).$$

From the Prime Number Theorem, $\pi(n)$ is asymptotic to $n/\log_e n$ (that is, the ratio $\pi(n)/(n/\log_e n)$ tends to 1 as n tends to infinity) and hence $n/\log_e n \in O(\delta(n))$. In this section, we actually prove that $\delta(n)$ is asymptotic to a linear function.

Theorem 2.4.10. *For every $n \geq 2$, we have*

$$n\log_e 2 - \frac{12n}{\log_e n} \leq \delta(n) \leq n\log_e 2 + \frac{19n}{2\log_e n} + \frac{137n}{2\log_e^2 n} + \frac{4\sqrt{n}}{\log_e n} + \frac{3\sqrt{n}}{2}\log_e n \leq n\log_e 2 + \frac{112n}{\log_e n}.$$

In particular, $\delta(n) = n\log_e 2 + O(n/\log_e n)$.

Proof. We start by collecting some basic inequalities that we use throughout this proof. From Theorem 1 and Theorem 2 in [147], we have

$$\pi(x) \leq \frac{x}{\log_e x}\left(1 + \frac{3}{2\log_e x}\right), \qquad \forall x > 1, \tag{2.4.7}$$

$$\pi(x) \geq \frac{x}{\log_e x - 1/2}, \qquad \forall x \geq 67. \tag{2.4.8}$$

Given a prime number p with $p \leq n$, $\ell(p,n) \leq \lfloor \log_p n \rfloor$ and hence

$$\begin{aligned} d_p(n) &\leq (p-1)(\ell(p,n) + (\ell(p,n)-1) + \cdots + 2 + 1) \\ &= (p-1)\frac{\ell(p,n)(\ell(p,n)+1)}{2} \leq (p-1)\frac{\log_p n(\log_p n + 1)}{2}. \end{aligned} \tag{2.4.9}$$

We define the two auxiliary functions

$$d'(n) := \sum_{p \leq \sqrt{n}} d_p(n); \quad d''(n) := \sum_{\sqrt{n} < p \leq n} d_p(n).$$

We aim to obtain explicit bounds on $d'(n)$ and $d''(n)$ as functions of n. We start with $d'(n)$.

From (2.4.9), we get

$$d'(n) \leq \frac{\log_e^2 n}{2} \sum_{p \leq \sqrt{n}} \frac{p-1}{\log_e^2 p} + \frac{\log_e n}{2} \sum_{p \leq \sqrt{n}} \frac{p-1}{\log_e p}. \tag{2.4.10}$$

For every $k \in \mathbb{N}$ with $k \geq 1$, we denote by p_k the k^{th} prime number. Using [147, Corollary, page 69], we have

$$k \log_e k < p_k < k(\log_e k + \log_e \log_e k),$$

where the first inequality is valid for every $k \geq 1$ and the second inequality is valid for every $k \geq 6$.

This shows that, for every $k \geq 6$,

$$\frac{p_k - 1}{\log_e p_k} \leq \frac{k(\log_e k + \log_e \log_e k)}{\log_e (k \log_e k)} = k. \tag{2.4.11}$$

An explicit computation yields that (2.4.11) is also valid when $k \in \{2, 3, 4, 5\}$.

Therefore, for $n \geq 11$, (2.4.7) and (2.4.11) yield:

$$\begin{aligned}
\sum_{p \leq \sqrt{n}} \frac{p-1}{\log_e p} &= \frac{1}{\log_e 2} + \sum_{2 < p \leq \sqrt{n}} \frac{p-1}{\log_e p} = \frac{1}{\log_e 2} + \sum_{k=2}^{\pi(\sqrt{n})} \frac{p_k - 1}{\log_e p_k} \leq \frac{1}{\log_e 2} + \sum_{k=2}^{\pi(\sqrt{n})} k \\
&= \frac{1}{\log_e 2} + \frac{\pi(\sqrt{n})(\pi(\sqrt{n})+1)}{2} - 1 = \frac{1}{\log_e 2} - 1 + \frac{\pi(\sqrt{n})^2}{2} + \frac{\pi(\sqrt{n})}{2} \\
&\leq -1 + \frac{1}{\log_e 2} + \frac{1}{2}\left(\frac{\sqrt{n}}{\log_e \sqrt{n}}\left(1 + \frac{3}{2\log_e \sqrt{n}}\right)\right)^2 + \frac{\sqrt{n}}{2\log_e \sqrt{n}}\left(1 + \frac{3}{2\log_e \sqrt{n}}\right) \\
&= -1 + \frac{1}{\log_e 2} + \frac{1}{2}\left(\frac{4n}{\log_e^2 n} + \frac{36n}{\log_e^4 n} + \frac{24n}{\log_e^3 n}\right) + \frac{\sqrt{n}}{\log_e n} + \frac{3\sqrt{n}}{\log_e^2 n} \\
&\leq \frac{2n}{\log_e^2 n} + \frac{24n}{\log_e^3 n}.
\end{aligned}$$

In fact, we only require n to be at least 11 for the last inequality above. Thus, using this, together with direct inspection for the cases $2 \leq n \leq 10$, we have:

$$\sum_{p \leq \sqrt{n}} \frac{p-1}{\log_e p} \leq \frac{2n}{\log_e^2 n} + \frac{24n}{\log_e^3 n}, \tag{2.4.12}$$

for every $n > 1$.

Arguing in a similar manner, for every $k \geq 6$, we obtain

$$\frac{p_k - 1}{\log_e^2 p_k} \leq \frac{k(\log_e k + \log_e \log_e k)}{\log_e^2 (k \log_e k)} = \frac{k}{\log_e k + \log_e \log_e k}. \tag{2.4.13}$$

An explicit computation yields that (2.4.13) is also valid when $k \in \{2, 3, 4, 5\}$. Therefore, using (2.4.13), we have

$$\sum_{p \leq \sqrt{n}} \frac{p-1}{\log_e^2 (p)} \leq \frac{1}{\log_e^2 (2)} + \sum_{k=2}^{\pi(\sqrt{n})} \frac{k}{\log_e k + \log_e \log_e k}.$$

For every $t \in \mathbb{N}$ with $t \geq 2$, write $f(t) := \sum_{k=2}^{t} k/(\log_e k + \log_e \log_e k)$. When $k > 2$, we have $k/(\log_e k + \log_e \log_e k) \leq k$. Moreover, when $k \geq \sqrt{t}$, we have

$$\begin{aligned}\frac{k}{\log_e k + \log_e \log_e k} &\leq \frac{k}{\log_e \sqrt{t} + \log_e \log_e(\sqrt{t})} = \frac{k}{\log_e t/2 + \log_e(\log_e t) - \log_e 2} \\ &\leq \frac{2k}{\log_e t},\end{aligned}$$

where the last inequality holds for $t \geq 8$. Therefore, for every $t \geq 8$, we have

$$\begin{aligned}f(t) &= \frac{2}{\log_e 2 + \log_e \log_e 2} + \sum_{2<k\leq\sqrt{t}} \frac{k}{\log_e k + \log_e \log_e k} + \sum_{\sqrt{t}<k\leq t} \frac{k}{\log_e k + \log_e \log_e k} \\ &\leq \frac{2}{\log_e 2 + \log_e \log_e 2} + \sum_{2<k\leq\sqrt{t}} k + \sum_{\sqrt{t}<k\leq t} \frac{2k}{\log_e t} \\ &\leq \frac{2}{\log_e 2 + \log_e \log_e 2} + \frac{\sqrt{t}(\sqrt{t}+1)}{2} - 3 + \frac{t(t+1)}{\log_e t} \leq \frac{t^2}{\log_e t} + t,\end{aligned}$$

where the last inequality follows with some elementary computations. A direct computation with $2 \leq t < 8$ shows that the same upper bound for $f(t)$ holds. Therefore, applying this upper bound with $t := \pi(\sqrt{n})$, we get

$$\sum_{p\leq\sqrt{n}} \frac{p-1}{\log_e^2(p)} \leq \frac{1}{\log_e^2 2} + f(\pi(\sqrt{n})) \leq \frac{1}{\log_e^2 2} + \frac{\pi(\sqrt{n})^2}{\log_e \pi(\sqrt{n})} + \pi(\sqrt{n}). \tag{2.4.14}$$

Now, for every $n \geq 67^2$, using (2.4.7) and (2.4.8), we see that the right hand side of (2.4.14) is bounded above by

$$\frac{1}{\log_e^2 2} + \frac{\left(\frac{\sqrt{n}}{\log_e \sqrt{n}}\left(1 + \frac{3}{2\log_e \sqrt{n}}\right)\right)^2}{\log_e\left(\frac{\sqrt{n}}{\log_e \sqrt{n} - 1/2}\right)} + \frac{\sqrt{n}}{\log_e \sqrt{n}}\left(1 + \frac{3}{2\log_e \sqrt{n}}\right). \tag{2.4.15}$$

The second summand of (2.4.15) is at most

$$\frac{\frac{4n}{\log_e^2 n}\left(1 + \frac{3}{\log_e n}\right)^2}{\log_e(\sqrt{n}/\log_e \sqrt{n})}.$$

Now, we have $\log_e(\sqrt{n}/\log_e \sqrt{n}) > \log_e n/4$. Thus the second summand of (2.4.15) is at most

$$\frac{16n}{\log_e^3 n} + \frac{96n}{\log_e^4 n} + \frac{144n}{\log_e^5 n} \leq \frac{16n}{\log_e^3 n} + \frac{114n}{\log_e^4 n},$$

where the last inequality follows with a computation using the fact that $n \geq 67^2$. For the first and third summand of (2.4.15), we have

$$\frac{1}{\log_e^2(2)} + \frac{2\sqrt{n}}{\log_e(n)} + \frac{6\sqrt{n}}{\log_e^2(n)} < \frac{3\sqrt{n}}{\log_e(n)},$$

where this inequality follows again with some elementary computations using the fact that $n \geq 67^2$. Summing up, for every $n \geq 67^2$, we have

$$\sum_{p\leq\sqrt{n}} \frac{p-1}{\log_e^2 p} \leq \frac{16n}{\log_e^3 n} + \frac{114n}{\log_e^4 n} + \frac{3\sqrt{n}}{\log_e n}. \tag{2.4.16}$$

A direct inspection shows that this bound is also valid for the natural numbers n with $n \leq 67^2$.

Summing up, from (2.4.10), (2.4.12) and (2.4.16), we get

$$\begin{aligned} d'(n) &\leq \frac{8n}{\log_e n} + \frac{57n}{\log_e^2 n} + \frac{3}{2}\sqrt{n}\log_e(n) + \frac{n}{\log_e n} + \frac{12n}{\log_e^2 n} \\ &= \frac{9n}{\log_e n} + \frac{69n}{\log_e^2 n} + \frac{3}{2}\sqrt{n}\log_e n. \end{aligned} \tag{2.4.17}$$

We now start working on the function $d''(n) = \sum_{\sqrt{n}<p\leq n} d_p(n)$. Here we are interested in a lower bound and in an upper bound for $d''(n)$. First we obtain an upper bound for $d''(n)$. As $p > \sqrt{n}$, the p-adic expansion of n is simply $n := a_1(p,n)p + a_0$ and hence $d_p(n) = a_1(p,n)$. Now we refine further $d''(n)$. For every $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor - 1\}$, we let

$$g_i(n) := \sum_{n/(i+1)<p\leq n/i} a_1(p,n)$$

and we let

$$g_{\lfloor\sqrt{n}\rfloor}(n) := \sum_{\sqrt{n}<p\leq n/\lfloor\sqrt{n}\rfloor} a_1(p,n).$$

When $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor\}$, we have $a_1(p,n) = i$ and hence $g_i(n)$ equals i times the number of prime numbers in the interval $(n/(i+1), n/i]$. Therefore, when $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor - 1\}$,

$$g_i(n) = i(\pi(n/i) - \pi(n/(i+1)))$$

and

$$g_{\lfloor\sqrt{n}\rfloor}(n) = \lfloor\sqrt{n}\rfloor(\pi(n/\lfloor\sqrt{n}\rfloor) - \pi(\sqrt{n})).$$

Since every prime p, with $\sqrt{n} < p \leq n$, lies in one of the intervals $(n/(i+1), n/i]$, for some $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor - 1\}$, or in the interval $(\sqrt{n}, n/\lfloor\sqrt{n}\rfloor]$, we have

$$\begin{aligned} d''(n) = \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} g_i(n) &= \sum_{i=1}^{\lfloor\sqrt{n}\rfloor-1} i(\pi(n/i) - \pi(n/(i+1))) + \lfloor\sqrt{n}\rfloor(\pi(n/\lfloor\sqrt{n}\rfloor) - \pi(\sqrt{n})) \\ &= \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \pi(n/i) - \lfloor\sqrt{n}\rfloor\pi(\sqrt{n}). \end{aligned} \tag{2.4.18}$$

Using (2.4.7), we have

$$\begin{aligned} \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \pi(n/i) &\leq \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)}\left(1 + \frac{3}{2\log_e(n/i)}\right) \\ &= \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)} + \frac{3}{2}\sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e^2(n/i)}. \end{aligned} \tag{2.4.19}$$

The function $x \mapsto (n/x)/\log_e(n/x)$ is decreasing in the interval $(0, \lfloor\sqrt{n}\rfloor]$ and hence we obtain for the first summand the estimate

$$\begin{aligned} \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)} &= \frac{n}{\log_e n} + \sum_{i=2}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)} \leq \frac{n}{\log_e n} + \int_1^{\lfloor\sqrt{n}\rfloor} \frac{n/x}{\log_e(n/x)}dx \\ &= \frac{n}{\log_e n} + [-n\log_e(\log_e(n/x))]_1^{\lfloor\sqrt{n}\rfloor} \\ &= \frac{n}{\log_e n} - n\log_e\log_e(n/\lfloor\sqrt{n}\rfloor) + n\log_e(\log_e n). \end{aligned} \tag{2.4.20}$$

For the second summand observe that the function $x \mapsto (n/x)/\log_e^2(n/x)$ is decreasing in the interval $(0, \lfloor\sqrt{n}\rfloor]$ and hence we obtain the estimate

$$\begin{aligned}\frac{3}{2}\sum_{i=1}^{\lfloor\sqrt{n}\rfloor}\frac{n/i}{\log_e^2(n/i)} &= \frac{3n}{2\log_e^2 n} + \frac{3}{2}\sum_{i=2}^{\lfloor\sqrt{n}\rfloor}\frac{n/i}{\log_e^2(n/i)} \\ &\leq \frac{3n}{2\log_e^2 n} + \frac{3}{2}\int_1^{\lfloor\sqrt{n}\rfloor}\frac{n/x}{\log_e^2(n/x)}dx \\ &= \frac{3n}{2\log_e^2(n)} + \frac{3}{2}\left[\frac{n}{\log_e(n/x)}\right]_1^{\lfloor\sqrt{n}\rfloor} \\ &= \frac{3n}{2\log_e^2(n)} + \frac{3n}{2\log_e(n/\lfloor\sqrt{n}\rfloor)} - \frac{3n}{2\log_e n}.\end{aligned} \tag{2.4.21}$$

Further, for $n \geq 67^2$, we get

$$\begin{aligned}\lfloor\sqrt{n}\rfloor\pi(\sqrt{n}) &\geq (\sqrt{n}-1)\frac{\sqrt{n}}{\log_e\sqrt{n}-1/2} = \frac{2n}{\log_e n - 1} - \frac{2\sqrt{n}}{\log_e n - 1} \\ &= \frac{2n}{\log_e n} + 2n\left(\frac{1}{\log_e n - 1} - \frac{1}{\log_e n}\right) - \frac{2\sqrt{n}}{\log_e n - 1} \\ &\geq \frac{2n}{\log_e n} + \frac{2n}{\log_e n(\log_e n - 1)} - \frac{2\sqrt{n}}{\log_e n/2} \\ &\geq \frac{2n}{\log_e n} + \frac{2n}{\log_e^2 n} - \frac{4\sqrt{n}}{\log_e n}.\end{aligned} \tag{2.4.22}$$

Thus, from (2.4.18), (2.4.19), (2.4.20), (2.4.21) and (2.4.22), for every $n \geq 67^2$, we have that

$$\begin{aligned}d''(n) \leq\ & n\log_e(\log_e n) - n\log_e(\log_e(n/\lfloor\sqrt{n}\rfloor)) - \frac{n}{2\log_e n} + \frac{3n}{2\log_e^2 n} + \frac{3n}{2\log_e(n/\lfloor\sqrt{n}\rfloor)} \\ & - \frac{2n}{\log_e n} - \frac{2n}{\log_e^2 n} + \frac{4\sqrt{n}}{\log_e n}.\end{aligned}$$

First of all, as $n/\lfloor\sqrt{n}\rfloor \geq \sqrt{n}$, we get $\log_e(n/\lfloor\sqrt{n}\rfloor) \geq \log_e\sqrt{n} = \log_e(n)/2$ and hence

$$-\frac{n}{2\log_e n} + \frac{3n}{2\log_e(n/\lfloor\sqrt{n}\rfloor)} - \frac{2n}{\log_e n} \leq \left(-\frac{1}{2} + 3 - 2\right)\frac{n}{\log_e n} = \frac{n}{2\log_e n}.$$

Moreover,

$$\begin{aligned}n\log_e(\log_e n) - n\log_e(\log_e(n/\lfloor\sqrt{n}\rfloor)) &\leq n\log_e\log_e n - n\log_e\log_e(\sqrt{n}) \\ &= n\log_e\left(\frac{\log_e n}{\log_e\sqrt{n}}\right) = n\log_e 2.\end{aligned}$$

Summing up, for every $n \geq 67^2$,

$$d''(n) \leq n\log_e 2 + \frac{n}{2\log_e n} - \frac{n}{2\log_e^2 n} + \frac{4\sqrt{n}}{\log_e n}. \tag{2.4.23}$$

An explicit computation with the positive integers n with $2 \leq n < 67^2$ shows that the same upper bound remains true when $n \leq 67^2$.

Using the upper bounds (2.4.17) and (2.4.23), for every $n \geq 2$, we deduce

$$\delta(n) = d'(n) + d''(n) \leq n\log_e 2 + \frac{19n}{2\log_e n} + \frac{137n}{2\log_e^2 n} + \frac{4\sqrt{n}}{\log_e n} + \frac{3\sqrt{n}}{2}\log_e n \leq n\log_e 2 + \frac{112n}{\log_e n},$$

where the last inequality follows with some computation.

Now, we use the argument above to obtain also a lower bound for $d''(n)$ and hence for $d''(n)$. Using (2.4.8) and (2.4.18), we have

$$\begin{aligned} d''(n) &= \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \pi(n/i) - \lfloor\sqrt{n}\rfloor\pi(\sqrt{n}) \geq \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i) - 1/2} - \lfloor\sqrt{n}\rfloor\pi(\sqrt{n}) \\ &\geq \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)} - \sqrt{n}\pi(\sqrt{n}). \end{aligned}$$

The function $x \mapsto (n/x)/\log_e(n/x)$ is decreasing in the interval $(0, \lfloor\sqrt{n}\rfloor]$ and hence we obtain the estimate

$$\begin{aligned} \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log_e(n/i)} &\geq \int_1^{\lfloor\sqrt{n}\rfloor} \frac{n/x}{\log_e(n/x)} dx = [-n\log_e(\log_e(n/x))]_1^{\lfloor\sqrt{n}\rfloor} \\ &= -n\log_e\log_e(n/\lfloor\sqrt{n}\rfloor) + n\log_e(\log_e n) = n\log_e\left(\frac{\log_e n}{\log_e(n/\lfloor\sqrt{n}\rfloor)}\right) \\ &= n\log_e\left(\frac{\log_e n}{\log_e n - \log_e(\lfloor\sqrt{n}\rfloor)}\right) = n\log_e\left(\frac{\log_e n}{\log_e n - \log_e\sqrt{n} - \log_e(\lfloor\sqrt{n}\rfloor/\sqrt{n})}\right) \\ &= n\log_e\left(\frac{\log_e n}{(\log_e n)/2 - \log_e(\lfloor\sqrt{n}\rfloor/\sqrt{n})}\right) \geq n\log_e 2, \end{aligned}$$

where in the last inequality we used the fact that $\lfloor\sqrt{n}\rfloor/\sqrt{n} \leq 1$ and hence $\log_e(\lfloor\sqrt{n}\rfloor/\sqrt{n}) \leq 0$. Furthermore, from (2.4.7), we have

$$\sqrt{n}\pi(\sqrt{n}) \leq \frac{n}{\log_e\sqrt{n}}\left(1 + \frac{3}{2\log_e\sqrt{n}}\right) = \frac{2n}{\log_e n}\left(1 + \frac{3}{\log_e n}\right) \leq \frac{12n}{\log_e n},$$

where the last inequality follows from an easy computation. Summing up,

$$\delta(n) = d'(n) + d''(n) \geq d''(n) \geq n\log_e 2 - \frac{12n}{\log_e n}. \quad \square$$

2.5 The Tarski Irredundant basis theorem and the finite soluble groups

2.5.1 Preliminaties

We start by reviewing some results of [39] that we will use in our proofs.

Let V be a finite dimensional vector space over a finite field of prime order. Let H be a linear soluble group acting irreducibly and faithfully on V. For a positive integer δ we consider the semidirect product $G = V^\delta \rtimes H$ where H acts in the same way on each of the δ direct factors. We set $F = \mathrm{End}_H(V)$.

Proposition 2.5.1. [39, Proposition 2.1] *Let $H = \langle h_1, \ldots, h_t\rangle$ and $w_i = (v_{1,i}, \ldots, v_{\delta,i}) \in V^\delta$ with $1 \leq i \leq t$. The following are equivalent.*

1. *$G \neq \langle h_1 w_1, \ldots, h_t w_t\rangle$;*
2. *there exist $\lambda_1, \ldots, \lambda_\delta \in F$ and $w \in V$ with $(\lambda_1, \ldots, \lambda_\delta, w) \neq (0, \ldots, 0, 0)$ such that $\sum_{1\leq j\leq\delta} \lambda_j v_{j,i} = w - wh_i$ for each $i \in \{1, \ldots, t\}$.*

Let n be the dimension of V over F. We may identify $H = \langle h_1, \dots, h_t \rangle$ with a subgroup of $GL(n, F)$. In this identification h_i becomes an $n \times n$ matrix A_i with coefficients in F. Let $w_i = (v_{i,1}, \dots, v_{i,\delta}) \in V^\delta$. Then every $v_{i,j}$ can be viewed as a $1 \times n$ matrix. Denote the $\delta \times n$ matrix with rows $v_{i,1}, \dots, v_{i,\delta}$ by X_i. By Proposition 2.5.1, the elements $h_1 w_1, \dots, h_t w_t$ generate a proper subgroup of G if and only if there exists a non-zero vector $(\lambda_1, \dots, \lambda_\delta; \mu_1, \dots, \mu_n)$ in $F^{\delta+n}$ such that

$$(\lambda_1, \dots, \lambda_\delta) X_i = (\mu_1, \dots, \mu_n)(1 - A_i) \text{ for each } 1 \leq i \leq t.$$

This implies that $\langle h_1 w_1, \dots, h_t w_t \rangle = G$ if and only if

$$\operatorname{rank} \begin{pmatrix} 1 - A_1 & \cdots & 1 - A_t \\ X_1 & \cdots & X_t \end{pmatrix} = n + \delta. \tag{2.5.1}$$

From this it follows that G cannot be generated by t elements if $n + \delta > nt$. Notice also that the fact that $h_1, \dots, h_t$ generates H implies that the linear map $\alpha : F^n \to (F^n)^t$, $w \mapsto (w(1 - A_1), \dots, w(1 - A_t))$ is injective. Therefore the matrix $\begin{pmatrix} 1 - A_1 \dots 1 - A_t \end{pmatrix}$ has rank n, so it is possible to find $X_1, \dots, X_t$ satisfying (2.5.1) whenever $n + \delta \leq nt$. Hence $d(V^\delta \rtimes H) \leq t$ whenever $\delta \leq n(t - 1)$.

2.5.2 Proof of Theorem 2.0.17

To prove Theorem 2.0.17 we need an elementary lemma in linear algebra. Denote by $M_{r,s}(F)$ the ring of the $r \times s$ matrices with coefficients in the field F.

Lemma 2.5.2. *Assume that $A_1, \dots, A_t \in M_{n,n}(F)$ and that $\operatorname{rank}(A_1 \cdots A_t) = n$. If $\delta \leq n(t - 1)$, then there exist $v_{j,i} \in M_{1,n}$, with $1 \leq j \leq \delta$, and $1 \leq i \leq t$, such that*

$$\operatorname{rank} \begin{pmatrix} A_1 & \dots & A_t \\ v_{1,1} & \dots & v_{1,t} \\ \vdots & \ddots & \vdots \\ v_{\delta,1} & \dots & v_{\delta,t} \end{pmatrix} = n + \delta.$$

Moreover, we may choose the vectors $v_{j,i}$ in such a way that for every $j \in \{1, \dots, \delta\}$, there exists a unique $i \in \{1, \dots, t\}$ such that $v_{j,i} \neq 0$.

Proof. We describe how the vectors $v_{j,i}$ can be chosen. First let $n_1 = \operatorname{rank}(A_1)$ and let $r_1 = n - n_1$. We choose $v_{1,1}, \dots, v_{r_1,1}$ is a such a way that

$$\operatorname{rank} \begin{pmatrix} A_1 \\ v_{1,1} \\ \vdots \\ v_{r_1,1} \end{pmatrix} = n$$

and we set $v_{j,1} = 0$ if $j > r_1$. Now let

$$\operatorname{rank} \begin{pmatrix} A_1 & A_2 \\ v_{1,1} & 0 \\ \vdots & \\ v_{r_1,1} & 0 \end{pmatrix} = n_2$$

and let $r_2 = n - n_2$. We choose $v_{r_1+1,2}, \dots, v_{r_1+r_2,2}$ is a such a way that

$$\operatorname{rank}\begin{pmatrix} A_1 & A_2 \\ v_{1,1} & 0 \\ \vdots & \vdots \\ v_{r_1,1} & 0 \\ 0 & v_{r_1+1,2} \\ \vdots & \vdots \\ 0 & v_{r_1+r_2,2} \end{pmatrix} = 2n$$

and we set $v_{j,2} = 0$ if $j > r_1 + r_2$. Continuing in this way we get the result. □

Proof of Theorem 2.3.1. We work by induction on $|G|$. Clearly we may assume $\operatorname{Frat} G = 1$. So let $A, R = R_G(A), D, C = C_G(A)$ as in Corollary 1.2.5. There exists a positive integer δ such that $D \cong_G A^\delta$. Moreover, there exists a complement H of D in G with $R \leq H$. Let $d = d(G), m = m(G)$, $a = d(H)$ and $b = m(H)$. By [104, Theorem 2], $m(G)$ coincides with the number of non-Frattini factors in a chief series of G, hence $m = b + \delta$. By induction, there exists a generating set $\{h_1, \dots, h_a\}$ for H which is strongly totally extendible.
To prove our statement it is enough to prove that the following is true.

(∗) There exist a generating set ω of G of cardinality d and $u_1, \dots, u_\delta \in D$ such that $\{h_1, \dots, h_a, u_1, \dots, u_\delta\}$ is a strong descendant of ω.

Indeed, since $\{h_1, \dots, h_a\}$ is a strongly totally extendible generating set of H, there is a sequence of strong immediate descendants from $\{h_1, \dots, h_a\}$ to a generating set $\{k_1, \dots, k_b\}$ of H of maximal cardinality. We can use this sequence, to construct a sequence of strong immediate descendants from $\{h_1, \dots, h_a, u_1, \dots, u_\delta\}$ to $\{k_1, \dots, k_b, u_1, \dots, u_\delta\}$.

Now we want to prove (∗). We have $C/R = DR/R \cong D \cong A^\delta$ and either $A \cong C_p$ is a trivial G-module and $G/R \cong (C_p)^\delta$, or $G/R \cong C/R \rtimes H/R$ where H/R acts in the same say on each of the δ factors of $C/R \cong A^\delta$ and this action is faithful and irreducible. We denote by $\overline{G}$ the quotient group G/R and, for every $g \in G$, we set $\overline{g} = gR$. By Corollary 1.2.5, if $(u_1, \dots, u_d) \in D^d$, then $G = \langle h_1u_1, \dots, h_au_a, u_{a+1}, \dots, u_d\rangle$ if and only if $\overline{G} = \langle \overline{h_1u_1}, \dots, \overline{h_au_a}, \overline{u_{a+1}}, \dots, \overline{u_d}\rangle$. Further, in this case, $\{h_1u_1, \dots, h_au_a, u_{a+1}, \dots, u_d\}$ is a minimal generating set if and only if $\langle \overline{h_1u_1}, \dots, \overline{h_au_a}, \overline{u_{a+1}}, \dots, \overline{u_{j-1}}, \overline{u_{j+1}}, \dots \overline{u_d}\rangle \neq \overline{G}$ for any $a + 1 \leq j \leq d$.

First assume that $A \cong C_p$ is a trivial G-module. In this case $H = R$, $G = D \times R$. Hence $\overline{G} = \overline{D} \cong D$ is a vector space of dimension δ over the field $\mathbb{F}_p$ with p-elements and $d = \max\{\delta, a\}$. More precisely, $G = \langle x_1, \dots, x_d\rangle$ where $x_i = h_iu_i$ when $i \leq \rho = \min\{\delta, a\}$, whilst for $i > \rho$, then $x_i = h_i$ when $\rho = \delta$ and $x_i = u_i$ when $\rho = a$. For $1 \leq i \leq a$, we have that

$$\{h_1, \dots, h_i, x_{i+1}, \dots, x_d, u_1, \dots, u_i\}$$

is an immediate strong descendant of

$$\{h_1, \dots, h_{i-1}, x_i, \dots, x_d, u_1, \dots, u_{i-1}\}.$$

This implies that $\{h_1, \dots, h_a, u_1, \dots, u_\delta\}$ is a strong descendant of $\{x_1, \dots, x_d\}$ and so (∗) has been proved when A is a trivial G-module.

Now assume that A is a non-trivial G-module, let $F = \operatorname{End}_G A$ and $n = \dim_F A$. We may identify $\overline{H}$ with a subgroup of $\mathrm{GL}(n, F)$. We denote by A_i the matrix $1 - \overline{h}_i$. We write $D = V_1 \times \cdots \times V_\delta$ with $V_i \cong_G A$. Let $u_1, \dots, u_t \in D$, with $t \geq a$, and write u_i in the form $u_i = \sum_{1 \leq j \leq \delta} v_{j,i}$ with $v_{j,i} \in V_j$ (for D we use the additive notation). It follows from the

results in Subsection 2.5.1 that $\{h_1u_1, \dots, h_au_a, u_{a+1}, \dots, u_t\}$ is a minimal generating set of G if and only if

$$\operatorname{rank} \begin{pmatrix} A_1 & \cdots & A_a & 0 & \cdots & 0 \\ v_{1,1} & \cdots & v_{1,a} & v_{1,a+1} & \cdots & v_{1,t} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ v_{\delta,1} & \cdots & v_{\delta,a} & v_{\delta,a+1} & \cdots & v_{\delta,t} \end{pmatrix} = n + \delta$$

and, for every $a < i \leq t$,

$$\operatorname{rank} \begin{pmatrix} A_1 & \cdots & A_a & 0 & \cdots & 0 & 0 & \cdots & 0 \\ v_{1,1} & \dots & v_{1,a} & v_{1,a+1} & \cdots & v_{1,i-1} & v_{1,i+1} & \cdots & v_{1,t} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ v_{\delta,1} & \cdots & v_{\delta,a} & v_{\delta,a+1} & \cdots & v_{\delta,i-1} & v_{\delta,i+1} & \cdots & v_{\delta,t} \end{pmatrix} < n + \delta.$$

We can find vectors $v_{j,i}$ with this property if and only if $\delta \leq n(t-1)$. This implies in particular that

$$d = \max\left\{a, \left\lceil \frac{\delta}{n} + 1 \right\rceil\right\}.$$

Moreover, by Lemma 2.5.2, there exist d elements of D, say $u_i = \sum_{1 \leq j \leq \delta} v_{j,i}$, $1 \leq i \leq d$, such that

1. $\{h_1u_1, \dots, h_au_a, u_{a+1}, \dots, u_d\}$ is an independent generating set of G;
2. for every $j \in \{1, \dots, \delta\}$, there is a unique $i \in \{1, \dots, d\}$ such that $v_{j,i} \neq 0$.

We claim that there exist $\tilde{w}_1, \dots, \tilde{w}_\delta \in U$ such that $\{h_1, \dots, h_a, \tilde{w}_1, \dots, \tilde{w}_d\}$ is a strong descendant of $\omega = \{h_1u_1, \dots, h_au_a, u_{a+1}, \dots, u_d\}$. Indeed, let us assume that there exists $i \leq a$ such that $u_i \neq 0$, let i be the smallest integer with this property and let $\Omega_i = \{j_1, \dots, j_r\}$ be the subset of $\{1, \dots, \delta\}$ characterized by the fact that $v_{j,i} \neq 0$ if and only if $j \in \Omega_i$. We obtain the following sequence of strong immediate descendants of $\omega = \{h_1, \dots, h_{i-1}, h_i(v_{j_1,i} + \cdots + v_{j_r,i}), h_{i+1}u_{i+1}, \dots, h_au_a, u_{a+1}, \dots, u_d\}$:

$$\begin{aligned} \omega_1 &= \{h_1, \dots, h_{i-1}, h_i(v_{j_2,i} + \cdots + v_{j_r,i}), h_{i+1}u_{i+1}, \dots, u_d, v_{j_1,i}\}, \\ \omega_1 &= \{h_1, \dots, h_{i-1}, h_i(v_{j_3,i} + \cdots + v_{j_r,i}), h_{i+1}u_{i+1}, \dots, u_d, v_{j_1,i}, v_{j_2,i}\}, \\ &\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ \omega_{r-1} &= \{h_1, \dots, h_{i-1}, h_iv_{j_r,i}, h_{i+1}u_{i+1} \dots, u_d, v_{j_1,i}, \cdots, v_{j_{r-1},i}\}, \\ \omega_r &= \{h_1, \dots, h_{i-1}, h_i, h_{i+1}u_{i+1}, \dots, u_d, v_{j_1,i}, \cdots, v_{j_r,i}\}. \end{aligned}$$

We repeat this argument until there exists $k \leq a$ with $u_k \neq 0$. In this way we can find $w_1, \dots, w_r \in D$, with $w_i = \sum_{1 \leq j \leq \delta} z_{j,i}$, such that $\omega^* = \{h_1, \dots, h_a, w_1, \dots, w_r\}$ is a strong descendant of ω and, for every $j \in \{1, \dots, \delta\}$, there is a unique $i \in \{1, \dots, d\}$ with $z_{j,i} \neq 0$. For $i \in \{1, \dots, r\}$, let $\Delta_i = \{j \mid z_{j,i} \neq 0\}$. Assume that, for some i, the set $\Omega_i = \{j_1, \dots, j_r\}$ contains more than one element. Then

$$\{h_1, \dots, h_a, w_1, \dots, w_{i-1}, w_i - z_{j_r,i}, w_{i+1}, \dots, w_r, z_{j_r,i}\}$$

is an extension of ω^*. Repeating this argument we can find $\tilde{w}_1, \dots, \tilde{w}_s$ with the properties that $\omega^{**} = (h_1, \dots, h_a, \tilde{w}_1, \dots \tilde{w}_s)$ is a strong descendant of ω^* and for each $1 \leq j \leq \delta$ there exists and is unique $i \in \{1, \dots, s\}$ with $\tilde{w}_i \in V_j$: this implies in particular $s = \delta$. Thus $(*)$ has been proved also in this case. □

2.5.3 The strong extension property

In this section we investigate the structure of the finite soluble groups with the strong extension property. First we consider the nilpotent case.

Proposition 2.5.3. *A finite nilpotent G has the extension property if and only if either G is a p-group or G is cyclic and $|\pi(G)| = 2$.*

Proof. If G is a p-group, then $d(G) = m(G)$ so obviously G has the (strong) extension property.

On the other hand, if $G = \langle g \rangle$ has order $p^a q^b$, with p and q distinct primes, then $\{g^{p^a}, g^{q^b}\}$ is a (strong) descendant of $\{g\}$, so G has the (strong) extension property. We now prove the converse. It is not restrictive to assume $\operatorname{Frat} G = 1$, so that G is a direct product of cyclic groups of prime order. Assume that $|G|$ is divisible by at least three different primes p, q, r and let a, b, c be elements of G of order, respectively, p, q, r. There exists $H \leq G$ such that $G = \langle abc \rangle \times H$ and $m(G) = m(H) + 3$. Let $t = m(H)$, let $\{h_1, \dots h_t\}$ be a minimal generating set of H and consider the generating set $\omega := \{ab, ac, h_1, \dots, h_t\}$ of G. It can be easily seen that, for every $y \in \omega$, the subset $\omega \setminus \{y\}$ generates a maximal subgroup of G so the cardinality of a minimal generating set of G containing $\omega \setminus \{y\}$ coincides with the cardinality of ω. This implies that ω has no immediate descendant. Finally assume that p and q are the unique prime divisor of $|G|$. If the Sylow p-subgroup of G is not cyclic, than there exists a_1, a_2, b such that $|a_1| = |a_2| = p$, $|b| = q$ and $\langle a_1, a_2, b \rangle$ has order $p^2 q$. We have $G = \langle a_1, a_2, b \rangle \times H$ and $m(G) = m(H) + 3$. Let $H = \langle h_1, \dots, h_t \rangle$ with $t = m(H)$ and consider the generating set $\omega := \{a_1 b, a_2 b, h_1, \dots, h_t\}$. As in the previous case, if we delete an element from ω, the remaining elements generate a maximal subgroup of G, and this implies that ω has no immediate descendant. □

In order to study the soluble but not nilpotent groups with the extension property, we first need some lemmas.

Lemma 2.5.4. *Assume that F is a field with q elements and let $A_1, A_2, A_3 \in M_{n,n}(F)$. If $q^n > 2$, then there exists $(x_1, \dots, x_{3n}) \in F^{3n}$ with the following properties:*

1. *$(x_1, \dots, x_n, x_{n+1}, \dots, x_{2n})$ does not belong to F-subspace of F^{2n} spanned by the rows of the matrix $(A_1 \ A_2)$.*
2. *$(x_1, \dots, x_n, x_{2n+1}, \dots, x_{3n})$ does not belong to F-subspace of F^{2n} spanned by the rows of the matrix $(A_1 \ A_3)$.*
3. *$(x_{n+1}, \dots, x_{2n}, x_{2n+1}, \dots, x_{3n})$ does not belong to F-subspace of F^{2n} spanned by the rows of the matrix $(A_2 \ A_3)$.*

Proof. For $1 \leq i < j \leq 3$, let Δ_{ij} be the F-subspace of F^{2n} spanned by the rows of the matrix $(A_i \ A_j)$. Let

$$\Omega_{12} = \{(y_1, \dots, y_{3n}) \in F^{3n} \mid (y_1, \dots, y_n, y_{n+1}, \dots, y_{2n}) \in \Delta_{12}\},$$
$$\Omega_{13} = \{(y_1, \dots, y_{3n}) \in F^{3n} \mid (y_1, \dots, y_n, y_{2n+1}, \dots, y_{3n}) \in \Delta_{13}\},$$
$$\Omega_{23} = \{(y_1, \dots, y_{3n}) \in F^{3n} \mid (y_{n+1}, \dots, y_{2n}, y_{2n+1}, \dots, y_{3n}) \in \Delta_{23}\}.$$

Since $\dim_F \Delta_{ij} \leq n$, we have $|\Omega_{ij}| \leq q^{2n}$. Moreover, $(0, \dots, 0) \in \Omega_{12} \cap \Omega_{13} \cap \Omega_{23}$, so $|\Omega_{12} \cup \Omega_{13} \cup \Omega_{23}| \leq |\Omega_{12}| + |\Omega_{13}| + |\Omega_{23}| - |\Omega_{12} \cap \Omega_{13} \cap \Omega_{23}| < 3q^{2n}$. If $q^n > 2$, then $|F^{3n}| = q^{3n} \geq 3q^{2n} > |\Omega_{12} \cup \Omega_{13} \cup \Omega_{23}|$, so there exists $(x_1, \dots, x_{3n}) \in F^{3n} \setminus (\Omega_{12} \cup \Omega_{13} \cup \Omega_{23})$. □

Definition 2.5.5. *A minimal generating set Ω of G of cardinality $m(G)$ is called stable if the following holds: for every $g \in \Omega$ and every $\Delta \subseteq G$, if $G = \langle \Omega \setminus \{g\}, \Delta \rangle$, then there exists $x \in \Delta$ such that $G = \langle \Omega \setminus \{g\}, x \rangle$.*

Lemma 2.5.6. *A finite soluble group contains at least one stable minimal generating set.*

Proof. We procede by induction on $|G|$. Clearly we may assume $\operatorname{Frat} G = 1$. So let $A, R = R_G(A), D, C = C_G(A)$ as in Corollary 1.2.5. There exists a positive integer δ such that $D \cong_G A^\delta$. Moreover, there exists a complement H of D in G with $R \leq H$. Let $d = d(G)$, $a = d(H)$ and $b = m(H)$. Recall that, by [104, Theorem 2], $m(G) = m = b + \delta$. We write $D = V_1 \times \cdots \times V_\delta$ with $V_i \cong_G A$. By induction, H contains a generating set Λ of size b which satisfies the statement of the Lemma. For $1 \leq i \leq \delta$, let v_i be a non trivial element of V_i and let $\Omega = \Lambda \cup \{v_1, \ldots, v_\delta\}$. Clearly Ω is a minimal generating set of G. We claim that Ω satisfies the requested property. Let $g \in \Omega$ and $\Delta \subseteq G$ and assume $G = \langle \Omega \setminus \{g\}, \Delta \rangle$. We distinguish two cases. First assume that $g \in \Lambda$ and denote by π the projection $G \to H$. By induction there exists $x \in \Delta$ such that $H = \langle \Lambda \setminus \{g\}, \pi(x) \rangle$. It can be easily seen that $G = \langle \Omega \setminus \{g\}, x \rangle$. Finally assume $g = v_i$, for some $1 \leq i \leq \delta$. In this case $M = \langle \Omega \setminus \{g\} \rangle$ is a maximal subgroup of G (it is a complement of V_i) and Δ must contain an element $x \notin M$. Clearly $G = \langle \Omega \setminus \{g\}, x \rangle$. □

Notice that not all the minimal generating sets of cardinality $m(G)$ are stable. Consider for example the following group of order 20: $G = \langle a, b \mid a^5 = 1, b^4 = 1, a^b = a^2 \rangle$. We have $m(G) = 2$ and $G = \langle b, b^2a^3 \rangle$. We also have that $G = \langle b^2a^3, a, ba \rangle$, however $\langle b^2a^3, a \rangle = \langle b^2, a \rangle \neq G$ and, since $b^2a^3 = (ba)^2$, $\langle b^2a^3, ba \rangle = \langle ba \rangle \neq G$.

Lemma 2.5.7. *Let G be a soluble non-nilpotent group with $\operatorname{Frat} G = 1$ and choose $A, R = R_G(A), D, C = C_G(A)$ as in Corollary 1.2.5. If G has the extension property, then $m(G/D) \leq 2$*

Proof. There exists a positive integer δ such that $D \cong_G A^\delta$, and, from Lemma 1.2.6, A can be choose to be non-trivial. Moreover, there exists a complement H of D in G with $R \leq H$. Let $d = d(G), m = m(G)$, $a = d(H)$ and $b = m(H)$. As usual, by [104, Theorem 2], $m(G)$ coincides with the number of non-Frattini factors in a chief series of G, hence $m = b + \delta$.

We are going to prove that if $b \geq 3$, then G does not satisfy the extension property. Assume that $b \geq 3$ and let $\{h_1, \ldots, h_b\}$ be a stable generating set of H. We have $C/R = DR/R \cong D \cong A^\delta$ and $G/R \cong C/R \rtimes H/R$ where H/R acts in the same say on each of the δ factors of $C/R \cong A^\delta$ and this action is faithful and irreducible. We denote by $\overline{G}$ the quotient group G/R and, for every $g \in G$, we set $\overline{g} = gR$.

Let $F = \operatorname{End}_G A$ and $n = \dim_F A$. We may identify $\overline{H}$ with a subgroup of $\mathrm{GL}(n, F)$. We denote by A_i the matrix $1 - \overline{h}_i$. We write $D = V_1 \times \cdots \times V_\delta$ with $V_i \cong_G A$. Any $u \in D$ can be written in the form $u = \sum_{1 \leq j \leq \delta} v_j$ with $v_j \in V_j$, so it may be identified with the $\delta \times n$ matrix

$$u = \begin{pmatrix} v_1 \\ \vdots \\ v_\delta \end{pmatrix}.$$

Since A is a non-trivial G-module, $|A| = q^n \neq 2$, so we may choose $x_1, \ldots, x_{3n}$ so that A_1, A_2, A_3 and $(x_1, \ldots, x_{3n})$ satisfy the statement of Lemma 2.5.4. Let

$$w_1 := \begin{pmatrix} x_1 & \cdots & x_n \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}, w_2 := \begin{pmatrix} x_{n+1} & \cdots & x_{2n} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}, \; w_3 := \begin{pmatrix} x_{2n+1} & \cdots & x_{3n} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix},$$

$$u_1 := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \; u_2 := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \; \ldots \; , \; u_{\delta-1} := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

Consider $\omega := \{h_1w_1, h_2w_2, h_3w_3, h_4, \ldots, h_b, u_1, \ldots, u_{\delta-1}\}$. Since the matrix

$$X = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 & \cdots & A_b & 0 & \cdots & 0 \\ w_1 & w_2 & w_3 & 0 & \cdots & 0 & u_1 & \cdots & u_{\delta-1} \end{pmatrix} =$$

$$\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & \cdots & A_b & 0 & \cdots & 0 \\ x_1 \ldots x_n & x_{n+1} \ldots x_{2n} & x_{2n+1} \ldots x_{3n} & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \ldots 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 1 \ldots 0 \end{pmatrix}$$

has rank $n + \delta$, we deduce that ω is a generating set for G. Moreover if we remove the columns corresponding to u_j with $j \in \{1, \ldots, \delta - 1\}$ from the block matrix X we obtain a matrix of lower rank, and this implies that ω is a minimal generating set. We claim that ω has no immediate descendant. Assume that we may obtain a new minimal generating set $\tilde{\omega}$ by replacing $y \in \omega$ by two elements g_1 and g_2. We may write $g_1 = k_1v_1$, $g_2 = k_2v_2$, with $k_1, k_2 \in H$ and $v_1, v_2 \in D$. Let $\omega^* = \omega \setminus \{y\}$. First assume $y = u_j$ for some $1 \leq j \leq \delta-1$. Since ω^* contains $h_1w_1, h_2w_2, h_3w_3, h_4, \ldots, h_b$, we have that $\langle \omega^* \rangle D = G$. Thus a subset containing ω^* generates G if and only if the matrix X^* obtained from X by deleting the columns corresponding to y and adding the columns corresponding to the other generators has rank $n+\delta$. But X^* has rank $n+\delta-1$, so if we add the columns corresponding to g_i (for $1 \leq i \leq 2$), then either the rank remains the same (in which case g_i is a redundant generator) or the rank is $n + \delta$ and in this case $\omega^* \cup \{g_i\}$ is already a generating set. This means that $\tilde{\omega}$ is not a minimal generating set. Now assume $\overline{y} = \overline{h}_j$ for $1 \leq j \leq b$. Since $\tilde{\omega}$ generates G, we must have $H = \langle h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_b, k_1, k_2 \rangle$. Since $h_1, \ldots, h_b$ have been chosen satisfying the statement of Lemma 2.5.6, we may assume $H = \langle h_1, \ldots, h_{j-1}, h_{j+1}, \ldots, h_b, k_1 \rangle$. Our choice of $x_1, \ldots, x_{3n}$ ensures that in this case the matrix the matrix X^* obtained from X by deleting the columns corresponding to y has still rank $n + \delta$ and this implies that g_2 is a redundant generator. □

Lemma 2.5.8. *Assume that G is a finite soluble group with $d(G) = m(G) = 2$.*

1. *If $N \trianglelefteq G$ and G/N is cyclic, then there exists a stable generating set $\{x, y\}$ in G with the property that $x \in N$.*

2. *Let V be an irreducible G-module. If there exists a generating pair $\{g_1, g_2\}$ of G with the property that $C_V(g_1) \neq 0$ and $C_V(g_2) \neq 0$, then there exists also a stable generating pair with the same property.*

Proof. Let $\overline{G} = G/\operatorname{Frat} G$ and for $g \in G$ set $\overline{g} = g \operatorname{Frat} G$. Since $d(G) = m(G) = 2$, then, by [1, Theorem 1.4], either $\overline{G}$ is an elementary p-group of rank 2 or $\overline{G} = P \rtimes Q$ where P is an elementary abelian p-group which is a non-trivial irreducible Q-module and Q is a non-trivial cyclic q-group. If $\overline{G}$ is a p-group then all the generating pairs are stable and there is nothing to prove. So we may assume $\overline{G} = P \rtimes Q$, with P an elementary p-group and $|Q| = q^a$ for some positive integer a. If G/N is cyclic, then $G/(N \operatorname{Frat} G)$ is cyclic, and this implies that $\overline{N}$ contains the Sylow p-subgroup of $\overline{G}$. As a consequence there exists $x \in N$ such that $|\overline{x}| = p$.

Choose y such that $|\overline{y}| = q^a$. We claim that $\{x, y\}$ is a stable generating pair. To see this it suffices to show that $\{\overline{x}, \overline{y}\}$ is a stable generating pair of $\overline{G}$. Notice that if $g \in G$, then $|\overline{g}|$ either divides p or divides q^a and any generating set of $\overline{G}$ contains at least an element of order q^a. If $\Delta \subseteq \overline{G}$ and $\langle \overline{x}, \Delta\rangle = G$ then Δ contains at least one elements $\overline{g}$ of order q^a, hence $\langle \overline{x}, \overline{g}\rangle = \overline{G}$. On the other hand if $\Delta \subseteq \overline{G}$ and $\langle \overline{y}, \Delta\rangle = G$, then Δ contains at least one elements $\overline{g} \notin \langle \overline{y}\rangle$, hence $\langle \overline{y}, \overline{g}\rangle = \overline{G}$ (since $\langle \overline{y}\rangle$ is a maximal subgroup of $\overline{G}$). This proves (1). Now we want to prove (2), in the case when G is not a p-group. Suppose that the generating pair $\{g_1, g_2\}$ has the property that $C_V(g_1) \neq 0$ and $C_V(g_2) \neq 0$. As we notice before, we may assume $|\overline{g_1}| = q^a$. Choose $\overline{x} \notin N_{\overline{G}}(\langle \overline{g_1}\rangle)$. It can be easily seen that $G = \langle g_1, g_1^x\rangle$ and clearly $|C_V(g_1^x)| = |C_V(g_1)| \neq 0$. Arguing as before, it can be easily seen that $\{g_1, g_1^x\}$ is a stable generating set. □

Lemma 2.5.9. *Let H be a finite soluble group with $m(H) = 2$ and let V be a non-trivial irreducible H-module. Moreover assume $\delta_H(V) = 0$. Let $F = \mathrm{End}_H(V)$ and $n = \dim_F(V)$. Consider the semidirect product $G = V^\delta \rtimes H$. If G has the extension property, then the following hold.*

1. *H is not cyclic.*
2. *$\delta = 1$.*
3. *if $\{h_1, h_2\}$ is a minimal generating set of H, then there exists $i \in \{1, 2\}$ such that $C_V(h_i) = \{0\}$.*

Proof. Write $V^\delta = V_1 \times \cdots \times V_\delta$ and let $\overline{H} = H/C_H(V) \leq \mathrm{GL}(n, q)$ and, for every $h \in H$, set $\overline{h} = hC_H(V)$. The assumption $\delta_H(V) = 0$ implies that $C_G(V) = V^\delta C_H(V)$ and $R_G(V) = C_H(V)$. By Corollary 1.2.5, if $\langle h_1, h_2\rangle = H$ and $u_1, u_2 \in D = V^\delta$, then $\langle h_1u_1, h_2u_2\rangle = G$ if and only if $\langle h_1u_1, h_2u_2\rangle C_H(V) = G$.

Suppose that $H = \langle h\rangle$ is cyclic. For $1 \leq i \leq \delta$, let v_i be a non trivial element of V_i. The set $\omega = \{h, hv_1, v_2, \ldots, v_\delta\}$ is a minimal generating set of G and $|\omega| = \delta + 1 < m(G) = \delta + 2$. On the other hand if we remove one element from ω, the remaining elements generate a maximal subgroup of G. So ω has no immediate descendent and G cannot satisfy the extension property. This proves (1).

We now prove (2). First, we assume $n \neq 1$. Let $\{h_1, h_2\}$ be a stable minimal generating set of H (its existence is ensured by Lemma 2.5.6). Now, choose $x_1, \ldots, x_{2n} \in F$ such that $(x_1, \ldots, x_{2n})$ do not belong to the subspace of F^{2n} spanned by the rows of the matrix $\begin{pmatrix} A_1 & A_2 \end{pmatrix}$, where $A_i = 1 - \overline{h_i}$. Assume that $(y_1, \ldots, y_n)$ and $(z_1, \ldots, z_n)$ are two F-linearly independent elements of F^n. If $\delta \geq 2$, then define

$$w_1 := \begin{pmatrix} x_1 & \cdots & x_n \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}, w_2 := \begin{pmatrix} x_{n+1} & \cdots & x_{2n} \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix},$$

$$u_1 := \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ z_1 & z_2 & \cdots & z_n \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, u_2 := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \ldots, u_{\delta-1} := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

As in the proof of Lemma 2.5.7, it can be noticed that $\omega := \{h_1w_1, h_2w_2, u_1, \ldots, u_{\delta-1}\}$ is a minimal generating set of G. Assume that we may obtain a new minimal generating set $\tilde{\omega}$ by

replacing $y \in \omega$ by two elements g_1 and g_2. We write $g_1 = k_1v_1$, $g_2 = k_2v_2$, with $k_1, k_2 \in H$ and $v_1, v_2 \in D$. If $y = u_i$ for some $i \in \{1, \dots, \delta - 1\}$, then $\omega \setminus \{y\}$ generated a maximal subgroup of G (indeed a complement of V_{i+1}), so it must be $y \in \{h_1w_1, h_2w_2\}$. Assume for example $y = h_1w_1$. Since $\langle \tilde{\omega} \rangle = G$, we must have $H = \langle h_2, k_1, k_2 \rangle$. Since $\langle h_1, h_2 \rangle$ is a stable generating set, we may assume $H = \langle h_2, k_1 \rangle$. Let $B_1 = 1 - \overline{k_1}$. Our choice of $u_1, \dots, u_{\delta-1}$ ensures that in this case the matrix

$$X^* = \begin{pmatrix} B_1 & A_2 & 0 & \cdots & 0 \\ v_1 & w_2 & u_1 & \cdots & u_{\delta-1} \end{pmatrix}$$

has still rank $n + \delta$ and this implies that g_2 is a redundant generator. Thus (2) has been proved when $n > 1$. Suppose now $n = 1$. In particular $H/C_H(V) \leq \mathrm{GL}(1, F)$ is cyclic and so, by Lemma 2.5.8, we can find a stable generating pair $\{h_1, h_2\}$ such that $H = \langle h_1, h_2 \rangle$, $h_1 \notin C_H(V)$, $h_2 \in C_H(V)$. Assume $\delta > 1$ and for $1 \leq i \leq \delta$, let v_i be a non trivial element of V_i (so that v_i corresponds to a matrix in $M_{\delta,1}(F)$ with 0 everywhere, except in the i-th row). We claim that the set $\omega = \{h_1, h_2v_1, \dots, h_2v_\delta\}$ is a minimal generating set with no immediate descendent. Assume that we may obtain a new minimal generating set $\tilde{\omega}$ by replacing $y \in \omega$ by two elements g_1 and g_2. We write $g_1 = k_1w_1$, $g_2 = k_2w_2$, with $k_1, k_2 \in H$ and $w_1, w_2 \in D$. For every $1 \leq i \leq \delta$, the subset $\omega \setminus \{h_2v_i\}$ generates a complement of V_i in G, so we must have $y = h_1$. Since $\{h_1, h_2\}$ is stable, we may assume $H = \langle h_2, k_1 \rangle$. Since V is a non-trivial H-module and $\overline{h_2} = 1$, we have $1 - \overline{k_1} \neq 0$. Thus the matrix

$$X^* = \begin{pmatrix} 1 - \overline{k_1} & 0 & \cdots & 0 \\ w_1 & v_1 & \cdots & v_\delta \end{pmatrix}$$

has still rank $1 + \delta$ and this implies that g_2 is a redundant generator. So G does not satisfies the extension property.

Now we may prove (3), under the additional assumption $\delta = 1$. We want to prove that if there exists a generating set $\{h_1, h_2\}$ such that $C_V(h_1) \neq 0$ and $C_V(h_2) \neq 0$ then G cannot satisfies the extension property. By Lemma 2.5.8, we may assume that $\{h_1, h_2\}$ is a stable generating set. We identify H with a subgroup of $\mathrm{GL}(n, F)$. Choose $(x_1, \dots, x_n)$ which does not belong to the vector space spanned by the rows of the matrix $A_1 = 1 - \overline{h_1}$ and $(x_{n+1}, \dots, x_{2n})$ which does not belong to the vector space spanned by the rows of the matrix $A_2 = 1 - \overline{h_2}$. Define $w_1 = (x_1, \dots, x_n)$ and $w_2 = (x_{n+1}, \dots, x_{2n})$. The set $\omega := \{h_1w_1, h_2w_2\}$ is a minimal generating set of G. Assume that we may obtain a new minimal generating set $\tilde{\omega}$ by replacing $y \in \omega$ by two elements g_1 and g_2. We write $g_1 = y_1v_1$, $g_2 = y_2v_2$, with $y_1, y_2 \in H$ and $v_1, v_2 \in D$. Assume for example $y = h_1w_1$. Since $\langle \tilde{\omega} \rangle = G$, we must have $H = \langle h_2, y_1, y_2 \rangle$. Being $\{h_1, h_2\}$ stable, we may assume $H = \langle h_2, y_1 \rangle$. Let $B_1 = 1 - \overline{y_1}$. Since $H = \langle h_2, y_1 \rangle$, we have $\mathrm{rank} \begin{pmatrix} B_1 & A_2 \end{pmatrix} = n$. Moreover, our choice of $x_{n+1}, \dots, x_{2n}$ ensures that

$$\mathrm{rank} \begin{pmatrix} B_1 & A_2 \\ v_1 & w_2 \end{pmatrix} = n + 1.$$

This implies that $G = \langle g_1, h_2w_2 \rangle$ and so g_2 is a redundant generator. This completes the proof of (3). □

Proof of Theorem 2.0.18. If G is nilpotent, then the statement follows from Proposition 2.5.3.

Assume that G is soluble, non-nilpotent, finite group with the extension property. Clearly $G/\operatorname{Frat} G$ satisfies also the extension property so, by Lemma 2.5.7, $G/\operatorname{Frat} G = V^\delta \rtimes H$, where $m(H) \leq 2$ and V is a non-trivial irreducible H-module. If $m(H) = 1$, then $d(G) = d(G/\operatorname{Frat} G) = \delta + 1 = m(G/\operatorname{Frat} G) = m(G)$. If $m(H) = 2$, then $\delta = 1$ by Lemma 2.5.9. In this case $d(G) = d(G/\operatorname{Frat} G) = 2$ and $m(G) = m(G/\operatorname{Frat} G) = 3$.

Now, we want prove that if G satisfies either (1) or (2) then G has the extension property. Clearly the statement is true if $d(G) = m(G)$. Since G satisfies the extension property if and only if $G/\operatorname{Frat} G$ satisfies the extension property, to conclude our proof, we have to prove that if $G = V \rtimes H$ is a semidirect product with the properties described in (2), then every generating pair (g_1, g_2) of G has a strong immediate descendant. Let $g_1 = h_1 v_1$ and $g_2 = h_2 v_2$, with $h_1, h_2 \in H$ and $v_1, v_2 \in V$. It is not restrictive to assume $C_V(h_1) = 0$. In particular, the set $\{h_1^w \mid w \in V\}$ has size $|V : C_V(h_1)| = |V|$, and consequently $\{h_1^w \mid w \in V\} = \{h_1 w \mid w \in V\}$. That is, there exists $w \in V$ such that $g_1 = h_1^w$. We have that $g_2 = h_2^w [w, h_2] v_2$ and that $\{h_1^w, h_2^w, [w, h_2] v_2\}$ is a minimal generating set of G. □

Chapter 3

Problems in permutation groups

Let the permutation group G act on a set Ω of size n. A subset $\mathcal{B}$ of Ω is a *base* for G if the pointwise stabilizer $G_{(\mathcal{B})}$ is trivial. The *base size* of G is the minimal cardinality of a base for G, and we denote this by $b(G, \Omega)$, or just $b(G)$ when the meaning is clear. Equivalently, $b(G)$ is the minimal cardinality of a set of conjugates of a pointstabiliser H such that their intersection is trivial. Determining the base size of a given permutation group is a classical problem in permutation group theory, with a long tradition and many applications.

In the 19th century, a problem that attracted a lot of attention was that of bounding the order of a finite primitive permutation group. Since the elements of G are uniquely determined by their effect on a base, then

$$|G| \leq |\Omega|^{b(G)}. \tag{3.0.1}$$

So one can find an upper bound on the order of a permutation group by bounding the minimal base size. One of the earliest results in this direction is a theorem of Bochert [17] from 1889, which states that if G is a primitive permutation group of degree n not containing the alternating group $\mathrm{Alt}(n)$, then $b(G) \leq n/2$. The permutation group G is *large base* if there exist integers m and $r \geq 1$ such that $\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \mathrm{wr} \mathrm{Sym}(r)$, where the action of $\mathrm{Sym}(m)$ is on k-element subsets of $\{1, \ldots, m\}$ and the wreath product acts with product action. Note that this includes the natural action of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$. Using the Classification of Finite Simple Groups and building on earlier work by Cameron [31], Liebeck proved the following remarkable result.

Theorem 3.0.1 (Liebeck, [86])**.** *Let G be a primitive permutation group of degree n. If G is not large base, then $b(G) \leq 9 \log n$.*

From (3.0.1) it follows that $b(G) \geq \log |G| / \log n$ for every permutation group of degree n. On the other hand, in 1993, Pyber [138] asked whether there exists a universal constant c such that $b(G) \leq c \log |G| / \log n$ for any primitive group G of degree n. This question generalizes the Cameron–Kantor conjecture [32, 35], which asserts that there exists an absolute constant c such that $b(G) \leq c$ for all finite almost simple groups G in faithful primitive nonstandard actions (non-standard actions are defined in Definition 3.1.20). In [26, Theorem 1.3], Liebeck and Shalev proved the Cameron–Kantor conjecture, but without specifying the absolute constant c. In a series of papers [22, 27, 25], Burness and others proved that $b(G) \leq 7$, with equality if and only if H is the largest Mathieu group M_{24} in its 5-transitive action of degree 24; that is, the Cameron-Kantor conjecture is true with the constant $c = 7$. Despite the great attention, Pyber's conjecture remained open until very recently. Starting on earlier work of Benbenishty [15], Burness et al. [22, 27, 25, 28], Fawcett [52], Gluck and Magaard [54], Halasi and Maróti [66], Liebeck and Shalev [89, 90], and Seress [150], it is shown in [50] that there exists a universal constant c such that $b(G) \leq 45(\log |G| / \log n) + c$, for every

primitive permutation group G of degree n. Much more recently, Liebeck, Halasi and Maróti showed in [65, Proof of Corollary 1.3] that for almost all non-large base primitive groups, $b(G) \leq 2\lfloor \log n \rfloor + 26$; then Roney-Dougal and Siccha noted in [145] that this bound applies to all primitive groups that are not large base. In [122], we prove a better estimation for the base size of a non-large base primitive groups. Precisely the following result holds.

Theorem 3.0.2. *Let G be a primitive permutation group of degree n. If G is not large base then $b(G) \leq \max\{7, \lceil \log n \rceil + 1\}$. Furthermore, there are infinitely many such groups G for which $b(G) > \log n + 1$.*

Notice that if G is the largest Mathieu group M_{24} in its 5-transitive action of degree 24 then $b(G) = 7 > \lceil \log n \rceil + 1$. We shall prove in Proposition 3.1.33 that if $G = \mathrm{Sp}_{2m}(2)$, acting on the cosets of the maximal subgroup $\mathrm{GO}^-_{2m}(2)$, then $b(G) = \lceil \log n \rceil + 1 > \log n + 1$. In Section 3.1 we prove Theorem 3.0.2 using the version of the O'Nan-Scott theorem presented in [92] (see Section 1.5).

In computational group theory, the elements of $G \leq \mathrm{Sym}(\Omega)$ are stored as $|\Omega|$-tuples; hence, from (3.0.1), it follows that the element of G can be stored as $b(G)$-tuples. Clearly it is more convenient to store $b(G)$-tuples, rather than $|\Omega|$-tuples; whence Theorem 3.0.2 and bounds on the base size in general are not only appealing for their own sake, but can also be used for practical applications (see [149, Chapter 4] for further details).

Another question motivated by computational interest in permutation group theory is the following.

Question 2. [30] *Is the number of maximal blocks of imprimitivity through a point for a transitive group G of degree n bounded above polynomially in terms of degree n?*

This question was firstly asked by Cameron (see [30] for the motivation for this question), and extends naturally an old question. Let us explain this better. In 1961, Wall [160] has conjectured that the number of maximal subgroups of a finite group G is less than the group order $|G|$. Wall himself proved the conjecture under the additional hypothesis that G is soluble. The first remarkable progress towards a good understanding of Wall's conjecture is due to Liebeck, Pyber and Shalev [95]; they proved that all, but (possibly) finitely many, simple groups satisfy Wall's conjecture. Actually, Liebeck, Pyber and Shalev proved [95, Theorem 1.3] a polynomial version of Wall's conjecture: there exists an absolute constant c such that, every finite group G has at most $c|G|^{3/2}$ maximal subgroups. Based on the conjecture of Guralnick on the dimension of certain first cohomology groups [62] and on some computer computations of Frank Lübeck, Wall's conjecture was disproved in 2012 by the participants of an AIM workshop, see [63].

To see that Question 2 extends naturally the question of Wall we fix some notation. Given a finite group G and a subgroup H of G, we denote by

$$\max(H, G) := |\{M \mid M \text{ maximal subgroup of } G \text{ with } H \leq M\}|,$$

the number of maximal subgroups of G containing H. Now, if Ω is the domain of a transitive permutation group G and $\omega \in \Omega$, then there exists a one-to-one correspondence between the maximal systems of imprimitivity of G and the maximal subgroups of G containing the point stabiliser G_ω and hence Question 2 asks for a polynomial upper bound for $\max(G_\omega, G)$ as a function of $n = |G : G_\omega|$. When $n = |G|$, that is, G acts regularly on itself, the question of Cameron reduces to the question of Wall and [95, Theorem 1.3] yields a positive solution in this case, with exponent $3/2$. In [112] we gave a positive solution to Question 2.

Theorem 3.0.3. [112, Theorem 1.2] *There exists a constant a such that, for every finite group G and for every subgroup H of G, we have $\max(H, G) \leq a|G : H|^{3/2}$. In particular, a transitive permutation group of degree n has at most $an^{3/2}$ maximal systems of imprimitivity.*

In the case of soluble groups we actually obtain a much tighter bound, which extends the result of Wall [160, (8.6), page 58] for soluble groups on his own conjecture.

Theorem 3.0.4. [112, Theorem 1.3] *If G is a finite soluble group and H is a proper subgroup of G, then* $\max(H, G) \leq |G : H| - 1$. *In particular, a soluble transitive permutation group of degree $n \geq 2$ has at most $n - 1$ maximal systems of imprimitivity.*

With the use of the crowns 1.2 we prove Theorems 3.0.3, 3.0.4 in Section 3.2

Finally, in [111], we analyzed a problem quite different in permutation group theory. Let us introduce the general setting. Let G be a finite group, let H be a subgroup of G, and let

$$\mathcal{O}_G(H) := \{K \mid K \text{ subgroup of } G \text{ with } H \leq K\}$$

be the set of subgroups of G containing H. Clearly, $\mathcal{O}_G(H)$ is a lattice under the operations of taking "intersection" and taking "subgroup generated"; it is called the *overgroup lattice*. The problem of determining whether every finite lattice is isomorphic to some $\mathcal{O}_G(H)$ for a finite group G arose originally in universal algebra with the work of Pálfy-Pudlák [132]. In 1938, Ore proved that a finite group is cyclic if and only if its subgroup lattice is distributive [127, Theorem 4]. Further he proved that for a finite group G and a subgroup H of G such that the overgroup lattice $\mathcal{O}_G(H)$ is distributive, then there exists a coset Hg generating G [127, Theorem 7]. In [130], Palcoux obtained a dual version of Ore's theorem, more precisely, he proved that if $\mathcal{O}_G(H)$ is distributive then there exists an irreducible complex representation V of G such that $G_{(V^H)} = H$ (where V^H is the H-fixed points subspace of V). Let G be a finite group, the *Euler totient of* G, $\varphi(G)$, is the number of elements g such that $\langle g \rangle = G$. Then $\varphi(G)$ is nonzero if and only if G is cyclic, and when $G = C_n$ is the cyclic group of order n, $\varphi(C_n)$ coincides with the usual Euler's totient function $\varphi(n)$. For a subgroup $H \subset G$, the *Euler totient* $\varphi(H, G)$ is the number of cosets Hg such that $\langle Hg \rangle = G$. Hall [64] described $\varphi(H, G)$ in terms of the Möbius function μ on the overgroup lattice $\mathcal{O}_G(H)$, precisely he showed that

$$\varphi(H, G) = \sum_{K \in \mathcal{O}_G(H)} \mu(K, G)|K : H|.$$

Note that $\varphi(H, G)$ is nonzero (if and) only if there is a coset Hg generating G. In [131] it was proved that for any subgroup $H \subset G$, if the *dual Euler totient*

$$\hat{\varphi}(H, G) := \sum_{K \in \mathcal{O}_G(H)} \mu(H, K)|G : K|,$$

is nonzero then there is an irreducible complex representation V such that $G_{(V^H)} = H$ (in particular, if $\hat{\varphi}(G) := \hat{\varphi}(1, G)$ is nonzero then G is *linearly primitive*, that is G admits a faithful irreducible complex representation).

So the dual Ore's theorem appears as a natural consequence of the following conjecture:

Conjecture 6. [13, Conjecture 1.5] *If $\mathcal{O}_G(H)$ is Boolean, then $\hat{\varphi}(H, G)$ is nonzero.*

(See Subsection 3.3.1 for the definition of boolean lattice.) In [13, page 58], the authors asked whether the lower bound $\hat{\varphi}(H, G) \geq 2^\ell$ holds when $\mathcal{O}_G(H)$ is Boolean of rank $\ell + 1$. As they pointed out, if the lower bound is correct, then it is optimal because $\hat{\varphi}(S_1 \times S_2^\ell, S_2 \times S_3^\ell) = 2^\ell$. To highlight previous progress on this context, let us consider the *(reduced) Euler characteristic*:

$$\chi(H, G) = -\sum_{K \in \mathcal{O}_G(H)} \mu(K, G)|G : K|.$$

The Euler characteristic is an invariant related to $\hat{\varphi}(H, G)$ in the following sense: when $K \in \mathcal{O}_G(H)$, and $\mathcal{O}_G(H)$ is Boolean of rank ℓ, then $\mu(K, G) = (-1)^\ell \mu(H, K)$, so that

$\chi(H,G) = \pm\hat{\varphi}(H,G)$. It follows that Conjecture 6 reduces to investigation of the non-vanishing of $\chi(H,G)$. The problem of studying whether $\chi(G) := \chi(1,G)$ is nonzero for every finite group G is mentioned as open in [152, page 760] and attributed to Brown. It was first approached by Gaschütz, who showed in [55] that $\chi(G) \neq 0$ when G is a solvable group. Later, Patassini proved that $\chi(G) \neq 0$ for many almost simple groups G in [134, 135], and obtained further results for some groups with minimal normal subgroups that are products of alternating groups in [136]. Despite these results, it is still unknown whether $\chi(G)$ is nonzero for every finite group G.

A first step to attack Conjecture 6 could be to prove the case where G is a finite simple group, hence as a preliminary aim one should try to classify the inclusions $H \subset G$ when G is finite simple group and $\mathcal{O}_G(H)$ Boolean. In [13, Example 4.21] it is noticed that if H is the Borel subgroup of a BN-pair structure (of rank ℓ) on G, then $\mathcal{O}_G(H)$ is Boolean (of rank ℓ), and $\chi(H,G)$ is nonzero, moreover if G is a finite simple group of Lie type (over a finite field of characteristic p) then its absolute value $\hat{\varphi}(H,G)$ is the p-contribution in the order of G, which is at least $p^{\frac{1}{2}\ell(\ell+1)}$. Further, Shareshian suggestes us examples of boolean $\mathcal{O}_G(H)$ of any rank when G is the alternating group, involving stabilizers of non-trivial regular partitions, as shown in [8] for the rank 2. In [111] not only we proved the existence of these examples for G alternating (or symmetric), but mainly we showed that (besides some sporadic cases) there is just one other infinite family of examples arising from stabilizers of regular product structures. As a consequence, Conjecture 6 holds true in this case (together with the expected lower bound).

Let G be an almost simple group with socle an alternating group $\mathrm{Alt}(n)$, for some $n \in \mathbb{N}$. When $n \leq 5$, nothing interesting happens: the largest Boolean lattice of the form $\mathcal{O}_G(H)$ has rank at most 1. Moreover, when $G = \mathrm{Alt}(6)$, the largest Boolean lattice has rank 2 and it is of the form $(D_4, \mathrm{Sym}(4), \mathrm{Sym}(4))$ or $(D_5, \mathrm{Alt}(5), \mathrm{Alt}(5))$. When G is $\mathrm{PGL}_2(9)$, M_{10} or $\mathrm{P\Gamma L}_2(9)$, the largest Boolean lattice has rank 1. When $G = \mathrm{Sym}(6) \cong \mathrm{P\Sigma L}_2(9)$, the largest Boolean lattice has rank 2 and it is of the form $(D_4 \times C_2, 2.\mathrm{Sym}(4), 2.\mathrm{Sym}(4))$ or $(C_5 \rtimes C_4, \mathrm{Sym}(5), \mathrm{Sym}(5))$. Hence for the rest of this chapter we can assume that G is either $\mathrm{Alt}(\Omega)$ or $\mathrm{Sym}(\Omega)$, for some a finite set Ω of size bigger than 7. The statement of the following theorem contains terms which are defined in Section 3.3.

Theorem 3.0.5. [111, Theorem 1.2] *Let Ω be a finite set, let G be $\mathrm{Alt}(\Omega)$ or $\mathrm{Sym}(\Omega)$, let H be a subgroup of G and suppose that the lattice $\mathcal{O}_G(H) = \{K \mid H \leq K \leq G\}$ is Boolean of rank $\ell \geq 3$. Let $G_1, \ldots, G_\ell$ be the maximal elements of $\mathcal{O}_G(H)$. Then one of the following holds:*

1. *For every $i \in \{1, \ldots, \ell\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$; moreover, relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $\Sigma_1 < \cdots < \Sigma_\ell$.*

2. *$G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$; moreover, relabeling the index set $\{1, \ldots, \ell - 1\}$ if necessary, $\Sigma_1 < \cdots < \Sigma_{\ell-1}$.*

3. *$|\Omega|$ is odd. For every $i \in \{1, \ldots, \ell\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_\ell$.*

4. *$|\Omega|$ is an odd and $G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell - 1\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-1}$.*

5. *$|\Omega|$ is an odd prime power. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, G_ℓ is maximal subgroup of O'Nan-Scott type HA, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial*

regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1,\dots,\ell-1\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-1}$.

6. *$|\Omega|$ is odd prime power and $G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1,\dots,\ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$ and $G_{\ell-1}$ is a maximal subgroup of O'Nan-Scott type HA, for every $i \in \{1,\dots,\ell-2\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1,\dots,\ell-2\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-2}$.*

7. *$\ell = 3$, $G = \mathrm{Sym}(\Omega)$ and, relabeling the index set $\{1,2,3\}$ if necessary, G_1 is the stabilizer of a subset Γ of Ω with $1 \leq |\Gamma| < |\Omega|/2$, G_2 is the stabilizer of a non-trivial regular partition Σ with $\Gamma \in \Sigma$ and $G_3 = \mathrm{Alt}(\Omega)$;*

8. *$\ell = 3$, $G = \mathrm{Sym}(\Omega)$ and, relabeling the index set $\{1,2,3\}$ if necessary, G_1 is the stabilizer of a subset Γ of Ω with $|\Gamma| = 1$, $G_2 \cong \mathrm{PGL}_2(p)$ for some prime number p, $|\Omega| = p+1$ and $G_3 = \mathrm{Alt}(\Omega)$;*

9. *$\ell = 3$, $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$ and the Boolean lattice $\mathcal{O}_G(H)$ is in Figure 3.2.*

10. *$\ell = 3$, $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 24$, and, relabeling the index set $\{1,2,3\}$ if necessary, G_1 is the stabilizer of a subset Γ of Ω with $|\Gamma| = 1$, $G_2 \cong G_3 \cong M_{24}$.*

In Subsection 3.3.6 we prove Theorem 3.0.5. In Subsection 3.3.7, we show that the cases in Theorem 3.0.5 (1) and (2) do occur for arbitrary values of ℓ. In Subsection 3.3.8, we show that there exist Boolean lattices of arbitrary large rank whose maximal elements are stabilizers of regular product structures.

Finally, Section 3.3.9 is dedicated to the proof of the following theorem where (4) is a consequence of Theorem 3.0.5, and where the proof for (5) was already mentioned above.

Theorem 3.0.6. [111, Theorem 1.3] *Let G be a finite group and H a subgroup such that the overgroup lattice $\mathcal{O}_G(H)$ is Boolean of rank ℓ. Then the lower bound on the dual Euler totient $\hat{\varphi}(H,G) \geq 2^{\ell-1}$ holds in each of the following cases:*

1. *$\ell \leq 3$,*

2. *$\mathcal{O}_G(H)$ group-complemented,*

3. *G solvable,*

4. *G alternating or symmetric,*

5. *G of Lie type and H a Borel subgroup.*

As a consequence, the reduced Euler characteristic $\chi(H,G)$ is nonzero.

3.1 Base size of primitive permutation group

The proof is divided in various steps, and for this proof we use the version of the O'Nan-Scott theorem presented in [92] (see 1.5).

The bulk of the proof is the the almost simple case, hence we analyze this case in various subsections. In Subsection 3.1.1 we estimate the base of an almost simple group G acting on a G-orbit of (totally singular or non-degenerate of a fixed isometry type) one- and two-subspace of the natural module V in terms of the dimension of V. In Subsection 3.1.2 we give the Definition 3.1.20 of a standard action of an almost simple group, and we deal with the almost simple groups in non-standard actions. In Subsection 3.1.3 we analyze the case when the group is an alternating or a symmetric group acting on partitions. Then in Subsection 3.1.4 we deal with subspace actions. Finally, in Subsection 3.1.5 we prove Theorem 3.0.2.

The following easy result is used throughout this Section.

Lemma 3.1.1. *To bound the base size of the primitive groups G that are not large base, it suffices to bound the base size of those primitive groups G that are maximal amongst the non-large-base groups G.*

Proof. Let $H \leq G \leq \mathrm{Sym}(n)$, and let $\mathcal{B}$ be a base for G. Then $H_{(\mathcal{B})} \leq G_{(\mathcal{B})} = 1$, so $\mathcal{B}$ is a base for H. Hence $b(H) \leq b(G)$. □

3.1.1 One- and Two-dimensional subspaces

Let G be an almost simple classical group G with natural module V. In this section we analyze the action of G acting on a G-orbit of totally singular or non-degenerate one- or two-dimensional subspaces of V. We start by collecting some preliminaries results and Definitions.

Notation 1. *Let $A \in \mathrm{GL}_d(q)$. If A is block diagonal, of the form*

$$A = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_t \end{bmatrix}$$

with $A_i \in \mathrm{GL}_{d_i}(q)$ for $1 \leq i \leq t$, then we write $A = \mathrm{Diag}(A_1, A_2, \ldots, A_t)$. If $d_i = 1$ for all i, then we also write $A = \mathrm{Diag}(\alpha_1, \ldots, \alpha_d)$.

We write $\mathbb{F}^*$ for the nonzero elements of the finite field $\mathbb{F}$.

Lemma 3.1.2. *Let $V = \mathbb{F}_q^d$ and let $G = \mathrm{GL}_d(q)$. Let $v_1, \ldots, v_d$ be linearly independent elements of V, and let $S = \{\langle v_1 \rangle, \ldots, \langle v_d \rangle\}$.*

(1) $G_{(S)}$ is conjugate to a group of diagonal matrices, and is trivial when $q = 2$.

(2) For all $\mu := (\mu_1, \ldots, \mu_d) \in (\mathbb{F}_q^*)^d$, let $S(\mu) = S \cup \{\langle \mu_1 v_1 + \cdots + \mu_d v_d \rangle\}$. Then $G_{(S(\mu))} = Z(\mathrm{GL}_d(q))$.

Proof. (1) Let $g \in G_{(S)}$, then there exist $\lambda_1, \ldots, \lambda_d \in \mathbb{F}_q$ such that $v_i g = \lambda_i v_i$, for $1 \leq i \leq m$. Hence with respect to the basis $v_1, \ldots v_d$ the group $G_{(S)}$ consists of diagonal matrices. The second claim is immediate.

(2) Let $g \in G_{S(\mu)}$. By Part (1), with respect to the basis $v_1, \ldots, v_d$ the matrix g is equal to $\mathrm{Diag}(\lambda_1, \ldots, \lambda_d)$. Furthermore, there exists an $\alpha \in \mathbb{F}_q^*$ such that

$$(\mu_1 v_1 + \cdots + \mu_d v_d)g = \lambda_1 \mu_1 v_1 + \cdots + \lambda_d \mu_d v_d = \alpha(\mu_1 v_1 + \cdots + \mu_d v_d),$$

and consequently $\lambda_1 = \cdots = \lambda_d = \alpha$. □

Lemma 3.1.3. *Let B be a non-degenerate sesquilinear form on $V = \mathbb{F}^d$, with $d > 2$. Let $\mathbb{F} = \mathbb{F}_q$ if B is bilinear, and $\mathbb{F} = \mathbb{F}_{q^2}$ otherwise. Let $u, v \in V$ be such that $\langle u, v \rangle$ is non-degenerate. Let g be an isometry of V such that $ug = \alpha u$ for some $\alpha \in \mathbb{F}^*$.*

1. *Assume that $vg = \beta v$, for some $\beta \in \mathbb{F}^*$, and that there exist a nonzero $w \in \langle u, v \rangle^\perp$, $\gamma_1, \gamma_3 \in \mathbb{F}^*$, and $\gamma_2 \in \mathbb{F}$, such that g stabilizes $\langle \gamma_1 u + \gamma_2 v + \gamma_3 w \rangle$. Then $wg = \alpha w$. Furthermore, if $\gamma_2 \neq 0$ then $\beta = \alpha$, and if, in addition, $B(u, v) \neq 0$ then $\alpha = \alpha^{-q}$.*

2. *Assume that B is symmetric, and that (u, v) satisfy $B(u, u) = B(v, v) = 0$ and $B(u, v) = 1$. If g stabilizes $\langle u, v \rangle$, then $vg = \alpha^{-1} v$.*

Proof. (1). Since $\langle u, v\rangle$ is non-degenerate, we can write $V = \langle u, v\rangle \oplus \langle u, v\rangle^{\perp}$. Let $\{u, v, w, w_4 \ldots, w_d\}$ be a basis of V such that $w, w_4, \ldots, w_d$ is a basis of $\langle u, v\rangle^{\perp}$. Since g stabilizes $\langle u, v\rangle$, the matrix g also stabilises $\langle u, v\rangle^{\perp}$. In particular, there exist $\lambda_0, \lambda_4, \ldots, \lambda_d$ such that $wg = \lambda_0 w + \sum_{i=4}^{d} \lambda_i w_i$. Further, there exists $\mu \in \mathbb{F}_q$ such that

$$\mu(\gamma_1 u + \gamma_2 v + \gamma_3 w) = (\gamma_1 u + \gamma_2 v + \gamma_3 w)g = \gamma_1 \alpha u + \gamma_2 \beta v + \gamma_3(\lambda_0 w + \sum_{i=4}^{d} \lambda_i w_i).$$

Hence $\mu = \alpha = \lambda_0$ and $\lambda_i = 0$ for $4 \leq i \leq d$. Furthermore, if $\gamma_2 \neq 0$ then $\mu = \beta$. The final claim is clear.
(2). There exist $\beta, \gamma \in \mathbb{F}^*$, such that $vg = \beta u + \gamma v$. Since

$$0 = B(v, v) = B(vg, vg) = B(\beta u + \gamma v, \beta u + \gamma v) = 2\beta\gamma,$$

either β or γ is 0. Furthermore,

$$1 = B(ug, vg) = \alpha\gamma$$

yields that $\gamma = \alpha^{-1} \neq 0$. Consequently $\beta = 0$. □

Lemma 3.1.4. *Let $G = \mathrm{GL}_d(q)$ and let Ω be the set of 2-spaces of $V = \mathbb{F}_q^d$. Let $d = 2a + r$ with $0 \leq r \leq 1$ and let $V = V_1 \oplus \cdots \oplus V_a \oplus U = X \oplus U$ be any direct sum decomposition with $\dim V_i = 2$ for all $1 \leq i \leq a$ and $\dim U = r$. For $1 \leq i \leq a$, let $v_{i,1}, v_{i,2}$ be linearly independent vectors in V_i.*

(1) Let $g \in G_{(V_1,\ldots,V_a)}$. Then with respect to any basis beginning $v_{1,1}, v_{1,2}, \ldots, v_{a,1}, v_{a,2}$ the restriction $g\,|_X = \mathrm{Diag}(X_1, \ldots, X_a)$, with $X_i \in \mathrm{GL}_2(q)$ for every $1 \leq i \leq a$.

(2) Let $I \subseteq \{1, \ldots, a\}$, let $w_1 = \sum_{i\in I} v_{i,1}$, let $w_2 = \sum_{i\in I} v_{i,2}$, and let $W = \langle w_1, w_2\rangle$. Let $g \in G_{(V_1,\ldots,V_a,W)}$. Then $g\,|_X = \mathrm{Diag}(X_1, \ldots, X_1)$, with $X_1 \in \mathrm{GL}_2(q)$.

Proof. (1) Since $V_i g = V_i$, there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}_q$ such that $v_{i,1}g = \alpha_i v_{i,1} + \beta_i v_{i,2}$, and $v_{i,2}g = \gamma_i v_{i,1} + \delta_i v_{i,2}$.

(2) For $1 \leq i \leq a$ the matrix $X_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix}$. Since $Wg = g$, there exist $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ such that

$$w_1 g = \sum_{i\in I} (\alpha_i v_{i,1} + \beta_i v_{i,2}) = \alpha w_1 + \beta w_2,$$
$$w_2 g = \sum_{i\in I} (\gamma_i v_{i,1} + \delta_i i v_{i,2}) = \gamma w_1 + \delta w_2.$$

Hence $\alpha_i = \alpha, \beta_i = \beta, \gamma_i = \gamma$ and $\delta_i = \delta$, for all $i \in I$. □

Lemma 3.1.5. *Let G be a finite almost simple primitive permutation group on Ω with socle G_0 that is not an alternating group, and let $G_0 \trianglelefteq G_1 \leq G$. If G/G_1 has a normal series of length k with all quotients cyclic, then $b(G, \Omega) \leq b(G_1, \Omega) + k$.*

Proof. By [59, Theorem 1.1] each element of G has a regular cycle. It follows that stabilising one point for each cyclic quotient suffices to extend a base for G_1 to one for G. □

Definition 3.1.6. *We fix some notation that we will use for the remainder of this paper. Let $\mathbb{F} = \mathbb{F}_{q^2}$ in the unitary case, and $\mathbb{F} = \mathbb{F}_q$ otherwise, and let σ the automorphism of $\mathbb{F}$ mapping $x \mapsto x^q$. Let $V = \mathbb{F}^d$.*

We fix the following standard forms on $V = \mathbb{F}$. Our standard unitary form B has basis

$$\begin{cases} \{e_1, \ldots, e_m, f_m, \ldots, f_1\} & \text{if } d = 2m, \\ \{e_1, \ldots, e_m, x, f_m, \ldots, f_1\} & \text{if } d = 2m + 1, \end{cases}$$

where for all i and j we set $B(e_i, e_j) = B(f_i, f_j) = 0$, $B(e_i, f_j) = \delta_{i,j}$, $B(e_i, x) = B(f_i, x) = 0$, and $B(x, x) = 1$.

Our standard symplectic form B has basis

$$\{e_1, \ldots, e_m, f_m, \ldots, f_1\}$$

where $d = 2m$ and for all i and j we set $B(e_i, e_j) = B(f_i, f_j) = 0, B(e_i, f_j) = \delta_{i,j}$.

Our standard quadratic form Q, with symmetric bilinear form $B = B_Q$, has basis

$$\begin{cases} \{e_1, \ldots, e_m, f_m, \ldots, f_1\} & d = 2m, \ Q \text{ is of } + \text{ type}, \\ \{e_1, \ldots, e_m, x, y, f_m, \ldots, f_1\} & d = 2m+2, \ Q \text{ is of } - \text{ type}, \\ \{e_1, \ldots, e_m, x, f_m, \ldots, f_1\} & d = 2m+1, \end{cases}$$

where for all i and j we set $Q(e_i) = Q(f_i) = 0, B(e_i, f_j) = \delta_{i,j}$, $B(e_i, x) = B(f_i, x) = B(e_i, y) = B(f_i, y) = 0$, $Q(x) = B(x, y) = 1$ and $Q(y) = \zeta$, where $X^2 + X + \zeta \in \mathbb{F}[X]$ is irreducible. We remark that will work, at times, with orthogonal groups of odd dimension in characteristic 2, and that that this is our standard form in this case as well: see, for example, [157, p139] for more information.

A pair (u, v) of vectors is a hyperbolic pair *if $B(u, u) = B(v, v) = 0$, $Q(u) = Q(v) = 0$ in the orthogonal case, and $B(u, v) = 1$.*

A pair (u, v) of vectors is an elliptic pair *if $Q(u) = 1$, $Q(v) = \zeta$, for some $\zeta \in \mathbb{F}$ such that $X^2 + X + \zeta$ is irreducible, and $B(u, v) = 1$.*

Definition 3.1.7. *If $d = 2m$, q is odd and Q is of $-$ type we work sometimes with the slightly modified basis form*

$$\{e_1, \ldots, e_m, x', y', f_m, \ldots, f_1\},$$

where for all i and j we set $Q(e_i) = Q(f_i) = 0, B(e_i, f_j) = \delta_{i,j}$, $B(e_i, x') = B(f_i, x') = B(e_i, y') = B(f_i, y') = 0$, $Q(x') = 1$, $B(x', y') = 0$ and $Q(y') = \alpha$, where $X^2 + \alpha \in \mathbb{F}[X]$ is irreducible (that is $-\alpha$ is a non-square in $\mathbb{F}$).

Totally singular

Here, we consider the unitary, symplectic and orthogonal groups G, and let $\mathcal{S}(G, k)$ be a G-orbit of totally singular k-spaces of $V = \mathbb{F}^d$, with $k \in \{1, 2\}$. Note that the actions of the groups G with $\mathrm{PSL}_d(q) \trianglelefteq G \trianglelefteq \mathrm{P\Gamma L}_d(q)$ on *one-* and *two-* spaces are included here.

Note that in all but $\operatorname{soc} G = \mathrm{P\Omega}^+_{2k}(q)$, the set $\mathcal{S}(G, k)$ contains all the totally singular k-spaces of V.

Lemma 3.1.8. *Let $G = G_d(q)$ be one of $\mathrm{PGU}_d(q), \mathrm{PSp}_d(q), \mathrm{PGO}^\varepsilon_d(q)$. Let $D = \{3, 4\}$ if G is unitary, $D = \{6\}$ if $G = \mathrm{PGO}^\pm_d(q)$, and $D = \{4, 5\}$ otherwise. Let $a \in D$ such that $d = 2k + a$, with $k \in \mathbb{N}$. Then $b(G, \mathcal{S}(G, 1)) \leq b(G_a(q), \mathcal{S}(G_a(q), 1)) + 2k$.*

Proof. We proceed by induction on k. If $k = 0$ the result is clear, so assume that $k > 0$, and that the result holds for $k - 1$.

For all n, let H_n denote the linear group corresponding to $G_n(q)$, so that $H_n \in \{\mathrm{GU}_n(q), \mathrm{Sp}_n(q), \mathrm{GO}^\varepsilon_n(q)\}$. Let $U = \langle e_2, \ldots, f_2 \rangle$. Then U is non-degenerate, so by the inductive hypothesis, there exists a set $\mathcal{T}$ of $b(G_a(q)) + 2(k-1)$ one-dimensional subspaces of U such that $(H_{n-2})_{(\mathcal{A})}$ acts as scalars on U. Up to conjugacy, we may assume that $\langle e_2 \rangle, \langle f_2 \rangle \in \mathcal{A}$.

Let $\mathcal{B} = \mathcal{T} \cup \{\langle e_1 + e_2 \rangle, \langle f_1 + f_2 \rangle\}$. We shall show that $\mathcal{B}$ is a base for H. Let $h \in H_{(\mathcal{B})}$. We first apply Lemma 3.1.3(1), with (e_2, f_2, e_1) here in place of (u, v, w) there to see that there exist $\alpha, \beta \in \mathbb{F}^*$ such that $e_2 h = \alpha e_2$, $f_2 h = \beta f_2$ and $e_1 h = \alpha e_1$. We then apply Lemma 3.1.3(1) to (e_2, f_2, f_1) to deduce that $f_1 h = \beta f_1$. Now h stabilises $\langle e_1, f_1 \rangle$, and so stabilises U. Hence, by our assumption on $\mathcal{A}$, the group H induces scalars on U. Therefore in particular, $\alpha = \beta$ and so $H_{(\mathcal{B})}$ consists of scalars, as required. □

Lemma 3.1.9. *Let $d \geq 3$, and let $G \in \{\mathrm{PGU}_d(q), \mathrm{PSp}_d(q)\}$. Then $b(G, \mathcal{S}(G,1)) \leq d$.*

Proof. Let B be our standard unitary or symplectic form, from Definition 3.1.6, let $\mathbb{F} = \mathbb{F}_{q^2}$ for the unitary case, let $\mathbb{F} = \mathbb{F}_q$ for the symplectic case, and let $U = \langle e_1, f_1 \rangle$.

Since $\mathbb{F}_{q^2}$ is perfect, the trace map

$$tr_{\mathbb{F}_q}^{\mathbb{F}_{q^2}} : a \in \mathbb{F}_{q^2} \mapsto a + a^q \in \mathbb{F}_q$$

is surjective, and so there exists $\mu \in \mathbb{F}_{q^2}$ such that $\mu^q + \mu + 1 = 0$. Hence for d odd (and so B unitary), $B(e_1 + x + \mu f_1, e_1 + x + \mu f_1) = \mu^q + 1 + \mu = 0$, so the vector $e_1 + x + \mu f_1$ is singular. Hence for odd d we may let

$$\mathcal{B}_3 = \{\langle e_1 \rangle, \langle f_1 \rangle, \langle e_1 + x + \mu f_1 \rangle\},$$

and let $g \in \mathrm{GU}_3(q)_{(\mathcal{B}_3)}$. Apply Lemma 3.1.3(1), with (e_1, f_1, x) in place of (u, v, w), to see that g is scalar. Hence $b(\mathrm{PGU}_3(q)) \leq 3$.

Let

$$\mathcal{B}_4 = \{\langle e_1 \rangle, \langle f_1 \rangle, \langle e_1 + e_2 \rangle, \langle f_2 + e_1 \rangle\} \subseteq \mathcal{S}(G,1),$$

and let $g \in \mathrm{GU}_4(q)_{(\mathcal{B}_4)}$ or $g \in \mathrm{Sp}_4(q)_{(\mathcal{B}_4)}$ Apply Lemma 3.1.3(1), first to (e_1, f_1, e_2) and then to (e_1, f_1, f_2), to see that $g = \mathrm{Diag}(\alpha, \alpha, \alpha, \beta)$, for some $\alpha, \beta \in \mathbb{F}$. Then from $B(\alpha e_2, \alpha f_2) = 1$ we see that $\alpha = \alpha^{-q}$, and from $B(\alpha e_1, \beta f_1) = 1$ we see that $\alpha\beta^q = 1$, so $\beta = \alpha^{-q} = \alpha$. Hence g is scalar, and so $b(\mathrm{PGU}_4(q)) \leq 4$ and $b(\mathrm{PSp}_4(q)) \leq 4$.

The result now follows for all $d \geq 3$ by Lemma 3.1.8. □

Lemma 3.1.10. *Let $d \geq 5$, let $\varepsilon \in \{+, -, \circ\}$, and let $G = \mathrm{PGO}_d^\varepsilon(q)$. Then $b(G, \mathcal{S}(G,1)) \leq d - 1$.*

Proof. Throughout, Q denotes our standard quadratic form, from Definition 3.1.6.

First, let d be odd, let

$$\mathcal{B}_5 = \{\langle e_1 \rangle, \langle f_1 \rangle, \langle -e_1 + x + f_1 \rangle, \langle e_1 + e_2 \rangle\} \subseteq \mathcal{S}(G,1),$$

and let $g \in \mathrm{GO}_5^\circ(q)_{(\mathcal{B}_5)}$. We apply Lemma 3.1.3(1), first with (e_1, f_1, x) for (u, v, w), and then with (e_1, f_1, e_2), to see that $g|_{\langle e_1, e_2, x, f_1 \rangle} = \mathrm{Diag}(\alpha, \alpha, \alpha, \alpha)$, for some $\alpha = \alpha^{-1} \in \mathbb{F}_q$. Applying Lemma 3.1.3(2) to $\{e_2, f_2\}$ yields $f_2 g = \alpha f_2$. Hence g is scalar, and so $b(\mathrm{PGO}_5^\circ(q)) \leq 4$.

Next, let Q be of minus type, let

$$\mathcal{B}_6^- = \{\langle e_1 \rangle, \langle f_1 \rangle, \langle e_1 + e_2 \rangle, \langle -e_1 + x + f_1 \rangle, \langle -\zeta e_1 + y + f_1 \rangle\} \subseteq \mathcal{S}(G,1),$$

and let $g \in \mathrm{GO}_6^-(q)_{(\mathcal{B}_6)}$. We apply Lemma 3.1.3(1), first with (e_1, f_1, x) for (u, v, w), then with (e_1, f_1, y), and finally with (e_1, f_1, e_2), to deduce that $g|_{\langle e_1, e_2, x, y, f_1 \rangle} = \mathrm{Diag}(\alpha, \alpha, \alpha, \alpha, \alpha)$, for some $\alpha = \alpha^{-1} \in \mathbb{F}_q$. Applying Lemma 3.1.3(2) to (e_2, f_2) shows that g is scalar, and so $b(\mathrm{PGO}_6^-(q)) \leq 5$.

Finally, let Q be of plus type, let

$$\mathcal{B}_6^+ = \{\langle e_1 \rangle, \langle f_1 \rangle, \langle e_1 + e_2 \rangle, \langle f_2 + e_1 \rangle, \langle e_2 + e_3 \rangle\} \subseteq \mathcal{S}(G,1),$$

and let $g \in \mathrm{GO}_6^+(q)_{\mathcal{B}_6}$. Let $W = \langle e_1, e_2, f_2, f_1 \rangle$. We apply Lemma 3.1.3(1), first to (e_1, f_1, e_2), and then to (e_1, f_1, f_2), to see that $g|_W = \mathrm{Diag}(\alpha, \alpha, \alpha, \alpha^{-1})$, for some $\alpha = \alpha^{-1} \in \mathbb{F}_q$. Next, we apply Lemma 3.1.3 to (e_2, f_2, e_3) to see that $e_3 g = \alpha e_3$. Now $W^\perp = \langle e_3, f_3 \rangle$ is stabilised by g, so Lemma 3.1.3(2) applied to $\{e_3, f_3\}$ shows that g is scalar. Hence $b(\mathrm{PGO}_6^+(q)) \leq 5$.

The result now follows for all $d \geq 5$ by Lemma 3.1.8. □

We shall prove that the bound in Lemma 3.1.10 is tight.

Lemma 3.1.11. *Let $d \geq 6$ be even, let $\varepsilon \in \{+,-\}$, and let $G = \mathrm{PGO}^{\varepsilon}_d(q)$. Then $b(G, \mathcal{S}(G,1)) = d-1$.*

Proof. Let V be the natural module for $H = \mathrm{GO}^{\varepsilon}_d(q)$, and let $\mathcal{A} = \{\langle v_1\rangle, \ldots, \langle v_{d-2}\rangle\}$ be a set of $d-2$ totally singular 1-spaces. Let W be any $d-2$-dimensional space containing the span of the 1-spaces in $\mathcal{A}$, and let $H_{(W)}$ denote the subgroup of H that acts as scalars on W. We shall show that there exists a nonscalar element of $H_{(W)}$, from which the result will follow.

If W is non-degenerate, then $H_{(W)}$ contains a subgroup which acts as $\mathrm{GO}(W^{\perp})$ on $W^{\perp}$, so the result is immediate. Thus we may assume that W is degenerate, so $U := \mathrm{Rad}(W) = W \cap W^{\perp}$ is a non-zero subspace of W.

First assume that there exists a $u \in U$ such that $Q(u) \neq 0$. This implies that q is even, so H has a single orbit on non-singular 1-spaces, and without loss of generality we can assume that $u = e_1 + f_1$. Notice that $e_1, f_1 \notin W$, since $B_Q(u, e_1) = B_Q(u, f_1) \neq 0$. We define a linear map g by

$$e_1 g = f_1, \quad f_1 g = e_1, \quad xg = x \text{ for all } x \in \langle e_1, f_1\rangle^{\perp}.$$

Let $v_1, v_2 \in V$, then for $i = 1, 2$ we can write $v_i = \alpha_i e_1 + \beta_i f_1 + x_i$, for some $\alpha_i, \beta_i \in \mathbb{F}_q$ and $x_i \in \langle e_1, f_1\rangle^{\perp}$. Then

$$\begin{aligned} Q(v_1 g) &= Q(\alpha_1 f_1 + \beta_1 e_1 + x_1) = \alpha_1\beta_1 + Q(x_1) = Q(v_1) \\ B_Q(v_1 g, v_2 g) &= B_Q(\alpha_1 f_1 + \beta_1 e_1 + x_1, \alpha_2 f_1 + \beta_2 e_1 + x_2) \\ &= \alpha_1\beta_2 + \beta_1\alpha_2 + B_Q(x_1, x_2) \\ &= B_Q(v_1, v_2), \end{aligned}$$

so $g \in H$. Furthermore, if $w \in W$ then $B_Q(w, e_1 + f_1) = 0$, so we can write $w = x + \alpha e_1 + \alpha f_1$, for some $x \in \langle e_1, f_1\rangle^{\perp}$ and $\alpha \in \mathbb{F}_q$. Hence $wg = w$, so $g \in H_{(W)}$, as required.

Next assume that $Q(u) = 0$ for all $u \in U$, so that U is totally singular. If $\dim(U) = 1$ then we can write $W = \langle u\rangle \perp W'$, with $\mathrm{Rad}(W') = 0$, when q is even this contradicting the fact that $\dim W = d-2$ is even. So, when $\dim(U) = 1$, we can assume that q is odd. Then there exists a $u' \in V \setminus W$ such that $B_Q(u, u') \neq 0$. Let $W_1 = \langle W, u'\rangle$. Then W_1 is non-degenerate, and $\dim(W_1) = d-1$, so $\dim(W_1^{\perp}) = 1$. Let x be a basis vector for $W_1^{\perp}$, and define $g \in \mathrm{GL}(V)$ from V to V by

$$w_1 g = w_1, \ \forall w_1 \in W_1, \text{ and } xg = -x.$$

Let $v \in V$, then we can write $v_1 = \alpha_1 w_1 + \beta_1 x$ and $v_2 = \alpha_2 w_2 + \beta_2 x$, for some $\alpha_i, \beta_i \in \mathbb{F}_q$ and $w_i \in W_1$. Hence

$$\begin{aligned} Q(v_1 g) &= Q(\alpha_1 w_1 - \beta_1 x) = \alpha^2 Q(w_1) + (-\beta)^2 Q(x) = Q(v_1) \\ B_Q(v_1 g, v_2 g) &= B_Q(\alpha_1 w_1 - \beta_1 x, \alpha_2 w_2 - \beta_2 x) \\ &= \alpha_1\alpha_2 B_Q(w_1, w_2) + \beta_1\beta_2 B_Q(x, x) \\ &= B_Q(v_1, v_2), \end{aligned}$$

so $g \in H$. Since $W \subseteq W_1$, then $wg = w$ so $g \in H_{(W)}$, as required.

Hence we can assume $\dim(U) = 2$, and we may let u_1, u_2 be a basis for U. There exists a vector $w_1 \in V$ such that $B_Q(u_1, w_1) = 1$, $Q(w_1) = 0$ and (replacing u_2 by another element of U if necessary) $B_Q(u_2, w_1) = 0$. Then $u_2 \in \langle u_1, w_1\rangle^{\perp}$, so there exists $w_2 \in \langle u_1, w_1\rangle^{\perp}$ such that $B_Q(u_2, w_2) = 1$ and $Q(w_2) = 0$. Then $w_1, w_2 \notin W$, so each $v \in V$ can be written as $x + \alpha w_1 + \beta w_2$ for some $\alpha, \beta \in \mathbb{F}_q$ and $x \in W$. We define an element $g \in \mathrm{GL}(V)$ by

$$w_1 g = w_1 + u_2, \quad w_2 g = w_2 - u_1 \quad xg = x \text{ for all } x \in W.$$

For $i = 1, 2$, let $v_i = \alpha_i w_1 + \beta_i w_2 + x_i$, with $x_i \in W$. Then

$$\begin{aligned} Q(v_1 g) &= Q(\alpha_1(w_1 + u_2) + \beta_1(w_2 - u_1)) + Q(x_1) + B_Q(\alpha_1(w_1 + u_2) + \beta_1(w_2 - u_1), x_1) \\ &= -\alpha_1\beta_1 + \alpha_1\beta_1 + Q(x_1) + B_Q(\alpha_1 w_1 + \beta_1 w_2, x_1) = Q(v_1) \\ B_Q(v_1 g, v_2 g) &= B_Q(\alpha_1(w_1 + u_2) + \beta_1(w_2 - u_1) + x_1, \alpha_2(w_1 + u_2) + \beta_2(w_2 - u_1) + x_2) \\ &= B_Q(x_1, x_2) = B_Q(v_1, v_2), \end{aligned}$$

so $g \in H$. It is then clear that B_Q, so $g \in H_{(W)}$, as required. □

We shall make repeated use of the following observation in the proof of this Section so record it as a lemma.

Lemma 3.1.12. *Let $v_1, \ldots, v_d$ be a basis for a vector space $V = \mathbb{F}^d$, and let $u = \sum_{i=1}^n \alpha_i v_i$ and $v = \sum_{i=1}^n \beta_i v_i$. Let $T = \langle u, v\rangle$, and let $g \in \mathrm{GL}(V)$ be such that $Tg = T$. If there exists a $j \in \{1, \ldots, n\}$ such that $\beta_j \neq 0$, and each nonzero vector in $\langle v_i g \ : \ \alpha_i \neq 0\rangle$ has v_j coefficient 0, then there exists $\eta \in \mathbb{F}^*$ such that $ug = \eta u$.*

Lemma 3.1.13. *Let $H = \mathrm{PGL}_d(q)$. If $d \geq 5$ then $b(H, \mathcal{S}(H, 2)) \leq \lceil \frac{d}{2} \rceil + 2$. If $d = 4$ then $b(H, \mathcal{S}(H, 2)) \leq 5$.*

Proof. Let $G = \mathrm{GL}_d(q)$ and let $v_1, \ldots, v_d$ be a basis for $\mathbb{F}_q^d$. Let $a = \lceil d/2 \rceil$, and let

$$\begin{aligned} V_i &:= \langle v_{2i-1}, v_{2i}\rangle, \text{ for } 1 \leq i \leq a \qquad (\text{if } d \text{ is odd, set } \ v_{d+1} = v_1) \\ W_1 &:= \langle v_1 + v_3 + \cdots + v_{2a-1},\ v_2 + v_4 + \cdots + v_{2a-2}\rangle. \end{aligned}$$

First assume that $d \geq 5$, and let

$$W_2 := \langle v_1, v_3 + v_{2a-2} + v_d\rangle.$$

We will show that $\mathcal{B} = \{V_i, W_1, W_2 \mid 1 \leq i \leq \lceil d/2 \rceil\}$ is a base for H. Let $g \in G_{(\mathcal{B})}$ and let $X = V_1 \oplus \cdots \oplus V_{a-1}$. Then g stabilises $W_1 \cap X = \langle v_2 + v_4 + \cdots + v_{2a-2}\rangle$. Hence there exists $\beta \in \mathbb{F}_q$ such that

$$v_{2j} g = \beta v_{2j}, \text{ for } 1 \leq j \leq a - 1. \tag{3.1.1}$$

Furthermore, g stabilises $V_1 \cap W_2 = \langle v_1\rangle$, and hence $v_1 g = \alpha v_1$ for some $\alpha \in \mathbb{F}$. Now, this and the fact that g stabilizes $V_2 \oplus \cdots \oplus V_{a-1} = \langle v_3, v_4, \ldots, v_{2a-3}, v_{2a-2}\rangle$ means that we may apply Lemma 3.1.12, with $T = W_1$, $u = v_1 + v_3 + \cdots + v_{2a-1}$ and $j = 2$ to deduce that

$$v_{2i-1} g = \alpha v_{2i-1}, \text{ for } 1 \leq i \leq a.$$

In particular, notice that $v_d g \in \langle v_{d-1}, v_d\rangle$, irrespective of whether d is even or odd. Now we may apply Lemma 3.1.12, with $T = W_2$, $u = v_3 + v_{2a-2} + v_d$ and $j = 1$ yields $\alpha = \beta$ and $v_d = \alpha v_d$. That is, g is scalar. The result follows.

Next let $d = 4$. We will show that

$$\mathcal{B} = \{V_1, V_2, W_1, W_3 = \langle v_2, v_4\rangle, W_4 = \langle v_1 + v_2, v_3\rangle\}$$

is a base for H in its action on 2-spaces, so let $g \in G_{(\mathcal{B})}$. Since $g \in G_{(V_1, V_2, W_1)}$, so Lemma 3.1.4 implies that $g = \mathrm{Diag}(X_1, X_1)$ with $X_1 \in \mathrm{GL}_2(q)$. Since g stabilises $V_1 \cap W_3 = \langle v_2\rangle$, there exists $\beta \in \mathbb{F}$ such that $v_2 g = \beta v_2$, and hence $v_4 g = \beta v_4$. Similarly, since g stabilises $V_2 \cap W_3 = \langle v_3\rangle$, there exists $\alpha \in \mathbb{F}$ such that $v_3 g = \alpha v_3$, and hence $v_1 g = \alpha v_1$. Applying Lemma 3.1.12, with $T = W_4$, $u = v_1 + v_2$ and $j = 3$ we see that $\alpha = \beta$, and so g is scalar, as required. □

Proposition 3.1.14. *Let $G \in \{\mathrm{PGU}_d(q), \mathrm{PSp}_d(q), \mathrm{PGO}_d^\varepsilon(q)\}$, and let $b = b(G, \mathcal{S}(G, 2))$. If $d \geq 7$ then $b \leq \lceil \frac{d}{2} \rceil$. If $G = \mathrm{PGU}_4(q)$ then $b \leq 5$, whilst if $G \in \{\mathrm{PGU}_5(q), \mathrm{PGU}_6(q), \mathrm{PSp}_4(q), \mathrm{PSp}_6(q)\}$ then $b \leq 4$.*

Proof. Let B be either our standard unitary or symplectic form, or the polar form of our standard quadratic form Q, from Definition 3.1.6. Let $\mathbb{F} = \mathbb{F}_{q^2}$ for the unitary case, and let $\mathbb{F} = \mathbb{F}_q$ otherwise. Let $a = \lceil d/2 \rceil$, and notice that if $d \geq 7$ then $a \geq 4$.

We first define some useful subspaces, and fix some notation. Let

$$V_1 = \langle e_1, e_2 \rangle, \qquad V_2 = \langle f_1, f_2 \rangle, \qquad W_i = \langle e_1 + e_i, e_2 - f_1 + f_i \rangle, \quad \text{for } 3 \leq i \leq a.$$

It is straightforward to verify that V_1, V_2 and W_i are in $\mathcal{S}(G, 2)$. Let $g \in G$ stabilise V_1 and V_2. Then for $i \in \{1, 2\}$ there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}$ such that

$$\begin{aligned} e_1 g &= \alpha_1 e_1 + \alpha_2 e_2, & e_2 g &= \beta_1 e_1 + \beta_2 e_2 \\ f_1 g &= \gamma_1 f_1 + \gamma_2 f_2, & f_2 g &= \delta_1 f_1 + \delta_2 f_2, \end{aligned} \tag{3.1.2}$$

Furthermore, let $U = V_1 \oplus V_2$, and let $W = U^\perp$. Since U is non-degenerate and $U^g = U$, it follows that $W^g = W$.

We shall deal with the cases where $d \leq 6$ at the end of the proof, so assume for now that $d \geq 7$ and let

$$\mathcal{A} := \{V_1, V_2, W_i \mid 3 \leq i \leq a - 1\} \subseteq \mathcal{S}(G, 2).$$

Let $g \in G_{(\mathcal{A})}$, and let $X = \langle \mathcal{A} \rangle$. We shall first show that there exist $\alpha, \beta \in \mathbb{F}$ such that

$$g|_X = \mathrm{Diag}(\alpha, \beta, \alpha, \ldots, \alpha, \beta, \ldots, \beta, \alpha, \beta). \tag{3.1.3}$$

For $3 \leq i \leq a - 1$, the element g stabilises $U_i := \langle V_1, V_2, W_i \rangle$, and so stabilises $U_i \cap W = \langle e_i, f_i \rangle$. Hence for $3 \leq i \leq a - 1$ there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}$ such that

$$e_i g = \alpha_i e_i + \beta_i f_i, \qquad f_i g = \gamma_i e_i + \delta_i f_i. \tag{3.1.4}$$

By Lemma 3.1.12, with $T = W_i$ and $v_j = f_1$, we deduce from (3.1.2) that $(e_1 + e_i)g = \eta(e_1 + e_i) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_i e_i + \beta_i f_i$. Hence, $\alpha_1 = \alpha_i$ and $\alpha_2 = \beta_i = 0$. That is,

$$e_i g = \alpha_1 e_i, \quad \text{for } i \in \{1, 3, 4, \ldots, a - 1\}. \tag{3.1.5}$$

Similarly, for $3 \leq i \leq a - 1$, there exist $\eta, \rho \in \mathbb{F}$ such that

$$\begin{aligned} (e_2 - f_1 + f_i)g &= \eta(e_1 + e_i) + \rho(e_2 - f_1 + f_i) \\ &= \beta_1 e_1 + \beta_2 e_2 - \gamma_1 f_1 - \gamma_2 f_2 + \gamma_i e_i + \delta_i f_i. \end{aligned}$$

Equating coefficients, we deduce that $\gamma_2 = 0$, $\beta_1 = \gamma_i$ and $\beta_2 = \gamma_1 = \delta_i$. Consequently, for $3 \leq i \leq a - 1$

$$f_1 g = \beta_2 f_1, \quad f_i g = \beta_1 e_i + \beta_2 f_i. \tag{3.1.6}$$

For $i \in \{1, 2\}$, let $U_i = \langle e_i, f_i \rangle$. From (3.1.5) and (3.1.6) we see that $U_1^g = U$. Hence g stabilises $U_1^\perp \cap U = U_2$, and so $(V_1 \cap U_2)^g = \langle e_2 \rangle^g = \langle e_2 \rangle$, and $(V_2 \cap U_2)^g = \langle f_2 \rangle^g = \langle f_2 \rangle$. From (3.1.2) it follows that $e_2 g = \beta_2 e_2$ and $f_2 g = \delta_2 f_2$, that is, $\beta_1 = \delta_1 = 0$. Then, from (3.1.6) we deduce that $f_i g = \beta_2 f_i$, for $3 \leq i \leq a - 1$.

Finally, $B(e_1 g, f_1 g) = B(e_2 g, f_2 g) = 1$ yields

$$\alpha_1 = \beta_2^{-q}, \text{ and } \beta_2 = \delta_2^{-q},$$

and hence $\alpha_1 = \delta_2$. Setting $\alpha = \alpha_1$ and $\beta = \beta_2$ yields (3.1.3).

We shall now extend $\mathcal{A}$ to a base for $G/Z(G)$, but the additional subspace depends on the type of G.

Odd dimensions Let G be $\mathrm{GU}_{2a-1}(q)$, or $\mathrm{GO}^{\circ}_{2a-1}(q)$. In the unitary case, let $\lambda \in \mathbb{F}$ satisfy $\lambda^q + \lambda = 1$ (this element exists because $\mathbb{F}_{q^2}$ is perfect, and the trace map $tr^{\mathbb{F}_{q^2}}_{\mathbb{F}_q} : a \in \mathbb{F}_{q^2} \mapsto a + a^q \in \mathbb{F}_q$ is surjective), otherwise let $\lambda = 1$. Let

$$T_3 = \langle -e_1 + x + \lambda f_1, f_2 + e_3 \rangle.$$

Then a short calculation shows that $T_3 \in \mathcal{S}(G, 2)$. We will show that

$$\mathcal{B} := \mathcal{A} \cup \{T_3\} \subseteq \mathcal{S}(G, 2),$$

is a base for $G/Z(G)$.

Let $g \in G_{(\mathcal{B})}$. By (3.1.3) we have $(X^{\perp})^g = X^{\perp}$, that is, there exists $\xi \in \mathbb{F}$ such that $xg = \xi x$. Since $g|_X$ is as in (3.1.3), we deduce from Lemma 3.1.12, with $T = T_2$ and $v_j = f_2$, that

$$(-e_1 + x + \lambda f_1)g = \eta(-e_1 + x + \lambda f_1) = -\alpha e_1 + \xi x + \lambda\beta f_1.$$

Hence $\alpha = \beta = \xi$, and $g = \alpha I_d$, as required.

Orthogonal groups of minus type. Let $G = \mathrm{GO}^{-}_{2a}(q)$, and let

$$U_3 = \langle -e_1 + x + f_1 + e_2, -\zeta e_1 + y + f_1 + \zeta f_2 \rangle.$$

Then a short calculation shows that $U_3 \in \mathcal{S}(d, 2)$. We claim that $\mathcal{B} := \mathcal{A} \cup \{V_3\} \subseteq \mathcal{S}(G, 2)$, is a base for $\mathrm{PGO}^{-}_{d}(q)$.

Let $g \in G_{(\mathcal{B})}$. Since $\langle x, y \rangle^g = \langle x, y \rangle$, there exist $\alpha_a, \beta_a, \gamma_a, \delta_a \in \mathbb{F}$ such that $xg = \alpha_a x + \beta_a y$ and $yg = \gamma_a x + \delta_a y$. Then we deduce from (3.1.3) and Lemma 3.1.12, with $T = U_3$ and $v_j = f_2$, that

$$(-e_1 + x + f_1 + e_2)g = \eta(-e_1 + x + f_1 + e_2) = -\alpha e_1 + \alpha_a x + \beta_a y + \beta f_1 + \beta e_2.$$

Hence $\beta_a = 0$ and $\alpha = \beta = \alpha_a$.

Similarly, setting $v_j = e_2$, we see that

$$(-\zeta e_1 + y + f_1 + \zeta f_2)g = \eta(-\zeta e_1 + y + f_1 + \zeta f_2) = -\zeta\alpha e_1 + \gamma_a x + \delta_a y + \alpha f_1 + \zeta\alpha f_2.$$

Consequently $\gamma_a = 0$, and $\alpha = \delta_a$. That is, g is scalar.

The remaining large groups Let G be one of $\mathrm{PGU}_{2a}(q), \mathrm{PSp}_{2a}(q)$, or $\mathrm{PGO}^{+}_{2a}(q)$. Let

$$V_3 := \langle e_1 + e_a, e_2 - e_a - f_1 + f_2 + f_a \rangle.$$

Then a short calculation shows that $V_3 \in \mathcal{S}(G, 2)$. Let $\mathcal{B} := \mathcal{A} \cup \{V_3\} \subseteq \mathcal{S}(G, 2)$. We shall show that $\mathcal{B}$ is a base for $G/Z(G)$.

Let $g \in G_{(\mathcal{B})}$. Since g is as in (3.1.3) and $V_3^g = V_3$, it follows that there exist $\alpha_a, \beta_a, \gamma_a, \delta_a \in \mathbb{F}$ such that $e_a g = \alpha_a e_a + \beta_a f_a$ and $f_a g = \gamma_a e_a + \delta_a f_a$. Then, by Lemma 3.1.12, with $T = V_3$ and $v_j = e_2$, we deduce that

$$(e_1 + e_a)g = \eta(e_1 + e_a) = \alpha e_1 + \alpha_a e_a + \beta_a f_a.$$

Hence $\beta_a = 0$ and $\alpha_a = \alpha$, that is $e_a g = \alpha e_a$. Moreover, setting $v_j = e_1$ we see that

$$(e_2 - e_a - f_1 + f_2 + f_a)g = \eta(e_2 - e_a - f_1 + f_2 + f_a) = \beta e_2 - \alpha e_a - \beta f_1 + \alpha f_2 + \gamma_a e_a + \delta_a f_a.$$

Consequently

$$\alpha = \beta = \delta_a = \alpha - \gamma_a$$

and so $\gamma_a = 0$, and g is scalar. □

Table 3.1: Bases in small dimension for $\mathcal{S}(G,2)$: $V_1 = \langle e_1, e_2\rangle, V_2 = \langle f_1, f_2\rangle$

G	$\mathcal{B}$	Notes
$\mathrm{PGU}_4(q)$	$\{V_1, V_2, \langle e_1+\mu f_1, e_2+\mu f_2\rangle, \langle e_1, f_2\rangle, \langle e_1-e_2, f_1+f_2\rangle\}$	$\mu^q+\mu=0$
$\mathrm{PSp}_4(q)$	$\{V_1, V_2, \langle e_1+f_1+f_2, e_2+f_1\rangle, \langle e_1+f_2, e_2+f_2+f_1\rangle\}$	q even
	$\{V_1, V_2, \langle e_1+f_1+f_2, e_2+f_1\rangle, \langle e_1+f_2, e_2+f_1\rangle\}$	q odd
$\mathrm{PGU}_5(q)$,	$\{V_1, V_2, \langle -e_2+x+\lambda f_2, f_1\rangle, \langle -e_1+x+\lambda f_1, f_2\rangle\}$	$\lambda^q+\lambda=1$
$\mathrm{PSp}_6(q)$, $\mathrm{PGU}_6(q)$	$\{V_1, V_2, \langle e_1+e_3, e_2-f_1+f_3\rangle, \langle e_1-e_2, f_1+f_2\rangle\}$	

Non-degenerate

In this subsection we consider the unitary and symplectic groups G, and let $\mathcal{N}(G,k)$ be a G-orbit of non-degenerate *one-* and *two*-dimensional spaces of $V = \mathbb{F}_q^d$. Further, we consider the orthogonal groups G on $\mathcal{N}(G,1)$ a G-orbit non-degenerate *one*-spaces of V, unless $k=1$ and q is even, in which case it will denote a G-orbit of non-singular 1-spaces. Finally, we consider the orthogonal groups G on $\mathcal{N}^{\pm}(G,k)$ a G-orbit of non-degenerate *two*-spaces of $+$ or $-$type.

Lemma 3.1.15. *Let $d \geq 3$, let $G = \mathrm{PGU}_d(q)$, and let $\mathcal{N} = \mathcal{N}(G,1)$. Then $b(G,\mathcal{N}) \leq d$.*

Proof. Let $\{v_1, \ldots, v_d\}$ be an orthonormal basis of the natural module V for G.

First assume that either d is odd or $q > 2$. For $\mu \in \mathbb{F}_q^*$, let $v = v(\mu) = v_1 + \cdots + v_{d-1} + \mu v_d$. Let α be a primitive element of $\mathbb{F}_q^*$. Then $\beta(v(\mu), v(\mu)) = d - 1 + \mu^{q+1}$, so for at least one value of μ in $\{\alpha, \alpha^{-1}, \alpha^2\}$ the vector $v(\mu)$ is non-degenerate. Fix this value of μ, and let

$$\mathcal{B} = \{\langle v_1\rangle, \ldots, \langle v_{d-1}\rangle, \langle v(\mu)\rangle\} \subseteq \mathcal{N}$$

Let $g \in \mathrm{GU}_d(q)_{(\mathcal{B})}$ and $U = \langle v_1, \ldots, v_{d-1}\rangle$. Since U is non-degenerate, $(U^\perp)^g = \langle v_d\rangle^g = \langle v_d\rangle$. That is g stabilizes d linearly independent vectors, so g is diagonal by Lemma 3.1.2(1). Then since g also stabilises $\langle v(\mu)\rangle$, Lemma 3.1.2(2) yields that g is scalar, and the result follows.

When $q = 2$ and d is even, let

$$\mathcal{B} = \{\langle v_1\rangle, \langle v_2\rangle, \langle v_i + v_1 + v_2\rangle \mid 3 \leq i \leq d\} \subseteq \mathcal{N},$$

let $g \in \mathrm{GU}_d(q)_{(\mathcal{B})}$, and let $U = \langle v_1, v_2\rangle$. Since U is non-degenerate we have $(U^\perp)^g = \langle v_3, \ldots, v_d\rangle^g = \langle v_3, \ldots, v_d\rangle$. Now, we are in the position to apply Lemma 3.1.3(1) to (v_1, v_2, v_i), for $3 \leq i \leq d$, to see that g is scalar, and so $b(G,\mathcal{N}) \leq d$. □

For the next result we use the following notation. Let $G = \mathrm{GO}^\circ_{2a+1}(q)$, and let $\mathcal{N}_\pm(G,1)$ be the G-orbit corresponding to the non-degenerate one-spaces of $V = \mathbb{F}_q^d$ having as orthogonal complement a $2a$-dimensional orthogonal space of $\pm$type. Furthermore, when $G_\pm = \mathrm{GO}^\pm_{2a}(q)$ we recall that $\mathcal{N}(G_\pm, 1)$ denotes a $G_\pm$-orbit of non-degenerate (respectively non-singular) one-spaces of V. Note that, when q is odd, there are two isometry classes of such spaces (but only one similarity class). The two orbits can be distinguished by considering the discriminant of the restriction of the underlying quadratic form on V. Since the actions of $G_\pm$ on the two orbits are equivalent, it is enough to consider one of them.

Lemma 3.1.16. *Let $d \geq 4$, let $H = \mathrm{PGO}^\varepsilon_d(q)$ be almost simple, and let $\mathcal{N}$ be an H-orbit of non-degenerate (q odd) or non-singular (q even) 1-spaces. If $(d,\mathcal{N}) \neq (4, \mathcal{N}(H,1)), (5, \mathcal{N}_-(H,1))$ then $b(H,\mathcal{N}) \leq d-1$. In addition $b(\mathrm{PGO}^-_4(q),\mathcal{N}) \leq 4$ and $b(\mathrm{PGO}^\circ_5(q),\mathcal{N}) \leq 5$.*

Table 3.2: Bases in small dimension for $\mathcal{N}(G,1)$ and $\mathcal{N}_\pm(G,1)$

G	Notes $\mathcal{B}$	
$\mathrm{PGO}_4^-(q)$	q even	$\{\langle x\rangle, \langle y\rangle, \langle e_1+x+y\rangle\}$
$\mathrm{PGO}_4^-(q)$	q odd, form from Definition 3.1.7	$\{\langle y'\rangle, \langle e_1+y'\rangle, \langle f_1+y'\rangle, \langle f_1+(\alpha-1)e_1+x'\rangle\}$
$\mathrm{PGO}_5^\circ(q)$	$\mathcal{N}_+(G,1)$	$\{\langle x\rangle, \langle e_1+x\rangle, \langle x+f_1\rangle, \langle e_2+x\rangle\}$
$\mathrm{PGO}_5^\circ(q)$	$\mathcal{N}_-(G,1)$, let $-\alpha^\star$ and $1-\beta^\star$ be non-squares in $\mathbb{F}$	$\{\langle e_1-\alpha^\star f_1\rangle, \langle e_1-\alpha^\star f_1+e_2\rangle, \langle e_1-\alpha^\star f_1+f_2\rangle, \langle e_2-\alpha^\star f_2+e_1\rangle, \langle e_2-\beta^\star f_2+x+f_1\rangle\}$

Proof. When $\varepsilon=-$ and q is odd, let Q be the form defined in Definition 3.1.7; otherwise let Q be our standard quadratic form for H. Let $G=\mathrm{GO}_d^\varepsilon(q,Q)$ preserve Q.

For $d=4$ we list a base of the specified size in Table 3.2, so assume $d\geq 6$. We first consider the orbits of type $\mathcal{N}(G,1)$ and $\mathcal{N}_+(G,1)$. Let

$$\mathcal{B}^+ := \{\langle e_1+f_1\rangle, \langle e_1+f_1+e_i\rangle, \langle e_1+f_1+f_j\rangle, \langle e_1+e_2+f_2\rangle \mid 2\leq i\leq a,\ 2\leq j\leq a-1\},$$

$$\mathcal{B}^- := \begin{cases} \{\langle x\rangle, \langle y\rangle, \langle e_i+x\rangle, \langle y+f_j\rangle, \mid 1\leq i\leq a,\ 1\leq j\leq a-1\}, & q \text{ even} \\ \{\langle y'\rangle, \langle e_i+y'\rangle, \langle y'+f_j\rangle, \langle f_1+(\alpha-1)e_1+x'\rangle \mid 1\leq i\leq a,\ 1\leq j\leq a-1\}, & \text{otherwise} \end{cases}$$

$$\mathcal{B}^\circ := \{\langle x\rangle, \langle e_i+x\rangle, \langle x+f_j\rangle \mid 1\leq i\leq a,\ 1\leq j\leq a-1\}.$$

If either $\varepsilon=+$ or $\varepsilon=-$ and q is even, we see that $Q(w)$ is a square for all $\langle w\rangle\in\mathcal{B}$, so $\mathcal{B}^\varepsilon\subseteq\mathcal{N}(G,1)$. Similarly, if $\varepsilon=-$ and q is odd then $Q(w)=\alpha$ for all $\langle w\rangle\in\mathcal{B}^-$, so $\mathcal{B}^\varepsilon\subseteq\mathcal{N}(G,1)$. It is straightforward to verify that $\langle v\rangle^\perp$ is of $+$ type for each $\langle v\rangle$ in $\mathcal{B}^\circ$, so $\mathcal{B}^\circ\subseteq\mathcal{N}_+(G,1)$. We shall show that $\mathcal{B}^\varepsilon$ is a base for H, so let $g\in G_{(\mathcal{B}^\varepsilon)}$.

We first consider $\varepsilon=\circ$, and $\varepsilon=-$ when q is even, and show that g acts as $\pm I$ on $\langle v:\langle v\rangle\in\mathcal{B}\rangle$. Let $U:=\langle x,y\rangle$ if $\varepsilon=-$, and $U:=\langle x\rangle$ otherwise. Since $U^g=U$ and U is non-degenerate, we deduce that $(U^\perp)^g=U^\perp=\langle e_1,\ldots,e_a,f_1,\ldots,f_a\rangle$. In particular, there exist $\mu,\psi\in\mathbb{F}_q^*$ and $u_i,v_j\in U^\perp$ for $1\leq i\leq a$ and $1\leq j\leq a-1$ such that $xg=\mu x$, $yg=\psi y$ if $\varepsilon=-$, $e_ig=u_i$ and $f_ig=v_i$. Now, for $1\leq i\leq a$ there exists $\nu_i\in\mathbb{F}_q^*$ such that

$$(e_i+x)g=\nu_i(e_i+x)=u_i+\mu x.$$

Equating coefficients shows that $e_ig=\nu_ie_i=\mu e_i$, for $1\leq i\leq a$. For $\epsilon=\circ$ we consider $x+f_j$ to see that $f_jg=\mu f_j$ for $1\leq j\leq a-1$. For $\epsilon=-$ we consider $y+f_j$ to deduce that $f_jg=\psi f_j$ for $1\leq j\leq a-1$. It follows from $Q((e_1+f_1)g)=Q(xg)=1$ that $\mu=\psi^{-1}=\psi\in\{\pm1\}$.

Now, we consider the case $\varepsilon=-$ and q odd. Here, we have that $d\geq 6$, that is $a\geq 2$. Since $y'g=\mu y'$ and $\langle y'\rangle$ is non-degenerate, we deduce that $(\langle y'\rangle^\perp)^g=\langle y'\rangle^\perp=\langle e_1,\ldots,e_a,x',f_1,\ldots,f_a\rangle$. In particular, there exist $u_i,v_j\in\langle y'\rangle^\perp$ for $1\leq i\leq a$ and $1\leq j\leq a-1$ such that $e_ig=u_i$ and $f_ig=v_i$.

Now, for $1\leq i\leq a$ there exists $\nu_i\in\mathbb{F}_q^*$ such that

$$(e_i+y')g=\nu_i(e_i+y')=u_i+\mu y'.$$

Equating coefficients shows that $e_ig=\nu_ie_i=\mu e_i$, for $1\leq i\leq a$. In the same way we deduce that $f_jg=\mu f_j$ for $1\leq j\leq a-1$. In particular, we deduce that

$$(\langle e_1,\ldots,e_{a-1},y',f_1,\ldots,f_{a-1}\rangle^\perp)^g=\langle e_a,x',f_a\rangle^g=\langle e_a,x',f_a\rangle,$$

and consequently we have that $x'g=u'$ for some $u'\in\langle e_a,x',f_a\rangle$.

Moreover, there exists $\psi\in\mathbb{F}$ such that $(e_1+(\alpha-1)f_1+x')g=\psi(e_1+(\alpha-1)f_1+x')=\mu(e_1+(\alpha-1)f_1)+u'$. Equating coefficients shows that $x'g=\mu x$, and $Q((e_1+f_1)g)=Q(xg)=1$ yields that $\mu=\pm1$.

For $\varepsilon = +$, let $(e_1 + f_1)g = \mu(e_1 + f_1)$. For $2 \leq i \leq a$, there exists $\nu_i \in \mathbb{F}_q$ such that

$$(e_1 + f_1 + e_i)g = \nu_i(e_1 + f_1 + e_i) = \mu(e_1 + f_1) + e_i g.$$

Hence $e_i g = (\nu_i - \mu)(e_1 + f_1) + \nu_i e_i$, and $Q(e_i g) = 0$ yields $\nu_i = \mu$, so $e_i g = \mu e_i$ for $i \geq 2$. Similarly, $f_i g = \mu f_i$ for $2 \leq i \leq a-1$, and from $Q((e_2+f_2)g) = 1$ we see that $\mu \in \{\pm 1\}$. Since $\langle (e_2+f_2)+e_1\rangle \in \mathcal{B}$, we deduce in the same way that $e_1 g = \mu e_1$, and then $(e_1+f_1)g = \mu e_1 + f_1 g$ yields $f_1 g = \mu f_1$, as required.

Now, let ε and q be arbitrary. The space $\langle e_a, f_a\rangle^\perp$ is non-degenerate and stabilised by g, so $\langle e_a, f_a\rangle^g = \langle e_a, f_a\rangle$. Lemma 3.1.3, applied with $(u, v) = (e_a, f_a)$, yields $f_a g = \mu f_a$. That is $g = \pm I$, as required.

Now, we have to find a base for the action of $G = \mathrm{GO}^\circ_d(q)$ on $\mathcal{N} = \mathcal{N}_-(G, 1)$. Let $\alpha, \beta \in \mathbb{F}$, such that $-\alpha$ and $1 - \beta$ are non-squares in $\mathbb{F}$.

When $d = 5$ we list a base of the specified size in Table 3.2, so assume $d \geq 7$. Let

$$\begin{aligned}\mathcal{B} := \{&\langle e_1 - \alpha f_1\rangle, \langle e_1 - \alpha f_1 + e_i\rangle, \langle e_1 - \alpha f_1 + f_j\rangle, \langle e_2 - \alpha f_2 + e_1\rangle,\\ &\langle e_2 - \beta f_2 + x + f_1\rangle \mid 2 \leq i \leq a,\ 2 \leq j \leq a-1\}.\end{aligned}$$

First of all we shall show that $\mathcal{B} \in \mathcal{N}_-(G, 1)$.

Since $\langle e_1 - \alpha f_1\rangle^\perp = \langle e_1 + \alpha f_1, x\rangle \oplus \langle e_2, \ldots, e_a, f_a, \ldots, f_2\rangle$, from [80, Lemma 2.5.11(ii)], we deduce that $\langle e_1 - \alpha f_1\rangle^\perp$ has $-$type if and only if $\langle e_1 + \alpha f_1, x\rangle$ has $-$type. By [80, Propositions 2.5.10, 2.5.13] we get that $\langle e_1 + \alpha f_1, x\rangle$ has $-$type if and only if either the determinant of the Gram matrix of the (induced) bilinear form on $\langle e_1 + \alpha f_1, x\rangle$ is a non-square or $\frac{q-1}{2}$ is odd. If $q \equiv 3 \pmod 4$, there is nothing to prove, hence we can assume that $q \equiv 1 \pmod 4$. We claim that, when $q \equiv 1 \pmod 4$, we can choose α to be a non-square.

Assuming the claim holds true, since the determinant of the Gram matrix of the (induced) bilinear form on $\langle e_1+\alpha f_1, x\rangle$ is 4α and we can choose α to be a non-square, then $\langle e_1+\alpha f_1, x\rangle$ has $-$type and consequently $\langle e_1 - \alpha f_1\rangle \in \mathcal{N}_-(G, 1)$. Now, let us prove the claim. Since $q \equiv 1 \pmod 4$, then the Jacobi symbol the Jacobi symbol $\left(\frac{-1}{q}\right)$ is 1. Since q may be not a prime, then -1 may be a non-square. First, note that, since the set of the square $(\mathbb{F}^*)^2$ is a subgroup of $(\mathbb{F}^*)$ and since $-\alpha$ is a non-square, when -1 is a square, then α is a non-square. Whilst if -1 is non-square, then then the Legendre symbol $\left(\frac{-1}{p}\right)$ is -1, and consequently $\left(\frac{\alpha}{p}\right) = -\left(\frac{-\alpha}{p}\right) = 1$. That is α is a square. Thus $-\alpha \equiv -1 \pmod{(\mathbb{F}^*)^2}$, and since $|\,\mathbb{F}^*/(\mathbb{F}^*)^2| = 2$, there exists $\alpha^\star \in \mathbb{F}^*$ such that both $\alpha^\star$ and $-\alpha^\star$ are non-square. Replacing α with $\alpha^\star$ the claim follows.

From [80, Lemma 2.5.11(ii)], since

$$\langle e_1-\alpha f_1+e_i\rangle^\perp = \langle e_1+\alpha f_1, x, f_1-f_i, e_i\rangle \oplus \langle e_2, \ldots, e_{i-1}, e_{i+1}, \ldots, e_a, f_a, \ldots, f_{i+1}, f_{i-1}, \ldots, f_3\rangle,$$

we deduce that $\langle e_1 - \alpha f_1 + e_i\rangle^\perp$ has $-$type if and only if $\langle e_1 + \alpha f_1, x, f_1 - f_i, e_i\rangle$ has $-$type. By [80, Propositions 2.5.13] we get that$\langle e_1 + \alpha f_1, x, f_1 - f_i, e_i\rangle$ has $-$type if and only if the determinant of the Gram matrix of the (induced) bilinear form on $\langle e_1 + \alpha f_1, x, f_1 - f_i, e_i\rangle$ is a non-square. Being the determinant of the Gram matrix equal to -4α and being 4 always a square, from our choice of α, we deduce that$\langle e_1 + \alpha f_1, x, f_1 - f_i, e_i\rangle \in \mathcal{N}_-(G, 1)$. With the same argument one can prove that $\langle e_1 - \alpha f_1 + e_i\rangle, \langle e_1 - \alpha f_1 + f_j\rangle, \langle e_2 - \alpha f_2 + e_1\rangle \in \mathcal{N}_-(G, 1)$ for $3 \leq i \leq a$, $2 \leq j \leq a - 1$

Observe that $\langle e_2 - \beta f_2 + x + f_1\rangle^\perp = \langle e_2 + \beta f_2, x - 2e_1, f_1, x - 2f_2\rangle \oplus \langle e_3, \ldots, e_a, f_a, \ldots, f_3\rangle$. Now, since the determinant of the Gram matrix of the (induced) bilinear form on $\langle e_2 + \beta f_2, x - 2e_1, f_1, x - 2f_2\rangle$ is $16(1 - \beta)$, that is a non-square according with our choice of β, form [80, Propositions 2.5.11(ii), 2.5.13], we deduce that $\langle e_2 - \beta f_2 + x + f_1\rangle \in \mathcal{N}_-(G, 1)$.

Table 3.3: Bases in small dimension for $\mathcal{N}(G,2)$ and $\mathcal{N}^+(G,2)$: $V_1 = \langle e_1, f_1\rangle$

G	$\mathcal{B}$	Notes
$\mathrm{PGU}(5,q)$, $\mathrm{PGO}^\circ_5(q)$	$\{V_1, \langle e_1+e_2, f_2\rangle, \langle f_2+x, e_2+f_1\rangle\}$	
$\mathrm{PSp}_6(q), \mathrm{PGU}_6(q)$,	$\{V_1, \langle e_1+f_2, f_2\rangle, \langle e_3+f_1, e_2+f_3\rangle, \langle e_1+e_2, e_2+f_1+f_3\rangle\}$	q odd
$\mathrm{PGO}^+(6,q)$	$\{V_1, \langle e_1+f_2, f_2\rangle, \langle e_3+f_1, e_2+f_3\rangle, \langle e_1+e_3+f_2, e_2+f_3+f_1\rangle\}$	q even
$\mathrm{PGO}^-_6(q)$	$\{V_1, \langle e_2, f_2\rangle, \langle e_1+x-f_1, e_2+y-\zeta f_2\rangle$	

Here, we shall show that $\mathcal{B}$ is a base for H, so let $g \in G_{(\mathcal{B})}$. Since $V_1 := \langle e_1 - \alpha f_1\rangle$ is non-degenerate, then $(V_1^\perp)^g$. In particular, $e_i g, f_j g \in V_1^\perp$, and so there exist $u_i, v_j \in V_1^\perp$ such that $e_i g = u_i$ and $f_j g = v_j$, for $2 \le i \le a$, and $2 \le j \le a-1$. Now, for $1 \le i \le a$ there exists $\nu_i, \nu_j^\star \in \mathbb{F}_q^*$ such that

$$(e_1 - \alpha f_1 + e_i)g = \nu_i(e_1 - \alpha f_1 + e_i) = \mu(e_1 - \alpha f_1) + u_i,$$
$$(e_1 - \alpha f_1 + f_j)g = \nu_j^\star(e_1 - \alpha f_1 + f_j) = \mu(e_1 - \alpha f_1) + v_j.$$

Equating coefficients shows that $e_i g = \nu_i e_i = \mu e_i$, and $f_j g = \nu_j^\star f_j = \mu f_j$ for $1 \le i \le a$, and $2 \le j \le a-1$. Here, with a similar argument applied to $V_2 := \langle e_2 - \alpha f_2 + e_1\rangle$, it is possible to deduce that $e_1 g = \mu e_1$.

Since $\langle e_2, \dots, e_{a-1}, f_{a-1}, \dots f_2\rangle$ is stable, hence $\langle e_2, \dots, e_{a-1}, f_{a-1}, \dots f_2\rangle^\perp = \langle e_1, e_a, x, f_a, f_1\rangle$ is stable. Hence $f_1 g = w$, for some $w \in \langle e_1, e_a, x, f_a, f_1\rangle$. Consequently

$$(e_1 - \alpha f_1)g = \mu(e_1 - \alpha f_1) = \mu e_1 - \alpha w,$$

that is $f_1 g = \mu f_1$. Now, since $(\langle e_1, \dots, e_{a-1}, f_{a-1}, \dots f_1\rangle^\perp)^g = \langle e_a, x, f_a\rangle$, then $xg = w_2$ $w_2 \in \langle e_a, x, f_a\rangle$. Thus

$$(e_2 - \beta f_2 + x + f_1)g = \xi(e_2 - \beta f_2 + x + f_1) = \mu(e_2 - \beta f_2 + f_1) + w_2,$$

and equating the coefficient we get that $xg = \mu x$. Here, the space $\langle e_a, f_a\rangle^\perp$ is non-degenerate and stabilised by g, so $\langle e_a, f_a\rangle^g = \langle e_a, f_a\rangle$. Lemma 3.1.3, applied with $(u,v) = (e_a, f_a)$, yields $f_a g = \mu f_a$. That is $g = \pm I$, as required. □

Proposition 3.1.17. *Let $d \ge 5$, let $\varepsilon \in \{+,-,\circ\}$, let $H \in \{\mathrm{PGU}_d(q), \mathrm{PSp}_d(q), \mathrm{PGO}^\varepsilon_d(q)\}$. Let $\mathcal{N}$ be $\mathcal{N}(H,2)$ when H is unitary or symplectic, and be $\mathcal{N}^+(H,2)$ when H is orthogonal. Let $b = b(H,\mathcal{N})$. If $d \ne 6$ then $b \le \lceil \frac{d}{2} \rceil$, whilst if $d = 6$ then $b \le 4$.*

Proof. Let G be the classical group such that $G/Z(G) = H$, and let B be the sesquilinear form of G. Let $\mathbb{F} = \mathbb{F}_{q^2}$ for the unitary case, and let $\mathbb{F} = \mathbb{F}_q$ otherwise. Let $\zeta = Q(y)$ for $\mathrm{GO}^-_d(q)$. For $d \le 6$ we list a base of the specified size in Table 3.3, so assume $d \ge 7$, let $a = \lceil d/2 \rceil$, and notice that $a \ge 4$.

We first define some useful subspaces. Let

$$V_1 = \langle e_1, f_1\rangle, \qquad V_2 = \langle e_1 + e_2, f_2\rangle, \qquad W_i = \langle e_i + f_1, e_2 + f_i\rangle, \quad \text{for } 3 \le i \le a-1.$$

One can check that

$$\mathcal{A} := \{V_1, V_2, W_i \mid 3 \le i \le a-1\} \subseteq \mathcal{N}.$$

Let $g \in G_{(\mathcal{A})}$, and let $X = \langle \mathcal{A}\rangle = \langle e_1, \dots, e_{a-1}, f_{a-1}, \dots, f_1\rangle$. We claim that there exist $\alpha, \beta \in \mathbb{F}$ such that

$$g|_X = \mathrm{Diag}(\alpha, \alpha, \beta, \dots, \beta, \alpha, \dots, \alpha, \beta, \beta). \tag{3.1.7}$$

To see this, first notice that $V_1^g = V_1$, and V_1 is non-degenerate, so $(V_1^\perp)^g = \langle e_2, \dots, f_2\rangle^g = \langle e_2, \dots, f_2\rangle$. Thus applying Lemma 3.1.12, with $T = V_2$ and $v_j = e_1$, we deduce that $f_2 g = \delta_2 f_2$, for some $\delta_2 \in \mathbb{F}$. From $V_1, V_2 \in \mathcal{B}$, we see that

$$(e_1 + e_2)g = \mu(e_1 + e_2) + \nu f_2 = \alpha e_1 + \alpha_2 f_1 + e_2 g$$

for some $\alpha, \alpha_2, \mu, \nu \in \mathbb{F}$. Since $e_2 g \in V_1^\perp$, equating coefficients yields

$$e_1 g = \alpha e_1, \text{ and } e_2 g = \alpha e_2 + \nu f_2. \tag{3.1.8}$$

Let $U = V_1 \oplus V_2$, and let $W = U^\perp$, so that $W^g = W$. For $3 \le i \le a-1$, the element g stabilises $U_i := \langle U, W_i\rangle$, and so stabilises $U_i \cap W = \langle e_i, f_i\rangle$. Hence for $3 \le i \le a-1$ there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}$ such that

$$e_i g = \alpha_i e_i + \beta_i f_i, \qquad f_i g = \gamma_i e_i + \delta_i f_i. \tag{3.1.9}$$

By Lemma 3.1.12, with $T = W_i$ and $v_j = f_1$, we deduce from (3.1.8) and (3.1.9) that $(e_2 + f_i)g = \eta(e_2 + f_i) = \alpha_1 e_2 + \nu f_2 + \gamma_i e_i + \delta_i f_i$. Hence, $\alpha = \delta_i$ and $\nu = \gamma_i = 0$. That is,

$$e_2 g = \alpha e_2, \quad f_i g = \alpha f_i \text{ for } 3 \le i \le a-1. \tag{3.1.10}$$

Now notice that $V_1^g = V_1$ also implies that

$$f_1 g = \gamma e_1 + \beta f_1, \tag{3.1.11}$$

for some $\gamma_1, \beta \in \mathbb{F}$. From Lemma 3.1.12, with $T = W_i$ and $v_j = e_2$, we deduce from (3.1.11) and (3.1.9) that there exists $\eta \in \mathbb{F}$ such that $(e_i + f_1)g = \eta(e_i + f_1) = \alpha_i e_i + \beta_i f_i + \gamma_1 e_1 + \beta f_1$. Hence, $\alpha_i = \beta$ and $\beta_i = \gamma_1 = 0$. That is,

$$e_i g = \beta e_i, \quad f_1 g = \beta f_1 \quad \text{for } 3 \le i \le a-1. \tag{3.1.12}$$

Finally, $B(e_1 g, f_1 g) = B(e_2 g, f_2 g) = 1$ yields

$$\alpha = \beta^{-q}, \text{ and } \alpha = \delta_2^{-q},$$

and hence $\delta_2 = \beta$, as required.

We now let V_3 be as in Table 3.4 and let $\mathcal{B} = \mathcal{A} \cup \{V_3\}$. A short computation shows in each case that $V_3 \in \mathcal{N}$. We shall show in each case that $\mathcal{B}$ is a base for $G/Z(G)$, so let $g \in G_{(\mathcal{B})}$. It follows immediately from (3.1.7) that

$$(X^\perp)^g = X^\perp. \tag{3.1.13}$$

Let $v_1 = x$ and $v_2 = y$ for $\mathrm{GO}_d^-(q)$, and $v_1 = e_a$ and $v_2 = f_a$ for the remaining even-dimensional cases. Then from (3.1.13), we deduce that there exist $\alpha_a, \beta_a, \gamma_a, \delta_a \in \mathbb{F}$ such that $v_1 g = \alpha_a v_1 + \beta_a v_2$ and $v_2 g = \gamma_a v_1 + \delta_a v_2$. We shall now repeatedly apply Lemma 3.1.12, with $T = V_3$ and various choices of v_j.

Case G $= \mathrm{GO}_{\mathbf{d}}^-(\mathbf{q})$. By setting $(u, v_j) \in \{(e_1 + x - f_1, f_2), (\zeta e_2 + y - f_2, e_1)\}$, we deduce that there exist $\eta, \xi \in \mathbb{F}$ such that

$$\begin{aligned}(e_1 + x - f_1)g &= \eta(e_1 + x - f_1) = \alpha e_1 + \alpha_a x + \beta_a y - \beta f_1,\\ (\zeta e_2 + y - f_2)g &= \eta(\zeta e_2 + y - f_2) = \alpha\zeta e_2 + \gamma_a x + \delta_a y - \beta f_2.\end{aligned}$$

Hence $\beta_a = \gamma_a = 0$ and $\alpha = \alpha_a = \delta_a = \beta$, so g is scalar.

Table 3.4: The final 2-space

G	V_3	Notes
$\mathrm{GO}_d^-(q)$	$\langle e_1+x-f_1, \zeta e_2+y-f_2\rangle$	
$\mathrm{GU}_{2a}(q), \mathrm{Sp}_d(q), \mathrm{GO}_d^+(q)$	$\langle e_1+e_a, e_2+f_a+f_1\rangle$	q odd
	$\langle e_1+e_a+f_2, e_2+f_a+f_1\rangle$	q even
$\mathrm{GU}_{2a-1}(q), \mathrm{GO}_d^\circ(q)$	$\langle \lambda e_1+x-f_1, \lambda e_2+x-f_2\rangle$	$\mathrm{tr}(\lambda)=1$ if G unitary,
		$\lambda=1$ otherwise.

Table 3.5: Bases in small dimension for $\mathcal{N}^-(H,2)$

H	$\mathcal{B}$	Notes
$\mathrm{PGO}_5(q)$	$\{\langle x+f_1, e_1+\zeta f_1\rangle, \langle x+f_2, e_2+\zeta f_2\rangle, \langle x+f_2+f_1, \zeta x+f_2\rangle\}$	
$\mathrm{PGO}_6^+(q)$	$\{V_1, V_2, W_3\}$, the V_is are defined in the proof of Proposition 3.1.18	q odd
	$\{\langle e_1+e_2+e_3+f_1, \zeta e_2+f_3+f_2+f_1\rangle, \langle e_2+f_2, \zeta e_1+f_3+f_2+f_1\rangle,$	q even
	$\langle e_1+\zeta f_2+f_1, e_1+e_2+f_3+\zeta f_1\rangle, \langle e_1+\zeta e_3+f_3, e_2+f_2+f_1\rangle\}$,	
$\mathrm{PGO}_6^-(q)$	$\{\langle x, y\rangle, \langle e_1+x, e_2+y+f_1\rangle, \langle e_2+x, e_1+y+f_2\rangle\}$	q odd
	$\{\langle x, y\rangle, \langle e_1+x, e_1+y+f_2\rangle, \langle e_2+x, e_2+y+f_2\rangle$	q even

Case $G \in \{\mathrm{GU}_{2a}(q), \mathrm{Sp}_{2a}(q), \mathrm{GO}_{2a}^+(q)\}$. By setting $v_j = e_1$, we see that there exists $\eta \in \mathbb{F}$ such that

$$(e_2+f_1+f_a)g = \eta(e_2+f_1+f_a) = \alpha e_2 + \beta f_1 + \gamma_a e_a + \delta_a f_a.$$

Hence $\alpha = \beta = \delta_a$, and $\gamma_a = 0$. Then by setting $v_j = f_1$ we deduce that there exist $\eta, \xi \in \mathbb{F}$ such that

$$\begin{aligned} (e_1+e_a)g &= \eta(e_1+e_a) = \alpha e_1 + \alpha_a e_a + \beta_a f_a && q \text{ odd}, \\ (e_1+e_a+f_2)g &= \xi(e_1+e_a+f_2) = \alpha e_1 + \alpha_a e_a + \beta_a f_a + \alpha f_2 && q \text{ even}. \end{aligned}$$

Hence $\beta_a = 0$ and $\alpha_a = \alpha$, and so g is scalar.

Case $G \in \{\mathrm{GU}_{2a-1}(q), \mathrm{GO}_d^\circ(q)\}$ By (3.1.13), there exists $\xi \in \mathbb{F}$ such that $xg = \xi x$.

Lemma 3.1.12, with $T = V_3$ and $v_j = e_2$, shows that there exists $\eta \in \mathbb{F}$ such that

$$(\lambda e_1 + x - f_1)g = \eta(\lambda e_1 + x - f_1) = \lambda\alpha e_1 + \xi x - \beta f_1.$$

Hence $\alpha = \beta = \xi$, so g is scalar. □

Proposition 3.1.18. *Let $d \geq 7$ and let $H = \mathrm{PGO}_d^\varepsilon(q)$, with $\varepsilon \in \{\circ, +, -\}$. Then $b(H, \mathcal{N}^-(H,2)) \leq \lceil \frac{d}{2} \rceil$.*

Proof. Let Q and B be as in Definition 3.1.6, and let $\mathbb{F} = \mathbb{F}_q$. Let $a = \lceil d/2 \rceil$, and notice that $a \geq 4$. Let $\zeta = Q(y)$ if $\varepsilon = -$, and let ζ be such that $X^2 + X + \zeta$ is irreducible otherwise, noting that $\zeta = 1$ if $q = 2$.

We first define some useful subspaces. Let

$$\begin{aligned} V_1 &= \langle e_1+f_1, e_2+\zeta f_2+f_1\rangle, \\ V_2 &= \langle e_2+f_2+f_1, e_1+\zeta f_1\rangle, && \text{if } \zeta \neq 1 \\ &= \langle e_2+f_2, e_1+f_2+f_1\rangle, && \text{if } \zeta = 1 \\ W_i &= \langle e_1+f_1+e_i, e_2+\zeta e_i+f_i\rangle, && \text{for } 3 \leq i \leq a-1. \end{aligned}$$

It is straightforward to verify that the basis vectors of each of these subspaces are an elliptic pair, so

$$\mathcal{A} := \{V_1, V_2, W_i \mid 3 \leq i \leq a-1\} \subseteq \mathcal{N}^-(G, 2).$$

Let $g \in G_{(\mathcal{A})}$, and let $X = \langle W_i \mid 3 \leq i \leq a-1 \rangle$. We shall show next that there exists $\alpha = \alpha^{-1} \in \mathbb{F}$ such that

$$vg = \alpha v \quad \text{for } v \in \{e_2, \ldots, e_{a-1}, f_{a-1}, \ldots, f_3, (e_1 + f_1)\}. \tag{3.1.14}$$

Let $U = \langle V_1, V_2 \rangle = \langle e_1, e_2, f_2, f_1 \rangle$, and $W = U^\perp$. Since $U^g = U$, and U is non-degenerate, it follows that $W^g = W$. For $3 \leq i \leq a-1$, the element g stabilises $U_i := \langle U, W_i \rangle$, and so stabilises $U_i \cap W = \langle e_i, f_i \rangle$. Hence for $3 \leq i \leq a-1$ there exist $\alpha_i, \beta_i, \gamma_i, \delta_i \in \mathbb{F}$ such that

$$e_i g = \alpha_i e_i + \beta_i f_i, \qquad f_i g = \gamma_i e_i + \delta_i f_i. \tag{3.1.15}$$

Since $V_1 \in \mathcal{B}$ there exist $\mu, \nu \in \mathbb{F}$ such that

$$(e_1 + f_1)g = \mu(e_1 + f_1) + \nu(e_2 + \zeta f_2 + f_1).$$

Then, for $3 \leq i \leq a-1$, the fact that $W_i \in \mathcal{A}$ yields

$$\begin{aligned}(e_1 + f_1 + e_i)g &= \mu_i(e_1 + f_1 + e_i) + \nu_i(e_2 + \zeta e_i + f_i) \\ &= \mu(e_1 + f_1) + \nu(e_2 + \zeta f_2 + f_1) + \alpha_i e_i + \beta_i f_i\end{aligned}$$

for some $\mu_i, \nu_i \in \mathbb{F}$. Looking at f_2, we see that $\nu = 0$. Hence $\nu_i = 0$, and consequently $\beta_i = 0$, and $\alpha_i = \mu$. That is,

$$(e_1 + f_1)g = \mu(e_1 + f_1), \quad \text{and} \quad e_i g = \mu e_i, \quad \text{for } 3 \leq i \leq a-1.$$

We now apply Lemma 3.1.3(2) with $(u, v) = (e_i, f_i)$ to see that

$$f_i g = \mu^{-1} f_i, \quad \text{for } 3 \leq i \leq a-1.$$

Again, since $W_i \in \mathcal{A}$, there exist $\eta_i, \theta_i \in \mathbb{F}$ such that

$$\begin{aligned}(e_2 + \zeta e_i + f_i)g &= \eta_i(e_1 + f_1 + e_i) + \theta_i(e_2 + \zeta e_i + f_i) \\ &= e_2 g + \mu\zeta e_i + \mu^{-1} f_i.\end{aligned}$$

Hence, from $e_2 g \in U$, we get that $\mu\zeta = \eta_i + \theta_i\zeta$, $\mu^{-1} = \theta_i$ and $e_2 g = \eta_i e_1 + \eta_i f_1 + \mu^{-1} e_2$. Furthermore, $Q(e_2 g) = 0$ implies $\eta_i = 0$, that is $e_2 g = \mu^{-1} e_2$, and finally $(e_2 + \zeta e_i + f_i)g = \theta_i(e_2 + \zeta ei + f_i)$ yields $\mu = \theta_i = \mu^{-1}$. Setting $\alpha = \mu$ yields (3.1.14).

Now we prove that there exists $\alpha_1, \theta_1 \in \mathbb{F}$ such that

$$e_1 g = \alpha_1 e_1 + (\alpha - \alpha_1) f_1 + \theta_1 e_2, \qquad f_1 g = (\alpha - \alpha_1) e_1 + \alpha_1 f_1 - \theta_1 e_2. \tag{3.1.16}$$

From $e_1 g, f_1 g \in U$, together with $B(e_1 g, e_2 g) = B(e_1 g, \alpha e_2) = 0$, and $B(f_1 g, e_2 g) = B(f_1 g, \alpha e_2) = 0$, we deduce that there exist $\alpha_1, \beta_1, \gamma_1, \delta_1, \theta_1, \mu_1 \in \mathbb{F}$ such that

$$e_1 g = \alpha_1 e_1 + \beta_1 f_1 + \theta_1 e_2, \quad f_1 g = \gamma_1 e_1 + \delta_1 f_1 + \mu_1 e_2.$$

Now from $(e_1 + f_1)g = \alpha(e_1 + f_1)$ we deduce that

$$f_1 g = (\alpha - \alpha_1) e_1 + (\alpha - \beta_1) f_1 - \theta_1 e_2.$$

From $Q(e_1 g) = 0$ we see that $\alpha_1 \beta_1 = 0$, and from $Q(f_1 g) = 0$ we see that $(\alpha - \alpha_1)(\alpha - \beta_1) = \alpha^2 - \alpha(\alpha_1 + \beta_1) + \alpha_1\beta_1 = 0$. Setting $\alpha_1\beta_1 = 0$, and using the fact that $\alpha \neq 0$, we deduce that $\beta_1 = \alpha - \alpha_1$ so (3.1.16) follows.

We now add one further subspace, depending on the form type. Let V_3 be

$$\langle e_1+e_2+f_2+f_a, f_1+e_3+\zeta f_3\rangle \text{ if } \varepsilon=+, \qquad \langle e_1+x-e_3, f_1+y+f_3\rangle \quad \text{if } \varepsilon=-,$$
$$\langle x+e_2+f_1, e_3+\zeta f_3+e_1\rangle \qquad \text{if } \varepsilon=\circ.$$

Then in each case the given basis vectors form an elliptic pair, so $V_3 \in \mathcal{N}^-(G,2)$. Let $\mathcal{B} := \mathcal{A}\cup\{V_3\}$. We shall show that $\mathcal{B}$ is a base for $G/Z(G)$, so let $g \in G_{(\mathcal{B})}$. Let $W = \langle\mathcal{A}\rangle$. From $W^g = W$, it follows that g stabilises $W^\perp$. Notice that if we can show that $\langle e_1, f_1\rangle^g = \langle e_1, f_1\rangle$ then it will follow from $U^g = U$ that $\langle e_2, f_2\rangle^g = \langle e_2, f_2\rangle$. Hence, it will follow from Lemma 3.1.3(2), with $(u,v) = (e_2, f_2)$ that $f_2g = \alpha^{-1}f_2 = \alpha f_2$. Hence, to show that g is scalar it suffices to show that $vg = \alpha v$ for $v = e_1, f_1$ and for whichever of $v \in \{e_a, f_a, x, y\}$ is required for the case.

Case $\varepsilon = +$. First notice that $V_3 \cap W = \langle f_1+e_3+\zeta f_3\rangle$, so it follows from (3.1.14) that $f_1g = \alpha f_1$, and hence from (3.1.16) that $e_1g = \alpha e_1$. Next, we apply Lemma 3.1.12 with $T = V_3$, and $v_j = f_a$ to see that $f_ag = \alpha f_a$. Finally, Lemma 3.1.3, applied to (f_a, e_a), yields that g is scalar.

Case $\varepsilon = \circ$. By Lemma 3.1.12 applied with $T = V_3$ and $v_j = x$, respectively $v_j = e_3$, we deduce from (3.1.16) that there exist $\eta, \xi \in \mathbb{F}$ such that

$$(x+e_2+f_1)g = \eta(x+e_2+f_1) = \xi x + \alpha e_2 + (\alpha-\alpha_1)e_1 + \alpha_1 f_1 - \theta_1 e_2.$$

Hence $\alpha = \xi = \alpha_1$, and $\theta_1 = 0$. That is $f_1g = f_1e_2$ and $xg = \alpha x$, so from (3.1.16) we see that $e_1g = \alpha e_1$, and so g is scalar.

Case $\varepsilon = -$. There exist $\alpha_a, \beta_a, \gamma_a, \delta_a$ such that $xg = \alpha_a x + \beta_a y$ and $yg = \gamma_a x + \delta_a y$. Then Lemma 3.1.12, applied twice to $T = V_3$, with $v_j = e_3$ and $v_j = f_3$, combines with (3.1.16) to yield

$$\begin{aligned}(e_1+x-e_3)g &= \alpha(e_1+x-e_3) = \alpha_1 e_1 + (\alpha-\alpha_1)f_1 + \theta_1 e_2 + \alpha_a x + \beta_a y,\\ (f_1+y+f_3)g &= \alpha(f_1+y+f_3) = (\alpha-\alpha_1)e_1 + \alpha_1 f_1 - \theta_1 e_2\gamma_a x + \delta_a y + \alpha f_3.\end{aligned}$$

Equating coefficients shows that g is scalar. □

3.1.2 Non-standard actions of almost simple groups

Definition 3.1.19. *Let G be an almost simple group with socle G_0, a classical group with natural module V over a field of characteristic p. A subgroup H of G not containing G_0 is a* subspace *subgroup if for each maximal subgroup M of G_0 containing $H \cap G_0$ one of the following holds:*

(1) $M = G_U$ for some proper nonzero subspace U of V, where U is either totally singular, or non-degenerate, or, if G is orthogonal and $p = 2$, a nonsingular 1-space (U is any subspace if $G_0 = \mathrm{PSL}(V)$);

(2) $G_0 = \mathrm{Sp}_{2m}(q)$, with $p = 2$ and $M \cap G_0 = \mathrm{GO}^{\pm}_{2m}(q)$.

A transitive action of G is a subspace action *if the point stabiliser is a subspace subgroup of G.*

Definition 3.1.20. *Let G be an almost simple group with socle G_0. A transitive action of G on Ω is* standard *if, up to equivalence of actions, one of the following holds:*

1. $G_0 = \mathrm{Alt}(\ell)$ and Ω is an orbit of subsets or partitions of $\{1,\ldots,\ell\}$;

2. G is a classical group in a subspace action.

Otherwise, a transitive action is non-standard.

Since the definition of standard is only up to permutation equivalence, we must be careful with exceptional isomorphisms between simple groups. In particular, it follows from the precise statement of [22, Theorem 1.1, Remark 1.1 and Table 1] that the orthogonal groups have standard actions in dimension four, five and six, as well as in dimension greater than six.

Cameron and Kantor conjectured in [32, 35] that there exists an absolute constant c such that $b(G) \leq c$ for all finite almost simple groups G in faithful primitive nonstandard actions. In [26, Theorem 1.3], Liebeck and Shalev proved the Cameron–Kantor conjecture, but without specifying the absolute constant c. Later, in a series of papers [22, 27, 25], Burness and others proved that $b(G) \leq 7$, with equality if and only if H is the largest Mathieu group M_{24} in its 5-transitive action of degree 24; that is, the Cameron-Kantor conjecture is true with the constant $c = 7$. The following is now immediate.

Lemma 3.1.21. *Let G be an almost simple primitive permutation group, with a non-standard action. Then Theorem 3.0.2 holds for G.*

In particular, this explains the constant 7 in Theorem 3.0.2, since $7 > \lceil \log 24 \rceil + 1$.

3.1.3 Action on partitions

In this section, we consider $\mathrm{Alt}(\ell)$ and $\mathrm{Sym}(\ell)$ acting on partitions of $\{1, \ldots, \ell\}$ into $s > 1$ subsets of size $t = \ell/s > 1$. We show that Theorem **??** holds for these permutation groups. Notice that the degree n of G is $\ell!/(t!)^s s!$.

Theorem 3.1.22. *Let G be $\mathrm{Sym}(st)$, acting on the collection of partitions of $\{1, 2, \ldots, st\}$ into $s \geq 2$ subsets of size t.*

(i) *If $t = 2$ then $b(G) = 3$.*

(ii) *If $s \geq t \geq 3$, then $b(G) \leq 6$.*

(iii) *If $s < t$ and $t \geq 3$ then $b(G) \leq \lceil \log_s t \rceil + 3$.*

Proof. Part (i) is noted in [25, Remark 1.6(ii)]. Parts (ii) and (iii) are [16, Theorem 4]. □

Theorem 3.1.23. *Let $s \geq 2$ and $t \geq 2$, with $\ell := st \geq 5$, and let G be $\mathrm{Sym}(\ell)$, acting on the collection of partitions of $\{1, 2, \ldots, \ell\}$ into s subsets of size t. Let n be the degree of the action. Then $b(G) \leq \log n + 1$, and in particular Theorem 3.0.2 holds for G.*

Proof. First assume that $t = 2$, so that $s \geq 3$ and $n \geq \frac{6!}{2^3 \cdot 3!} = 15$. Then $b(G) = 3$ by Theorem 3.1.22(i), so $b(G) < \log n$.

Next assume that $s \geq t \geq 3$. Then $n \geq \frac{9!}{(3!)^3 3!} = 280$, whilst $b(G) \leq 6$ by Theorem 3.1.22(ii), so $b(G) < \log n$.

For the remaining cases, by Theorem 3.1.22(iii)

$$b(G) \leq \lceil \log_s t \rceil + 3 \leq \log_s t + 4 = \log_s(\ell/s) + 4 = \log_s \ell + 3. \tag{3.1.17}$$

Next, consider $s = 2$, so that $t \geq 3$. We check directly in Magma that for $t = 3$, 4, 5 the base size of G is at most 4, 5 and 5, respectively, whilst $n = 10$, 35, 126. Hence $b(G) \leq \log n + 1$ in each case. Assume therefore that $\ell \geq 12$. Then

$$n = \frac{\ell!}{2((\ell/2)!)^2} = \frac{(\ell)(\ell-1)\ldots(\ell-\ell/2+1)}{2(\ell/2)!} = \frac{(\ell)(\ell-1)\ldots(\ell/2+2)(\ell/2+1)}{(\ell/2)(\ell/2-1)\ldots 2 \cdot 2} \geq 2^t = 2^{\ell/2}.$$

In particular, since $\ell \geq 12$, we deduce from (3.1.17) that

$$b(G) \leq \log \ell + 3 \leq \frac{\ell}{2} + 1 \leq \log n + 1.$$

Next, let $s = 3$. We may assume that $t > s$, so $\ell \geq 12$. Then, reasoning as for $s = 2$, we deduce that $n \geq 2^{\ell/3} \cdot 3^{\ell/3} = 6^{\ell/3} > 2^{2\ell/3}$. Hence $\log n > 2\ell/3$, so (3.1.17) yields

$$b(G) \leq \log \ell + 3 \leq \frac{2\ell}{3} + 1 \leq \log n + 1,$$

as required.

We are therefore left with $4 \leq s < t$, so that $\ell \geq 20$. Notice that

$$\log_s \ell = \frac{\log \ell}{\log s} \leq \frac{\log \ell}{2} \leq \log \ell - 2.$$

For all ℓ, the groups $\mathrm{Alt}(\ell)$ and $\mathrm{Sym}(\ell)$ have no core-free subgroups of index less than ℓ, since any such subgroup corresponds to a faithful permutation representation of degree less than ℓ. Hence $\ell \leq n$, and from (3.1.17) we deduce that

$$b(G) \leq \log_s \ell + 3 \leq \log \ell + 1 \leq \log n + 1.$$

□

3.1.4 Subspace actions

In this section we analyze the base size for primitive almost simple classical group in a subspace action. Hence, here $G \leq \mathrm{Sym}(\Omega)$ is a primitive almost simple classical group over $\mathbb{F}_q$ with point stabiliser a subspace subgroup H. Here, Ω is a G-orbit of (either non-degenerate, totally singular, non-singular or arbitrary subspace in case $G_0 = \mathrm{PSL}(V)$) k-dimensional subspace of (the natural module) V, for some natural number k. When $\dim V = d$ and $U \in \Omega$, by replacing U with $U^\perp$ if necessary or, in the case where $G_0 = \mathrm{PSL}(V)$, by considering the equivalent action of G on $(d-k)$-dimensional subspaces, we can always assume that $k \leq d/2$. We refear to [24, Table 4.1.1, Remark 4.1.3] for a detailed description of these actions and to [24, Table 4.1.2] for the corresponding degrees.

Lemma 3.1.24. [65, Proof of Theorem 3.3] *Let G_0 a simple classical group, acting on an orbit of k-spaces with $k \geq 3$. Then the following hold true.*

(i) Either $(G_0, k) = (\mathrm{P}\Omega^+_{2m}(q), m)$ and $b(G_0, \mathcal{S}(G, m)) \leq 9$ or $b(G_0, \mathcal{S}(G, k)) \leq d/k + 10$.

(ii) $b(G_0, \mathcal{N}(G, k)) \leq d/k + 11$.

Proposition 3.1.25. *Let G be an almost simple group with classical socle $G_0 = \mathrm{PSL}_d(q)$ with $d \geq 2$ and $q \geq 4$ when $d = 2$. Let Ω be the set of k-dimensional subspaces of $\mathbb{F}_q^d$, let $n = |\Omega|$, and assume that G acts primitively on Ω. Then $b(G, \Omega) < \log n + 1$.*

Proof. The degree of the action is

$$n = |\mathcal{S}(G, k)| = \frac{\prod_{i=d-k+1}^{d}(q^i - 1)}{\prod_{i=1}^{k}(q^i - 1)}. \tag{3.1.18}$$

First let $k = 1$. By Lemma 3.1.2 and Lemma 3.1.5, since G does not contain a graph automorphism, we deduce that

$$\begin{aligned} b := b(G, \mathcal{S}(G, 1)) &\leq d + 2 \\ &\leq d + 1 \quad \text{when } q \text{ is prime or } (q-1, d) = 1 \\ &\leq d \quad \text{when } q = 2 \end{aligned} \tag{3.1.19}$$

If $d = 2$ then $n = q + 1$ and $q \geq 4$. If q is prime or even then $\log(q+1)+1 \geq 3 = b$. Otherwise, $q \geq 9$ so $\log(q+1)+1 > 4 = b$. Hence we may assume that $d \geq 3$.

If $q = 2$ then $\log n + 1 > d = b$, whilst if $q = 3$ then $\log n + 1 \geq (d-1)\log 3 + 1 > d + 1 = b$, for $d \geq 4$, $\log n + 1 = \log(13) + 1 > 4$ for $d = 3$. If $q \geq 4$ then we deduce from (**??**) and (3.1.19) that

$$\log n + 1 \geq (d-1)\log q + 1 \geq \frac{d}{2}\log 4 + \frac{1}{2}\log 4 + 1 = d + 2 \geq b.$$

Next let $k = 2$. Then $n > |\mathcal{S}(G,1)|$. Let $b = b(G, \mathcal{S}(G,2))$. If $d \geq 6$ then G does not contain the graph automorphism, so it follows from Lemma 3.1.13 and Lemma 3.1.5 that $b \leq \lceil d/2 \rceil + 3 \leq d$, so the result follows as for $k = 1$.

If $d = 4$, by Lemma 3.1.13 and Lemma 3.1.5, then $b \leq 5$, when $q \leq 3$, and $b \leq 6$, when $q \geq 4$. Hence immediately follows from $n \geq q^4$. If $d = 5$ then $b \leq 6$, whilst $n > 2^6$.

Next assume that $k \geq 3$, so that $d \geq 6$. Now,

$$n = \frac{q^d - 1}{q-1} \cdot \frac{q^{d-1}-1}{q^2-1} \cdot \frac{q^{d-2}-1}{q^3-1} \prod_{i=1}^{k-3} \frac{(q^{d-k+i}-1)}{(q^{i+3}-1)} > q^{(d-1)+4} = q^{d+3}. \tag{3.1.20}$$

It is shown in the proof of [65, Theorem 3.3] that $b(G_0) \leq d/k + 5$. Hence, by Lemma 3.1.5 we deduce that

$$\begin{array}{lll} b(G, \mathcal{S}(G,k))) & \leq 10 & \text{when } k = d/2 \\ & \leq \frac{d}{k} + 8 & \text{when } k < d/2 \end{array} \tag{3.1.21}$$

Combining (3.1.20) with (3.1.21), we see that $\log n + 1 \geq d + 4 \geq b(G, \mathcal{S}(G,k))$ for all $d \geq 6$ and all q. □

Proposition 3.1.26. *Let G be an almost simple group with classical socle $G_0 = \mathrm{PSU}_d(q)$, with $d \geq 3$ and $(d,q) \neq (3,2)$. Let Ω be the set of k-dimensional totally singular or non-degenerate subspaces of $\mathbb{F}_{q^2}^d$, and let $n = |\Omega|$. Then $b(G,\Omega) < \log n + 1$.*

Proof. First we let Ω be the set of totally singular k-spaces. The degree of the action is

$$n = \frac{\prod_{i=d-2k+1}^{d}(q^i - (-1)^i)}{\prod_{i=1}^{k}(q^{2i}-1)} = \prod_{i=1}^{k} \frac{(q^{d-2k+2i-1} - (-1)^{d+i})(q^{d-2k+2i} - (-1)^{d+i+1})}{q^{2i}-1} \tag{3.1.22}$$

$$\geq \prod_{i=1}^{k}(q^{d-2k+2i-1}+1) \geq q^{(d-1)+(d-3)+(d-5)} = q^{3d-9}. \tag{3.1.23}$$

If $k = 1$ then from Lemma 3.1.9 and Lemma 3.1.5 we deduce that $b(G,\Omega) \leq d + 1$. Hence from (3.1.22) with $k = 1$ we see that

$$\log n + 1 \geq d \log q + 1 \geq d + 1 \geq b(G)$$

as required.

Next let $k = 2$. If $d = 4$ then from (3.1.22) we see that $n > q^4$. If $q = 2$ one may check the result using MAGMA , whilst it follows from Proposition 3.1.14 that $b(G,\Omega) \leq 6$ for all $q \geq 3$, so the result follows. If $d = 5$ then $n = (q^5+1)(q^3+1) > q^8$, whilst it follows from Proposition 3.1.14 that $b(G,\Omega) \leq 5$, so the result is immediate. If $d \geq 6$ then we deduce from Lemma 3.1.5 and Proposition 3.1.14 that $b(G,\Omega) \leq \lceil d/2 \rceil + 2 < d$, whilst from (3.1.22) we see that $n > |\mathcal{S}(G,1)|$. The result now follows immediately from the case $k = 1$.

Next we consider $k \geq 3$. For $(d,q) \in \{(6,2),(6,3),(7,2)\}$ it is straightforward to check in Magma [19] that the base size of G is at most 8, and the result follows. Otherwise, we deduce from Lemma 3.1.24(i) that

$$b(G, \mathcal{S}(G,k)) \leq \frac{d}{k} + 12. \tag{3.1.24}$$

For $(d,q)=(7,3)$ the result follows from $n=14948416>2^{23}$. Ler $d\geq 8$ and $q\leq 2$ then

$$\begin{aligned}\log n+1&\geq (3d-9)+1=3d-8\geq \frac{d}{3}+12\geq b(G,\mathcal{S}(G,k)),\\ &\geq 3d\log 3-9\log 3+1\geq \frac{9}{2}d-17\geq \frac{d}{3}+12\geq b(G,\mathcal{S}(G,k)),\end{aligned}$$

as required. If $q\geq 4$ and $d\geq 6$, then we deduce from (3.1.23) and (3.1.24) that

$$\begin{aligned}\log n+1&\geq (3d-9)\log q+1=d\log q+(2d-9)\log q+1\\ &\geq d\log q+3\log q+1\geq 2d+7\geq \frac{d}{3}+12\geq b(G,\mathcal{S}(G,k)).\end{aligned}$$

Now let $\Omega=\mathcal{N}(G,k)$. Then

$$n=\frac{q^{k(d-k)}\prod_{i=d-k+1}^{d}(q^i-(-1)^i)}{\prod_{i=1}^{k}(q^i-(-1)^i)}.$$

If $k\leq 2$, then $|\Omega|>|\mathcal{S}(G,k)|$. Our upper bound $b(\mathrm{PGU}_d(q),\mathcal{N}(G,1))\leq d$ from Lemma 3.1.15 agrees with that for $b(G,\mathcal{S}(G,1))$, so the result follows. Arguing as for totally singular subspaces, our upper bound $b(\mathrm{PGU}_d(q),\mathcal{N}(G,2))\leq \lceil d/2\rceil+\delta_{6d}<d$ from Proposition 3.1.17 now yields the result for $k=2$.

For $k\geq 3$, since $d\geq 2k+1\geq 7$, we get $\prod_{i=d-k+1}^{d}(q^i-(-1)^i)\geq (q^d-(-1)^d)\prod_{i=1}^{k}(q^i-(-1)^i)$. Hence $n\geq q^{k^2+k}(q^d-(-1)^d)\geq q^{d+11}$, By Lemma 3.1.5 and Lemma 3.1.24(i), we have $b(G,\mathcal{N}(G,k))\leq d/k+13$, and consequently $\log n+1\geq (d+11)\log q+1\geq d+12\geq d/3+13\geq b(G,\mathcal{N}(G,k))$. □

Proposition 3.1.27. *Let G be an almost simple group with classical socle $G_0=\mathrm{PSp}_d(q)$, with $d\geq 4$ and $(d,q)\neq(4,2)$. If $d=4$ then assume that G does not induce the exceptional graph automorphism. Let Ω be the set of k-dimensional totally singular or non-degenerate subspace of $\mathbb{F}_q^d$, and let $n=|\Omega|$. Then $b(G,\Omega)<\log n+1$.*

Proof. First assume that Ω consists of totally singular k-spaces, and let $b=b(G,\Omega)$. Then

$$n=\frac{\prod_{i=\frac{(d-2k)}{2}+1}^{\frac{d}{2}}(q^{2i}-1)}{\prod_{i=1}^{k}(q^i-1)}=\prod_{i=1}^{k}\frac{q^{d-2k+2i}-1}{q^i-1}. \tag{3.1.25}$$

If $k=1$ then from Lemma 3.1.9 and Lemma 3.1.5 we deduce that

$$\begin{aligned} b &\leq d+2 &&\\ &\leq d+1 && \text{when } q \text{ is even or prime}\\ &\leq d && \text{when } q=2.\end{aligned} \tag{3.1.26}$$

Comparing (3.1.26) and (3.1.19), and noting that if q is even then $(q-1,d)=1$, we see that the result follows in the same way as for $G_0=\mathrm{PSL}_d(q)$.

If $k=2$ we see from Proposition 3.1.14 that if $d\geq 6$ then $b(G_0,\Omega)\leq d-2$, so $b(G)\leq d$, and the result follows immediately from the case $k=1$. If $d=4$ then $b(G,\Omega)\leq 6<\log 40+1\leq \log n+1$.

If $k\geq 3$ then we use Lemma 3.1.24(i), and argue as in the proof of [65, Theorem 3.1] to deduce that

$$b(G,\mathcal{S}(d,k))\leq \frac{d}{k}+12, \tag{3.1.27}$$

and that $b(G,\mathcal{S}(G,k))\leq \frac{d}{k}+11$ when q is prime or a power of 2.

First suppose that $d-2k \geq 2$, so that $d \geq 8$. Then the degree of G is greater than the degree of $\mathrm{P}\Omega_d^{\pm}(q)$, acting on singular k-spaces, whilst the upper bound on $b(G, \mathcal{S}(d,k))$ is less than the corresponding bound for the orthogonal groups. Hence except for $(d,q) = (8,2)$, the estimation follows from 3.1.29. It therefore suffices to check only $(d,q) = (8,2)$, since these are the only cases that were calculated directly for the orthogonal groups: we calculate in Magma that if $(d,q) = (8,2)$ then $b(G, \mathcal{S}(G,3)) \leq 6$, so the result follows in this case too.

We may therefore assume that $k = \frac{d}{2}$, so that $b(G) \leq 14$ in general, $b(G) \leq 13$ if q is an odd prime or a power of 2 bigger than 2, and $b(G) \leq 12$ if $q = 2$. In this case the degree is

$$n = \prod_{i=1}^{\frac{d}{2}} (q^i + 1) \geq \prod_{i=1}^{\frac{d}{2}} q^i = q^{\frac{d(d+2)}{8}}. \tag{3.1.28}$$

Hence $\log n + 1 \geq \frac{d(d+2)}{8} \log q + 1$. If $d \geq 10$ then the result is therefore immediate.

If $d = 6$ then $n \geq q^d$. It is straightforward to calculate in Magma [19] that if $q \leq 3$ then $b(G, \mathcal{S}(G,3)) \leq 6$, so we may assume that $q \geq 4$. If $4 \leq q \leq 7$, then $\log n + 1 \geq 6 \log 4 + 1 = 13 \geq b(G)$. Whilst when $q \geq 8$, then $\log q \geq 3$. So $\log n + 1 \geq d \log q + 1 \geq b(G, \mathcal{S}(G,3))$. If $d = 8$ then for $q \geq 3$ we deduce that

$$\log n + 1 \geq 10 \log q + 1 \geq 16 \geq b(G).$$

For $q = 2$, notice that $n = 3 \cdot 5 \cdot 9 \cdot 17$, so $\log n + 1 \geq 12 = b(G, \mathcal{S}(G,4))$.

Next assume that $\Omega = \mathcal{N}(G,k)$, so that k is even and $2 \leq k \leq n/2 - 1$. Then

$$n = \frac{q^{\frac{k(d-k)}{2}} \prod_{i=\frac{d-k+2}{2}}^{\frac{d}{2}} (q^{2i} - 1)}{\prod_{i=1}^{\frac{k}{2}} (q^{2i} - 1)}.$$

If $k = 2$ then notice from (3.1.25) that $n > |\mathcal{S}(G,2)|$, whilst we have the same upper bound on $b(G, \Omega)$. Hence the result follows from that for $\mathcal{S}(G,2)$.

If $k \geq 4$, since $d \geq 2k+2$, we have $\prod_{i=\frac{d-k+2}{2}}^{\frac{d}{2}} (q^{2i} - 1) \geq (q^d - 1) q^2 \prod_{i=1}^{\frac{k}{2}} (q^{2i} - 1)$, and consequently $n \geq q^{\frac{k^2}{2}+k}(q^d - 1)q^2 \geq q^{d+13}$. By Lemma 3.1.5 and Lemma 3.1.24(ii), we get that $b(G, \mathcal{N}(G,k)) \leq \frac{d}{k} + 13$. Hence $\log n + 1 \geq (d+13) \log q + 1 \geq d + 14 \geq d/4 + 13 \geq b(G, \mathcal{N}(G,k))$. □

Lemma 3.1.28. *Let G be an almost simple group with classical socle G_0 one of $\mathrm{P}\Omega_4^-(q)$, $\mathrm{P}\Omega_5(q)$, $\mathrm{P}\Omega_6^{\pm}(q)$. Let Ω be a G-orbit of 1-spaces that are non-degenerate when q is odd and non-singular when q is even. If $G_0 = \mathrm{P}\Omega_4^-(q)$ then assume that $q > 3$. Then $b(G, \Omega) < \log |\Omega| + 1$.*

Proof. First let $d = 4$, so that $\mathrm{PGO}_d^-(q) \cong \mathrm{PSL}_2(q^2).2$, and $q \geq 4$. From Table 3.2 and Lemma 3.1.5, we deduce that $b(G, \Omega) \leq 6$. Moreover,

$$|\Omega| = \frac{q(q^2+1)}{(q-1,2)} > 2^6.$$

The result is therefore immediate.

Next let $d = 5$, so that q is odd and $\mathrm{PGO}_d(q) \cong \mathrm{PSp}_4(q).2$. Then $\mathrm{Aut}(\mathrm{P}\Omega_5(q))/\mathrm{PGO}_5(q)$ is cyclic, so from Table 3.2 and Lemma 3.1.5, we deduce that $b(G, \mathcal{N}) \leq 6$, whilst

$$n = |\mathcal{N}_{\pm}(G,1)| = \frac{q^2(q^4-1)}{2(q^2 \mp 1)} \geq 36 > 2^5,$$

so the result follows.

Finally, let $d = 6$, so that $\mathrm{PGO}^+_d(q) \cong \mathrm{PSL}_4(q).2$ and $\mathrm{PGO}^-_d(q) \cong \mathrm{PSU}_4(q).2$. From Lemma 3.1.16 and Lemma 3.1.5, we deduce that $b(G, \mathcal{N}) \leq 5$ if $q = 2$, and is at most 7 for $q > 2$. Moreover,

$$|\Omega| = \frac{q^2(q^3 \mp 1)}{(q-1,2)} > \begin{cases} 2^4 & \text{if } q = 2 \\ 2^6 & \text{if } q \geq 3. \end{cases}$$

The result follows. □

Proposition 3.1.29. *Let G be an almost simple group with classical socle $G_0 = \mathrm{P}\Omega^{\pm}_d(q)$, with $d \geq 8$. Let Ω be a G-orbit of k-dimensional totally singular, non-degenerate, non singular (for $k = 1$ and q even) subspaces of $\mathbb{F}_q^d$, and let $n = |\Omega|$. Assume that G acts primitively on Ω. Then $b(G, \Omega) < \log n + 1$.*

Proof. Let $\varepsilon \in \{+, -\}$. We first consider the action on $\mathcal{S}(\mathrm{P}\Omega^{\varepsilon}_d(q), k)$, so that $1 \leq k \leq d/2$, and $k < d/2$ if $\varepsilon = -$. Let $\delta = 1$ if $k = d/2$ and $\varepsilon = +$, and let $\delta = (q^{\frac{d-2k}{2}} + \varepsilon 1)$ The degree of the action is

$$n = |\mathcal{S}(\mathrm{P}\Omega^{\varepsilon}_d(q), k)| = \frac{\delta(q^{\frac{d}{2}} - \varepsilon 1) \prod_{i=\frac{d-2k}{2}+1}^{\frac{d}{2}-1} (q^{2i} - 1)}{\prod_{i=1}^{k}(q^i - 1)}. \tag{3.1.29}$$

If $\delta = 1$ then $2k < d$ and we bound this as follows

$$n \geq \frac{\delta(q^{\frac{d}{2}} - \varepsilon 1)(q^{d-2} - 1)}{q-1)} \prod_{i=2}^{k}(q^i + 1) \geq q^{\frac{d}{2}+\frac{d-2k}{2}-1} \prod_{i=2}^{k} q^i \geq q^{d-1-k} q^{\sum_{i=2}^{k} i} = q^{d-2+\frac{k(k-1)}{2}}. \tag{3.1.30}$$

When $k = 1$ (3.1.30) yields $n \geq q^{d-2}$. By Lemma 3.1.10 and Lemma 3.1.5 we deduce that

$$\begin{aligned} b(G) &\leq d+1 \\ &\leq d \qquad \text{when } q \text{ is even or prime} \\ &\leq d-1 \qquad \text{when } q = 2. \end{aligned}$$

If $q = 2$ then $\log n + 1 = (d-2)\log q + 1 = d - 1 \geq b(G)$. If $q = 3$ then $\log n + 1 > \frac{3}{2}d - 3 > d \geq b(G)$. If $q \geq 4$ then $\log q \geq 2$, and the result follows easily.

Next consider $k = 2$. Then $n > |\mathcal{S}(G, 1)|$, whilst we deduce from Lemma 3.1.5 and Proposition 3.1.14 that the base size is at most $\lceil d/2 \rceil + 2 < d - 1$. The result now follows immediately from the case $k = 1$.

Next, consider $k = d/2$, hence $\varepsilon = +$ and $\delta = 1$ in (3.1.30). Then (3.1.30) simplifies to

$$n = \prod_{i=1}^{\frac{d}{2}}(q^i + 1) \geq \prod_{i=1}^{\frac{d}{2}} q^i = q^{\frac{d(d+2)}{8}}. \tag{3.1.31}$$

From Lemma 3.1.24 we have that $b(G_0) \leq 9$, so (noting that the triality automorphism does not preserve 4-spaces in dimension 8) we deduce that $b(G) \leq 10$ when $q = 2$, and $b(G) \leq 12$ otherwise. Hence the result follows.

We are left with $3 \leq k \leq d/2-1$, for which we shall use the bound $b(G_0, \Omega) \leq d/k+10$ from Lemma 3.1.24(i). First assume $q \leq 3$. We calculate in Magma that for $(d, k, q) = (8, 3, 2)$ then $b(G, \Omega) \leq 4$, whilst the degree is at least 765. For $(d, k, q) = (8, 3, 3)$ we use the exact values of n from (3.1.29), and the fact that $G/G_0 \leq D_8$, to see that $\log n + 1 > 15 \geq b(G, \mathcal{S}(8, 3))$. For $d \geq 10$ and $k = 3$, we see from (3.1.29) that

$$n \geq \frac{(q^{\frac{d}{2}} \mp 1)(q^{\frac{d-6}{2}} \pm 1)}{q-1}(q^4+1)(q^2+1)(q^3+1) > q^{d-4} q^{4+3+2} \geq q^{d+5}.$$

Hence if $q = 2$ then $\log n + 1 \geq d + 6 \geq \frac{d}{3} + 11 \geq b(G, \mathcal{S}(G, 3))$, and if $q = 3$ then $\log n + 1 \geq \frac{3}{2}(d + 5) + 1 \geq \frac{d}{3} + 13 \geq b(G, \mathcal{S}(G, 3))$. If $k \geq 4$ then from (3.1.30) we see that $\log n + 1 \geq (d + 4) \log q + 1 \geq b(G, \mathcal{S}(G, k))$.

We may therefore assume that $q \geq 4$. From (3.1.30) we deduce that

$$\log n + 1 \geq \log(d - 2 + k) \log q + 1 \geq (d + 1) \log q + 1 \geq 2d + 3 \geq \frac{d}{3} + 13 \geq b(G, \mathcal{S}(G, k)).$$

Next we consider the action of G on Ω a G-orbit of k-spaces that are non-degenerate of ε'-type, with $\varepsilon' \in \{+, -, \circ\}$-type, or non-singular, when $k = 1$ and q is even. First let $k = 1$, then $\Omega = \mathcal{N}(G, 1)$. From Lemma 3.1.16 and Lemma 3.1.5, we deduce that $b(G, \mathcal{N}(G, 1)) = b(G, \mathcal{S}(G, 1))$. Moreover,

$$n = \mathcal{N}(G, 1) = \frac{q^{\frac{d}{2}-1}(q^{\frac{d}{2}} - \varepsilon 1)}{(q - 1, 2)} \geq q^{d-2}$$

Hence the result follows from that for $|\mathcal{S}(G, 1)|$. We can assume that $k \geq 2$. Now let $\varepsilon' \in \{+, -\}$, and let G acts on $\Omega = \mathcal{N}^{\varepsilon'}(G, k)$ be a G-orbit of non-degenerate k-spaces of ε' type. Note that we are implicitely assuming that k is even. When $\varepsilon = +$ we can assume that $k \leq \frac{d}{2} - 1$, whilst when $\varepsilon = -$ we have to analyze even the case $k = d/2$ (see [80, Table 3.5.F] for details.)

When $G_0 = \mathrm{P}\Omega_d^+(q)$, the degree of the action is

$$n = \frac{q^{\frac{k(d-k)}{2}}(q^{\frac{d}{2}} - 1) \prod_{i=\frac{d-k}{2}}^{\frac{d}{2}-1}(q^{2i} - 1)}{2(q^{\frac{k}{2}} - \varepsilon' 1)(q^{\frac{d-k}{2}} - \varepsilon' 1) \prod_{i=1}^{\frac{k}{2}-1}(q^{2i} - 1)}$$

Whilst when $G_0 = \mathrm{P}\Omega_d^-(q)$, the degree of the action is

$$n = \frac{q^{\frac{k(d-k)}{2}}(q^{\frac{d}{2}} + 1) \prod_{i=\frac{d-k}{2}}^{\frac{d}{2}-1}(q^{2i} - 1)}{2(q^{\frac{k}{2}} - \varepsilon' 1)(q^{\frac{d-k}{2}} + \varepsilon' 1) \prod_{i=1}^{\frac{k}{2}-1}(q^{2i} - 1)}.$$

If $k = 2$ then it follows from (3.1.29) that $n > |\mathcal{S}(G, 1)|$, whilst from Propositions 3.1.17, 3.1.18 and Lemma 3.1.5 we get $b(G, \Omega) \leq d/2 + 2 < d - 1$. Hence the result follows from that for $|\mathcal{S}(G, 1)|$.

Hence we can assume that $k \geq 4$. Let first consider the case $G_0 = \mathrm{P}\Omega_8^-(q)$ and $k = d/2$. Since

$$\frac{\prod_{i=\frac{d}{4}}^{\frac{d}{2}-1}(q^{2i} - 1)}{\prod_{i=1}^{\frac{k}{2}-1}(q^{2i} - 1)} \geq (q^{d-2} - 1)(q^2 + 1),$$

we deduce that

$$n = \frac{q^{\frac{d^2}{8}}(q^{\frac{d}{2}} + 1) \prod_{i=\frac{d}{4}}^{\frac{d}{2}-1}(q^{2i} - 1)}{2(q^{\frac{d}{4}} - 1)(q^{\frac{d}{4}} + 1) \prod_{i=1}^{\frac{d}{4}-1}(q^{2i} - 1)} \geq \frac{q^{\frac{d^2}{8}}(q^{d-2} - 1)}{2} \geq \frac{q^{2d-3}}{2}.$$

When $q \geq 3$, then $\log n + 1 \geq (2d - 3) \log q = d \log q + (d - 3) \log q \geq d \log 3 + 5 \log 3 \geq \frac{3}{2}d + 7 \geq \frac{d}{4} + 15 \geq b(G, \mathcal{N}(G, k))$, where the last inequality follows from a combination of Lemma 3.1.5 and Lemma 3.1.24(ii). When $q = 2$, form Lemma 3.1.5 and Lemma 3.1.24(ii), we deduce that $b(G, \Omega) \leq \frac{d}{4} + 12$. Hence for $d \geq 12$ we deduce that $\log n + 1 \geq (2d - 3) \log q = 2d - 3 \geq \frac{d}{4} + 12 \geq b(G, \Omega)$. A direct inspection using the exact value of n shows that for $\log n + 1 \geq \frac{d}{4} + 12 \geq b(G, \Omega)$ also when $d = 8$.

Hence from now on, we can consider in both cases $G_0 = \mathrm{P}\Omega_d^{\pm}(q)$ that $d \geq 2k+2$. Since $k \geq 4$, and $d \geq 2k+2$, we have $\prod_{i=\frac{d-k}{2}+1}^{\frac{d}{2}-1}(q^{2i}-1) \geq \prod_{i=1}^{\frac{k}{2}-1}(q^{2i}-1)$, hence in all the cases we get that

$$\begin{aligned} n &\geq \frac{q^{\frac{k(d-k)}{2}}(q^{\frac{d}{2}}-1)\prod_{i=\frac{d-k}{2}}^{\frac{d}{2}-1}(q^{2i}-1)}{2(q^{\frac{k}{2}}+1)(q^{\frac{d-k}{2}}+1)\prod_{i=1}^{\frac{k}{2}-1}(q^{2i}-1)} \geq \frac{q^{\frac{k(d-k)}{2}}(q^{\frac{d}{2}}-1)(q^{d-k}-1)}{2(q^{\frac{k}{2}}+1)(q^{\frac{d-k}{2}}+1)} \\ &\geq \frac{q^{\frac{k(d-k)}{2}}(q^{\frac{d}{2}}-1)(q^{\frac{d-k}{2}}-1)}{2(q^{\frac{k}{2}}+1)} \geq \frac{q^{\frac{k(k+2)}{2}}(q^{\frac{d}{2}}-1)(q^{\frac{d-k}{2}}-1)}{2(q^{\frac{k}{2}}+1)} \\ &\geq \frac{q^{\frac{k^2}{2}+k}q^{\frac{d}{2}-1}q^{\frac{d-k}{2}-1}}{4q^{\frac{k}{2}}} \geq \frac{q^{\frac{k^2}{2}+d-2}}{4} \geq \frac{q^{d+6}}{4}. \end{aligned}$$

Let $q \geq 3$. Then $\log n + 1 \geq (d+6)\log q - 1 \geq \frac{3}{2}d + 8 \geq \frac{d}{4} + 15 \geq b(G,\Omega)$, where the last inequality follows from a combination of Lemma 3.1.5 and Lemma 3.1.24(ii). Let $q = 2$. Now, from Lemma 3.1.5 and Lemma 3.1.24(ii), it follows that $b(G,\Omega) \leq \frac{d}{k} + 12$, hence $\log n + 1 \geq (d+6)\log 2 - 1 = d + 5 \geq \frac{d}{4} + 12 \geq b(G,\Omega)$.
Now, let $G_0 = \mathrm{P}\Omega_d^{\pm}(q)$, and let G acts on Ω a G-orbit of k-spaces of $\circ$ type. The degree of the action is

$$n = \frac{q^{\frac{(dk-k^2-1)}{2}}(q^{\frac{d}{2}} \mp 1)\prod_{i=\frac{d-k+1}{2}}^{\frac{d}{2}-1}(q^{2i}-1)}{2\prod_{i=1}^{\frac{k-1}{2}}(q^{2i}-1)}$$

Since $k \geq 3$, and $d \geq 2k+2$, we have $\prod_{i=\frac{d-k+1}{2}}^{\frac{d}{2}-1}(q^{2i}-1) \geq (q^3+1)\prod_{i=1}^{\frac{k-1}{2}}(q^{2i}-1)$. This and the fact that q has to be odd in this case yield

$$\begin{aligned} n &\geq \frac{q^{\frac{(dk-k^2-1)}{2}}(q^{\frac{d}{2}} \mp 1)(q^3+1)}{2} \geq \frac{q^{\frac{(k(2k+2)-k^2-1)}{2}}(q^{\frac{d}{2}} \mp 1)(q^3+1)}{2} \\ &\geq \frac{q^{\frac{(k^2+2k-1)}{2}}(q^{\frac{d}{2}-1}+\cdots+q+1)(q-1)(q^3+1)}{2} \geq q^{\frac{d}{2}+9}. \end{aligned}$$

Since $q \geq 3$ we deduce that

$$\log n + 1 \geq \left(\frac{d}{2}+9\right)\log q + 1 > d + 18 > \frac{3}{4}d + 14 \geq \frac{d}{3} + 15 \geq b(G,\mathcal{N}(G,k)),$$

where the last inequality follows from a combination of Lemma 3.1.5 and Lemma 3.1.24(ii). □

Proposition 3.1.30. *Let G be an almost simple group with classical socle $G_0 = \mathrm{P}\Omega_d^{\circ}(q)$, with $d \geq 7$. Let Ω be a G-orbit of k-dimensional totally singular or non-degenerate subspaces of $\mathbb{F}_q^d$, and let $n = |\Omega|$. Assume that G acts primitively on Ω. Then $b(G,\Omega) < \log n + 1$.*

Proof. First let $\Omega = \mathcal{S}(G,k)$.Then

$$n = \frac{\prod_{i=\frac{d-2k+1}{2}}^{\frac{d-1}{2}}(q^{2i}-1)}{\prod_{i=1}^{k}(q^i-1)} = \frac{(q^{d-1}-1)(q^{d-3}-1)\dots(q^{d-2k+1}-1)}{(q^k-1)\dots(q-1)} \tag{3.1.32}$$

(3.1.33)

If $k = 1$ then this yields $n = (q^{d-1} - 1)/(q - 1) > q^{d-2}$, and from Lemma 3.1.10 and Lemma 3.1.5 we deduce that $b(G) \leq d$ when $q = 3$, and $b(G) \leq d + 1$ otherwise. Now

$$\log n + 1 > (d - 2)\log(3) + 1 > d \geq b(G).$$

Next consider $k = 2$. Then $n > |\mathcal{S}(G, 1)|$, whilst we deduce from Lemma 3.1.5 and Proposition 3.1.14 that the base size is at most $\lceil d/2 \rceil + 1 < d - 1$. The result now follows immediately from the case $k = 1$.

Next let $3 \leq k < \frac{d}{2} - 1$, so that $d \geq 9$ and

$$n \geq \frac{(q^{d-1} - 1)}{(q - 1)} \cdot \frac{(q^{2k} - 1)\dots(q^4 - 1)}{(q^k - 1)\dots(q^2 - 1)} \geq q^{d-2} q^{\sum_{i=2}^{k} i} = q^{d-3+\frac{k(k+1)}{2}} \geq q^{d+3}. \tag{3.1.34}$$

Since $q \geq 3$, it follows from Lemma 3.1.24(i) that

$$\log n + 1 \geq (d + 3)\log q + 1 \geq \frac{3}{2}d + \frac{11}{2} \geq \frac{d}{3} + 12 \geq b(G).$$

Finally, assume that $k = \frac{d-1}{2}$, so that (3.1.32) simplifies to

$$n = \prod_{i=1}^{\frac{d-1}{2}} (q^i + 1) \geq q^{\frac{d-1}{4}(\frac{d+1}{2})} = q^{(d^2-1)/8}, \tag{3.1.35}$$

We calculate in Magma that if $(d, q) = (7, 3)$ then $b(G, \mathcal{S}(G, 3)) \leq 4$, whilst $n = 1120$. For all other d and q, it follows from Lemma 3.1.24(i) that

$$b(G, \mathcal{S}(G, (d - 1)/2)) \leq \frac{d}{\frac{d-1}{2}} + 10 + 2 \leq 3 + 12 = 15.$$

If $(d, q) = (7, 5)$ then $\log n + 1 = \log(6 \cdot 26 \cdot 126) + 1 > 15$. For all other d and q the result follows from $\log n \geq ((d^2 - 1)/8)\log q$. Note that if $(d, q) \neq (7, 3), (7, 5)$ then this is greater than 2^{14}.

We now let $\Omega = \mathcal{N}^{\pm}(G, k)$ for k even, with $2 \leq k < d/2$. The degree of the action is

$$n = \frac{q^{\frac{k(d-k)}{2}} \prod_{i=\frac{d-k+1}{2}}^{\frac{d-1}{2}} (q^{2i} - 1)}{2(q^{\frac{k}{2}} \mp 1) \prod_{i=1}^{\frac{k}{2}-1} (q^{2i} - 1)}.$$

For $k \geq 4$, since $d \geq 2k + 1$, we have $\prod_{i=\frac{d-k+1}{2}}^{\frac{d-1}{2}} (q^{2i} - 1) \geq (q^{d-1} - 1)q^3 \prod_{i=1}^{\frac{k}{2}-1} (q^{2i} - 1)$, and consequently

$$n \geq \frac{q^{\frac{k^2}{2}+\frac{k}{2}}(q^{d-1} - 1)q^3}{2(q^{\frac{k}{2}} \mp 1)} \geq \frac{q^{\frac{k^2}{2}+3+d-2}}{4} \geq \frac{q^{d+9}}{4}.$$

Since $q \geq 3$, combining Lemma 3.1.5 and Lemma 3.1.24(ii), we deduce $\log n + 1 \geq (d + 9)\log q - 1 \geq 3d/2 + 12 \geq d/4 + 13 \geq b(G, \mathcal{N}^{\pm}(G, k))$.

Similarly, $|\mathcal{N}^{\pm}(G, 2)| \geq |\mathcal{S}(G, 2)|$, whilst $b(\mathrm{PGO}_d(q), \mathcal{N}^{\pm}(\mathrm{PGO}_d(q), 2) \leq \lceil d/2 \rceil$ by Propositions 3.1.17 and 3.1.18. This is the same bound as we found in Proposition 3.1.14 for $b(G, \mathcal{S}(G, 2))$, so the result for $\mathcal{N}^{\pm}(G, 2)$ follows immediately from that for $\mathcal{S}(G, 2)$.

Let G acts on non-degenerate k-spaces of $\circ$ type. Here, k is odd, $d \geq 2k + 1$, and the degree is

$$n = \frac{q^{\frac{k(d-k)}{2}} \prod_{i=\frac{k+1}{2}}^{\frac{d-1}{2}} (q^{2i} - 1)}{2(q^{\frac{d-k}{2}} \mp 1) \prod_{i=1}^{\frac{d-k}{2}-1} (q^{2i} - 1)}.$$

When $k = 1$, then

$$n = \frac{q^{\frac{(d-1)}{2}}(q^{d-1}-1)}{2(q^{\frac{d-1}{2}} \mp 1)} \geq \frac{q^{\frac{(d-1)}{2}}(q^{\frac{(d-1)}{2}}-1)}{2} \geq \frac{q^{d-2}}{2}.$$

From Lemma 3.1.5 and Lemma 3.1.16 we deduce that $b(G, \mathcal{N}(G,1)) \leq d-1$ if q is a prime and $b(G, \mathcal{N}(G,1)) \leq d$ otherwise. When $q = 3$ we have that $\log n + 1 \geq (d-2)\log q \geq 3/2d - 4 \geq d - 1 \geq b(G, \mathcal{N}(G,1))$, whilst for $q \geq 5$ we deduce that $\log n + 1 \geq (d-2)\log q \geq d/2 \log 5 + (d/2 - 2)\log 5 > d \geq b(G, \mathcal{N}(G,1)$. We can assume that $k \geq 3$. We have that $\prod_{i=\frac{k+1}{2}}^{\frac{d-1}{2}}(q^{2i}-1) \geq (q^{d-1}-1)q^2 \prod_{i=1}^{\frac{d-k}{2}-1}(q^{2i}-1)$, and consequently

$$n \geq \frac{q^{\frac{k(d-k)}{2}}q^2(q^{d-1}-1)}{2(q^{\frac{d-k}{2}} \mp 1)} \geq \frac{q^{\frac{k(d-k)}{2}}q^2(q^{d-1}-1)}{4q^{\frac{d-k}{2}}} = \frac{q^{\frac{(k-1)(d-k)}{2}}q^2(q^{d-1}-1)}{4} \geq \frac{q^4 q^2 q^{d-2}}{4} = \frac{q^{d+4}}{4}.$$

It follows that $\log n + 1 \geq (d+4)\log q - 1 \geq 3d/2 + 5 \geq d/3 + 13 \geq b(G, \mathcal{N}(G,k))$ (as usual, the last disequality follows combining Lemma 3.1.5 and Lemma 3.1.24(ii)).

□

Case (2)

Let G be an almost simple group with classical socle $\mathrm{Sp}_{2m}(2^f)$, and let $M = \mathrm{GO}^{\pm}_{2m}(2^f)$. In this section we will analyze the action of G on M/G the set of right cosets of M in G.

Lemma 3.1.31. *Let $g \in \mathrm{GO}^{\varepsilon}_d(2^f)$, with $\varepsilon \in \{+,-\}$, and let v be a non-singular vector (that is $Q(v) \neq 0$). If $\langle v \rangle^g = \langle v \rangle$, then $vg = v$.*

Proof. There exists $\beta \in \mathbb{F}^*$ such that $zg = \beta z$. Hence $Q(z) = Q(zg) = Q(\beta z) = \beta^2 Q(z)$, and consequently $\beta^2 = 1$. Since $\mathbb{F}$ has even characteristic, then $\beta = 1$. □

Proposition 3.1.32. *Let $G = \mathrm{Sp}_{2m}(2)$ with $2m \geq 6$, and let $M = \mathrm{GO}^{\pm}_{2m}(2)$. Then $b(G, M/G) = 2m$.*

Proof. We work by using the equivalent action of $\mathrm{GO}^{\pm}_{2m}(2)$ on the two orbits of non degenerate $2m$-dimensional subspaces of V of $\pm$ type.

Let $H = \mathrm{GO}^{\circ}_{2m+1}(2)$ with standard quadratic form Q of Witt index m and let $\mathcal{N}_{\pm}$ be the set of $2m$-dimensional subspace of V of type $\pm$. Let us first consider the action of H on $\mathcal{N}_+$. Let

$$\begin{aligned} T &:= \langle e_1, \ldots, e_m, f_m, \ldots, f_1 \rangle, \\ V_i &:= \langle e_1, \ldots, e_{2i}, e_{2i+1} + x, e_{2i+2}, \ldots, e_m, f_m, \ldots, f_1 \rangle, \\ W_j &:= \langle e_1, \ldots, e_m, f_m, \ldots, f_{2j+2}, f_{2j+1} + x, f_{2j}, \ldots, f_1 \rangle, \end{aligned}$$

and let $\mathcal{B} := \{T, V_i, W_j \mid 1 \leq i \leq m, 1 \leq j \leq m-1\}$. It is straightforward to show that $\mathcal{B} \in \mathcal{N}_+$, and we shall show that $\mathcal{B}$ is a base for H. Let $g \in H$. Note that

$$\left(\bigcap_{1 \leq i \leq m-1} (V_i \cap W_i) \right)^g = \langle e_m, f_m \rangle^g = \langle e_m, f_m \rangle,$$

$$\left(V_m \cap \bigcap_{1 \leq i \leq m-1} (V_i \cap W_i) \right)^g = \langle f_m \rangle^g = \langle f_m \rangle.$$

Using this and Lemma 3.1.3 we deduce that $e_m g = \alpha_m e_m, f_m g = \alpha_m^{-1} f_m$. Consequently

$$\Big(T \cap \langle e_m, f_m\rangle^{\perp}\Big)^g = \langle e_1, \dots, e_{m-1}, f_{m-1}, \dots f_1\rangle^g = \langle e_1, \dots, e_{m-1}, f_{m-1}, \dots f_1\rangle = T_m.$$

Let $1 \leq i \leq m-1$. Hence

$$\left(T_m \cap V_i \bigcap_{1\leq k\leq m-1, k\neq i} (V_k \cap W_k)\right)^g = \langle f_i\rangle^g = \langle f_i\rangle,$$
$$\left(T_m \cap W_i \bigcap_{1\leq k\leq m-1, k\neq i} (V_k \cap W_k)\right)^g = \langle e_i\rangle^g = \langle e_i\rangle,$$

that is $e_i g = \alpha_i e_i, f_i = \alpha^{-1} f_i$, for $1 \leq i \leq m-1$. Further, observe that $(T^{\perp})^g = \langle x\rangle^g = \langle x\rangle$. Consequently, from Lemma 3.1.31, we deduce that $xg = x$. Now, from Lemma 3.1.12, applied with $(u, v_j) = (e_i + x, f_i)$, we deduce that $(e_i + x)g = \nu(e_i + x) = \alpha_i e_i + x$, that is $\nu = \alpha_i = 1$. Hence $g = I$, as required.

Here, we analyze the action of H on $\mathcal{N}_-$. We can assume $d \geq 7$. First, we define some useful subspaces.

Let $A_k := \langle e_k, f_k\rangle$ for $1 \leq k \leq m$, let $2 \leq i \leq m$, let $2 \leq j \leq m-1$, and let

$$\begin{aligned}
T &:= \langle e_1 + x, f_1 + x\rangle \oplus A_2 \oplus \cdots \oplus A_m,\\
U_i &:= \langle e_1 + x, f_1 + x\rangle \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus \langle e_i, f_i + x\rangle \oplus A_{i+1} \oplus \cdots \oplus A_m\\
U_j^{\star} &:= \langle e_1 + x, f_1 + x\rangle \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus \langle e_i + x, f_i\rangle \oplus A_{i+1} \oplus \cdots \oplus A_m\\
U_m^{\star} &:= \langle e_1, f_1\rangle \oplus \langle e_2 + x, f_2 + x\rangle \oplus A_3 \oplus \cdots \oplus A_m\\
W &:= \langle e_1, f_1 + x\rangle \oplus \langle e_2 + x, f_2 + x\rangle \oplus A_3 \oplus \cdots \oplus A_m.
\end{aligned}$$

Let $\mathcal{B} := \{T, U_i, U_i^{\star}, W \mid 2 \leq i \leq m\}$. Since each subspaces is written as an orthogonal direct sum of non-degenerate 2-spaces, one can observe that $\mathcal{B} \in \mathcal{N}_-$. We shall show that $\mathcal{B}$ is a base for H.

Let $g \in H$, and let $2 \leq i \leq m$. Note that $T + U_i = V$, hence $\dim(T \cap U_i) = 2m-1$, and so

$$T \cap U_i = \langle e_1 + x, f_1 + x\rangle \oplus A_2 \oplus \cdots \oplus A_{i-1} \oplus A_{i+1} \oplus \cdots \oplus A_m \oplus \langle e_i\rangle.$$

The radical $\mathrm{Rad}(T \cap U_i) = \langle e_i\rangle$, and since $(T \cap U_i)^g = (T \cap U_i)$, we deduce that

$$(\mathrm{Rad}(T \cap U_i))^g = \langle e_i\rangle^g = \langle e_i\rangle,$$

that is $e_i g = e_i$ for $2 \leq i \leq m$. Similarly we deduce that $f_j g = f_j$, for $2 \leq j \leq m-1$. Since $A_2 \oplus \cdots \oplus A_{m-1}$ is non-degenerate and this is fixed by g, we deduce that

$$((A_2 \oplus \cdots \oplus A_{m-1})^{\perp})^g = (A_1 \oplus \langle x\rangle \oplus A_m)^g = A_1 \oplus \langle x\rangle \oplus A_m.$$

Now, since $(U_m^{\star})^g = U_m^{\star}$, we get that $(U_m^{\star} \cap (A_1 \oplus \langle x\rangle \oplus A_m))^g = (A_1 \oplus A_m)^g = A_1 \oplus A_m$. From this and from $W^g = W$, we deduce that $((A_1 \oplus A_m) \cap W)^g = (\langle e_1\rangle \oplus A_m)^g = \langle e_1\rangle \oplus A_m$. Consequently, $(\mathrm{Rad}(\langle e_1\rangle \oplus A_m))^g = \langle e_1\rangle^g = \langle e_1\rangle$, that is $e_1 g = e_1$. Moreover, $(\langle e_1\rangle \oplus A_m) \cap T = A_m^g = A_m$. Hence, since $e_m g = e_m$, from Lemma 3.1.3 with $(u, v) = (e_m, f_m)$, we deduce that $f_m g = f_m$. Consequently, $(A_m^{\perp} \cap (A_1 \oplus A_m))^g = A_1$, and applying Lemma 3.1.3 with $(u, v) = (e_1, f_1)$, we deduce $f_1 g = f_1$. Since $\langle x\rangle^g = \langle x\rangle$, we get that $g = I$, as required.

Let $H := \mathrm{GO}_{2m+1}(2)$ and let V be the natural module for H, so that $\mathrm{Rad}(V) = \langle x\rangle$. Hence B_Q induces a non-degenerate alternating form $\bar{B}$ on the quotient space $\bar{V} := V/\mathrm{Rad}(B) =$

$V/\langle x\rangle$, and H naturally acts on $\bar{V}$ as $G := \mathrm{Sp}_{2m}(2)$. Now, let $\mathcal{B} := \{T, V_1, \ldots, V_{2m-2}\}$ be a set containing $2m-1$ different non-degenerate $2m$-subspaces of the same type (either $+$ or $-$) in V; we want to show that $H_{(\mathcal{B})} \neq 1$. Note that the stabiliser in H of T is $H_T = \mathrm{GO}^{\varepsilon}_{2m}(2)$ and H_T acts on T as the subgroup $\mathrm{GO}^{-}_{2m}(2)$ of $\mathrm{Sp}_{2m}(2)$, whilst fixing $\langle x\rangle$.

Since $T \cap V_i$ has dimension $2m-1$, the restriction of B_Q to $T \cap V_i$ is degenerate, and so $T \cap V_i$ has one-dimensional radical $\langle v_i\rangle$, and so the 2-point stabiliser in G of T and V_i stabilises $v_i \in T$. Furthermore, $\dim(v_i^{\perp} \cap T) = 2m-1$, so $T \cap V_i = T \cap v_i^{\perp}$. Furthermore, since the action of G on the cosets of M is 2-transitive (see, for example, [48]), we may assume that $Q(v_i) = 0$ also. Hence the stabiliser of $\mathcal{B}$ in H is equal to the stabiliser of $2m-1$ totally singular 1-spaces in $\mathrm{GO}^{\varepsilon}_{2m}(2)$. This group is nontrivial by Lemma 3.1.11. □

Proposition 3.1.33. *Let $q = 2^f$, and let G be an almost simple group with socle $\mathrm{Sp}_d(q)$ where $d \geq 4$. Assume that if $d = 4$ then $q > 2$. Let $M = \mathrm{GO}^{\varepsilon}_d(q)$ and Ω the set of right cosets of M in G, and let $|\Omega| = n$. If $\varepsilon = -$ and $q = 2$ then $\log n + 1 < b(\mathrm{Sp}_d(2), \Omega) = \lceil \log n \rceil + 1$. Otherwise, $b(G, \Omega) \leq \log n + 1$.*

Proof. Let $d = 2m$ so that $m \geq 2$. Then $n = q^m(q^m - \varepsilon 1)/2$. If $q = 2$ by Proposition 3.1.32 we deduce that $b(G) = 2m$ If $\varepsilon = +$, then $n \geq q^{2m-1}$, hence $\log n + 1 \geq (2m-1)\log 2 + 1 = 2m = b(G)$. If $\varepsilon = -$ then $\lceil \log n \rceil + 1 = 2m = b(G)$.

Assume that $q \geq 4$. It is proved in [65] that $b(\mathrm{soc}(G), \Omega) \leq 2m+1$, so (since q is even), it follows from Lemma 3.1.5 that the base size of G is at most $2m+2$. Therefore

$$\begin{aligned}\log n + 1 &\geq \log\left(\frac{q^{2m-1}}{2}\right) + 1 \geq (2m-1)\log q \geq m\log q + (m-1)\log q \\ &\geq m\log q + \log q \geq 2m + 2 \geq b(G).\end{aligned}$$

□

Novelty

Let $G \leq \mathrm{Sym}(\Omega)$ be an almost simple classical group over $\mathbb{F}_q$ with socle G_0, with natural module V. It remains to deal with certain novelty subgroups H of G, where $H_0 = H \cap G_0$ is non-maximal in G_0. In particular, one of the following holds:

(i) $G_0 = \mathrm{PSL}_d(q)$, $d \geq 3$ and G contains graph or graph-field automorphisms;

(ii) $G_0 = \mathrm{PSp}_4(q)$, q even and G contains graph-field automorphisms;

(iii) $G_0 = \mathrm{P}\Omega^+_8(q)$ and G contains triality automorphisms.

Case (i) Let $G_0 = \mathrm{PSL}_d(q)$ with $d \geq 3$, and let

$$\begin{aligned}\mathcal{S}_1(G,k) &:= \{\{U, W\} \mid U \subset W, \dim U = k, \dim W = d-k\} \\ \mathcal{S}_2(G,k) &:= \{\{U, W\} \mid V = U \oplus W, \dim U = k < d/2\}.\end{aligned}$$

Proposition 3.1.34. *Let G be an almost simple group with socle $G_0 = \mathrm{PSL}_d(q)$, $d \geq 3$, containing a graph or graph-field automorphisms, let $i \in \{1, 2\}$, and let $n_i := |\mathcal{S}_i(G,k)|$. Then $b(G, \mathcal{S}_i(G,k)) \leq \log n_i + 1$.*

Proof. Recall that, $\mathcal{S}(G,k)$ denoted the set of k-dimensional subspaces of V.

Let $K_i = G_{(U,V)}$ be the stabilizers of the pairs U, V in $\mathcal{S}_i(G,k)$, and let $U \in \mathcal{S}(G,k)$. Then $K_i \cap G_0$ is a subgroup of $H = (G_0)_U$.

There exist b conjugates of H whose intersection is trivial. Here, by Lemma 3.1.5 we have that

$$b_i := b(G, \mathcal{S}_i(G,k)) \leq b + c, \tag{3.1.36}$$

with $c = 1$ when $q = 2$, $c = 2$ when $q = 3$, and $c = 3$ when $q \geq 4$. Denoting by $n = |\mathcal{S}(G, k)|$, it is not difficult to observe that

$$n \leq (n_i/2^c) \tag{3.1.37}$$

Now, from Proposition 3.1.25 and (3.1.36), (3.1.37) we deduce

$$b_i \leq b + c \leq \log n + 1 + c \leq \log(n_i/2^c) + 1 + c = \log n_i + 1,$$

as desidered.

□

Case (ii) Let $G_0 = \mathrm{PSp}_4(q)$, $q = 2^e \geq 4$, then $\Omega = G/H$ is the set of right cosets of $H = [q^4] \,.\, \mathrm{GL}_1(q)^2$.

Proposition 3.1.35. *Let G be an almost simple group with socle $G_0 = \mathrm{PSp}_4(q)$, $q = 2^e \geq 4$, containing graph-field automorphisms, and let $\tilde{n} = |\Omega|$ Then $b(G, \Omega) \leq \log \tilde{n} + 1$.*

Proof. Let $U \in \mathcal{S}(G, 1)$. Then $H \cap G_0$ is a subgroup of $K = (G_0)_U$. There exist b conjugates of H whose intersection is trivial. Here, by Lemma 3.1.5 we have that $b(G, \Omega) \leq b + 2$. Note that $n \leq (\tilde{n}/4)$, where $n = |\mathcal{S}(G, 1)|$. Hence, from Proposition 3.1.27, we deduce that $b(G, \Omega) \leq b + 2 \leq \log n + 1 + 2 \leq \log(\tilde{n}/4) + 1 + 2 = \log \tilde{n} + 1$, as required.

□

Case (iii) Let $G_0 = \mathrm{P}\Omega_8^+(q)$, then we have to consider the action of G on $\Omega = G/H$ the set of right cosets of $H = [q^{11}] : \left[\frac{q-1}{(2,q-1)}\right]^2 . \frac{1}{(2,q-1)} \mathrm{GL}_2(q) \,.d^2$.

Proposition 3.1.36. *Let G be an almost simple group with socle $G_0 = \mathrm{P}\Omega_8^+(q)$, containing triality automorphisms, and let $\tilde{n} = |\Omega|$. Then $b(G, \Omega) \leq \log \tilde{n} + 1$.*

Proof. Let $U \in \mathcal{S}(G, 1)$, and let $n = |\mathcal{S}(G, 1)|$. Then $H \cap G_0 = [q^{11}] \,.\, \mathrm{GL}_2(q)\mathrm{GL}_1(q)^2$ is a subgroup of $K = (G_0)_U$. From Proposition 3.1.29, we deduce that there exist $b \leq \log n + 1$ conjugates of K whose intersection is trivial. Now, by Lemma 3.1.5 we have that $b(G, \Omega) \leq b + 5$. Note that $n < (\tilde{n}/32)$. Hence we deduce that $b(G, \Omega) \leq b + 5 \leq \log n + 1 + 5 \leq \log(\tilde{n}/32) + 1 + 5 = \log \tilde{n} + 1$, as required.

□

3.1.5 Proof of Theorem 3.0.2

In this section, we prove Theorem 3.0.2.

Theorem 3.1.37. *Let $G \leq \mathrm{Sym}(\Omega)$ be an almost simple group of degree n, and assume that G is not large base. Then $b(G) \leq \lceil \log n \rceil + 1$. Moreover if $b(G) > \lceil \log n \rceil + 1$, then $G = M_{24}$, $n = 24$ and $b(G) = 7$.*

Proof. Let $G_0 = \mathrm{soc}(G)$. First notice that the only non-large-base almost simple groups of degree at most 8 are the actions of $\mathrm{Alt}(5)$ and $\mathrm{Sym}(5)$ on 6 points, of $\mathrm{PSL}_3(2)$ on 7 points, and of $\mathrm{PSL}_2(7)$ and $\mathrm{PGL}_2(7)$ on 8 points, all of which have base size 3, which is less than $\log n + 1$. Hence the result holds for $n \leq 8$, and for $b(G) \leq 3$.

Since the groups $\mathrm{PSL}_2(q)$ are isomorphic to many other simple groups, we shall consider them next. Let G be an almost simple group with socle $\mathrm{PSL}_2(q)$ for $q \geq 5$, and let Ω be the right cosets of some maximal subgroup H of G. We work through the choices for H, as described in [20, Table 8.1]. The result for $H \in \mathcal{C}_1$ follows from Proposition 3.1.25. Burness shows in [22, Table 3] that $b(G) \leq 3$ for the majority of the remaining choices of H. More precisely, he shows that $b(G) \leq 3$ if $H \in \mathcal{C}_2 \cup \mathcal{C}_3$, or if $H \in \mathcal{C}_5$ and the index $[q : q_0]$ is odd; or if $H \in \mathcal{C}_6$ and $q > 7$; or if $H \in \mathcal{C}_9$ and $q \neq 9$. We therefore need consider only the exceptions.

If $H \in \mathcal{C}_5$ and $[q_0 : q] = 2$ then the action of G_0 on Ω is equivalent to that of $\mathrm{P}\Omega_4^-(q_0)$ on non-degenerate 1-spaces. If $q_0 \in \{2, 3\}$ then $G_0 \cong \mathrm{Alt}(5), \mathrm{Alt}(6)$, respectively, and the action is equivalent to the (large base) action on 2-sets. Hence we can assume that $q \geq 4$, and the result follows from Lemma 3.1.28. If $H \in \mathcal{C}_6$ and $q = 5$ then G is large base; if $q = 7$ then the action of G_0 on Ω is equivalent to that of $\mathrm{PSL}_3(2)$ on 1-spaces, so the result follows from Proposition 3.1.25. Finally if $H \in \mathcal{C}_9$ and $q = 9$ then G is large base. Thus for the remainder of the proof we shall assume that $G_0 \ncong \mathrm{PSL}_2(q)$.

Next, assume that the action of G is not standard. Burness, Guralnick and Saxl show in [25] that if $G_0 \cong \mathrm{Alt}(n)$ then $b(G) \leq 3$. For classical groups, Burness shows in [22, Theorem 1.1] that either $b(G) \leq 4$ or $G = U_6(2).2$, $H = U_4(3).2^2$ and $b(G) = 5$. Looking at the primitive groups of degree at most 15 with classical socle, not isomorphic to $\mathrm{PSL}_2(q)$, we find only standard actions, whilst the degree of the given action of $U_6(2).2$ is 1408, so the result follows for classical G. For the exceptional groups G, it is shown by Burness, Liebeck and Shalev that $b(G) \leq 6$ for all faithful primitive actions; since the smallest degree of a faithful primitive representation of an exceptional group is 65 (see, for example, [48, Table B.2]), the result follows. Finally, Burness, O'Brien and Wilson show in [27] that if G is an almost simple sporadic group, then either $b(G) \leq 5$, or G is one of five specific exceptions. The sporadic groups with faithful primitive actions on at most 32 points are M_{11} on 11 or 12 points, with base size $4 \leq \log 11 + 1$, and the natural actions of M_{12}, M_{23} and M_{24}. Since $b(\mathrm{M}_{12}) = 5 \leq \lceil \log 12 \rceil + 1, b(\mathrm{M}_{23}) = 6 \leq \lceil \log 23 \rceil + 1$, and $b(\mathrm{M}_{24}) = 7 \leq \lceil \log 24 \rceil + 1$, the result holds. The remaining actions, namely the actions of Co_3, Co_2 and $\mathrm{Fi}_{22.2}$, have base size 6 and very large degree.

If $\mathrm{Alt}(\ell) \leq G \leq \mathrm{Sym}(\ell)$, then Ω is an orbit of partitions of $\{1, \ldots, \ell\}$, so $b(G) \leq \log n + 1$ by Theorem 3.1.23. Hence we may assume that G is a classical group in a subspace action.

If $G_0 = \mathrm{PSL}_d(q)$ and the action is on k-dimensional subspaces, then the result follows from Proposition 3.1.25.Otherwise, the orbit is on pairs of subspaces, and the result follows from Proposition 3.1.34.

If $G_0 = \mathrm{PSp}_d(q)$ then we may assume that $d \geq 4$, and $(d, q) \neq (4, 2)$, since $\mathrm{PSp}_4(2)' \cong \mathrm{PSL}_2(9)$. If the action is on k-dimensional subspaces then the result follows from Proposition 3.1.27. If q is even, and the action of G_0 is on the cosets of $\mathrm{GO}_d^{\pm}(q)$, then the result follows from Proposition 3.1.33. If the action is on the cosets of a novelty maximal subspace subgroup, then the result follows from Proposition 3.1.35.

If $G_0 = \mathrm{PSU}_d(q)$, then we may assume that $d \geq 3$. If the action is on k-dimensional subspaces then the result follows from Proposition 3.1.26. Consulting [80, Table 3.5.B] and [20] we see that there are no novelty maximal subspace subgroups.

If $G_0 = \mathrm{P}\Omega_d^{\varepsilon}(q)$ then $d \geq 5$, as $G_0 \ncong \mathrm{PSL}_2(q)$. If $d \leq 6$ and the action is on totally singular subspaces, then the action of G_0 on $G_0 \cap H$ is equivalent to that of $\mathrm{PSp}_4(q)$, $\mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$ on totally singular subspaces. If $d \leq 6$ and the action is on non-degenerate 2-dimensional spaces, then the action of G_0 is equivalent to that of $\mathrm{PSp}_4(q)$, $\mathrm{PSL}_4(q)$ or $\mathrm{PSU}_4(q)$ on their maximal subgroups in Class $\mathcal{C}_2$ or $\mathcal{C}_3$, and $b(G) \leq 3$ by [22, Table 3]. Thus for $5 \leq d \leq 6$ we may assume that the action is on an orbit of non-degenerate 1-spaces, and the result follows from Lemma 3.1.28. If $d \geq 7$ and $H \cap G_0$ is the stabiliser in G_0 of a k-dimensional subspace then the results follow from Proposition 3.1.29 for d even, and Proposition 3.1.30 for d odd. Thus it remains only to consider the case of H a novelty maximal subgroup, and here the result follows from Proposition 3.1.36. □

Diagonal-type

Proposition 3.1.38. *Let G be a primitive diagonal-type group of degree n. Then $b(G) \leq \max\{4, \log(\log n)\}$. In particular, $b(G) \leq \log n$, and Theorem 3.0.2 holds for G.*

Proof. Let $\mathrm{soc}(G) = T^k$, where T is a non abelian simple group and $k \geq 2$. Then $n = |T|^{k-1}$

and it suffices to assume that $G = T^k.(\mathrm{Out}(T) \times \mathrm{Sym}(k))$.

If $k = 2$, then it is shown in [52] that $b(G) \in \{3, 4\}$. Since $n \geq 60$ the result follows. Hence we can assume that $k \geq 3$. It is shown in [52] that

$$b(G) \leq \left\lceil \frac{\log k}{\log |T|} \right\rceil + 2. \tag{3.1.38}$$

If $3 \leq k \leq |T|$ then $b(G) \leq 3$ and the result follows, so assume that $k > |T| \geq 60$. Then $n \geq 60^7$, so $\log \log n > 5$, and hence

$$b(G) \leq \frac{\log k}{\log 60} + 3 \leq \frac{\log \log n}{5} + 3 \leq \log \log n.$$

For the final claim, notice that $n \geq 60$, so $\log n > 4$. □

Product action type

We recall the general set-up for product action type groups. Let $H \leq \mathrm{Sym}(\Gamma)$ be a primitive group of almost simple or diagonal type.

Let $k \geq 2$ be an integer and consider the wreath product $W = H \wr \mathrm{Sym}(k)$. This group has a natural product action on the Cartesian product $\Omega = \Gamma^k$, given by

$$(\gamma_1, \ldots, \gamma_k)^{(h_1,\ldots,h_k)p^{-1}} = (\gamma_{1^p}^{h_{1^p}}, \ldots, \gamma_{k^p}^{h_{k^p}}) \tag{3.1.39}$$

Let $T := \mathrm{soc}(H)$ and $B := \mathrm{soc}(W)$, so $B = T^k$. Following [92], a subgroup $G \leq W$ is primitive product-type group if

(1) $B \leq G$; and

(2) G induces a transitive group $P_G \leq \mathrm{Sym}(n)$ acting by conjugation on the k factors of B.

In particular, note that

$$\mathrm{soc}(G) = T^k \leq G \leq H \wr P_G.$$

Bases for primitive groups of product type were studied by Burness and Seress in [28]. By Lemma 3.1.1 we may suppose that $G = H \wr \mathrm{Sym}(k)$, and this assumption $G = H \wr \mathrm{Sym}(k)$ simplify the general discussion. For the sake of clearness, we repeat some of the arguments of [28] in our simplified general setting.

Lemma 3.1.39. *Let $G = H wr \mathrm{Sym}(k)$, where $H \leq \mathrm{Sym}(\Gamma)$ is a primitive group of almost simple or diagonal type. Let $a := \lceil \log k \rceil$ and $r := \lfloor \log |\Gamma| \rfloor$. Then there exists a collection of points $\{\alpha_1, \ldots, \alpha_{\lceil a/r \rceil}\}$ in Ω with the property that an element $g = (1, \ldots, 1)p \in G$ fixes each α_i if and only if $p = 1$.*

Proof. This is essentially [28, Lemma 3.8]. To see that the value of a is as stated there, notice that it is shown in the proof of [28, Proposition 3.2] that there exists a set of $\lceil \log k \rceil$ 2-partitions of $\{1, \ldots, k\}$, such that the intersection in $\mathrm{Sym}(k)$ of the stabilizers of these partitions is trivial. □

Lemma 3.1.40. *Let $G = H \wr \mathrm{Sym}(k) \leq \mathrm{Sym}(\Omega)$ be primitive of product action type, with $H \leq \mathrm{Sym}(\Gamma)$, and let $m = |\Gamma|$. Then*

$$b(G, \Omega) \leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + b(H, \Gamma).$$

Proof. Let $\{\gamma_1, \dots, \gamma_b\} \subseteq \Gamma$ be a base of minimal size for the action of H on Γ. Let $\alpha'_i := (\gamma_i, \dots, \gamma_i) \in \Gamma^k = \Omega$ for $1 \leq i \leq b$. Let $\{\alpha_1, \dots, \alpha_{\lceil a/r \rceil}\}$ be the set given in Lemma 3.1.39. As noted in [28, Equation (13)], the set

$$\mathcal{B} := \{\alpha_1, \dots, \alpha_{\lceil a/r \rceil}\} \cup \{\alpha'_1, \dots, \alpha'_b\}$$

is a base for G. Indeed, given $g = (h_1, \dots, h_k)\sigma^{-1} \in G_{(\mathcal{B})}$, for $1 \leq i \leq b$

$$\alpha_i'^g = (\gamma_i^{h_{1\sigma}}, \dots, \gamma_i^{h_{k\sigma}}) = (\gamma_i, \dots, \gamma_i)$$

if and only if $\gamma_i^{h_j} = \gamma_i$ for $1 \leq j \leq k$. That is $h_j \in \bigcap_{1 \leq i \leq b} H_{\gamma_i} = 1$, and hence $g = (1, \dots, 1)\sigma^{-1}$. Now, the result follows by the choice of $\{\alpha_1, \dots, \alpha_{\lceil a/r \rceil}\}$ and Lemma 3.1.39. □

Proposition 3.1.41. *Let $G = H \wr \mathrm{Sym}(k) \leq \mathrm{Sym}(\Omega)$ be a primitive permutation group of product-type of degree n, with $H \leq \mathrm{Sym}(\Gamma)$ either an almost simple group in a non-large-base action or a group of diagonal type of degree m. Then $b(G, \Omega) \leq \log n + 1$. In particular, Theorem 3.0.2 holds for G.*

Proof. From Theorem 3.1.37 and Proposition 3.1.38, we see that either $b(H, \Gamma) \leq \lceil \log m \rceil + 1 \leq \log m + 2$, or $H = \mathrm{M}_{24}$ and $m = 24$.

We deal first with $H = \mathrm{M}_{24}$. Here $m = 24$ and $b(H, \Gamma) = 7$, so for all $k \geq 2$, by Lemma 3.1.40,

$$b(G) \leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + b(H, \Gamma) \leq \left(\frac{1 + \log k}{4} + 1 \right) + 7 < k \log(24) + 1.$$

We now consider the general case, and assume first that $k \leq 4$, so that in particular $\lceil \log k \rceil \leq \lfloor \log m \rfloor$. Then by Lemma 3.1.40

$$b(G, \Omega) \leq 1 + b(H, \Gamma) \leq (2 + \log m) + 1 < 2 \log m + 1 \leq k \log m + 1 = \log n + 1.$$

If instead $k \geq 5$, then

$$\begin{aligned} b(G, \Omega) &\leq \left\lceil \frac{\lceil \log k \rceil}{\lfloor \log m \rfloor} \right\rceil + \lceil \log m \rceil + 1 \leq \frac{1 + \log k}{\lfloor \log m \rfloor} + \log m + 3 \leq \left(\frac{1 + \log k}{2} + 2 \right) + \log m + 1 \\ &< (k - 1) + \log m + 1 < k \log m + 1 = \log n + 1. \end{aligned}$$

as required. □

Twisted wreath product

Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive twisted wreath product group with socle T^k, where T is a non-abelian simple group and $k \geq 6$. Note that T^k is a regular normal subgroup of G. Let $P = G_\omega$ be the stabilizer of a point $\omega \in \Omega$. Then $G = T^k P$ is a semidirect product, and the top group P is a transitive subgroup of $\mathrm{Sym}(k)$. In terms of degree, the smallest primitive group of this type arises when $T = \mathrm{Alt}(5)$ and $k = 6$, in which case $|\Omega| = 60^6$.

Proposition 3.1.42. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group of degree n and of twisted wreath product type, then $b(G) \leq \log n + 1$. In particular, Theorem 3.0.2 holds for G.*

Proof. As explained in [140, Section 3.6], we can embed G in a primitive group $L \leq \mathrm{Sym}(\Omega)$ of product-type, where $L = T^2 \wr P = (T^2)^k . P$. To be precise $L = H \wr P$ is of product-type with base group H of diagonal-type. Hence the result follows combining Proposition **??** and Lemma 3.1.1. □

Affine type

Proposition 3.1.43. *Let $G \leq \mathrm{AGL}(V)$ be a primitive permutation group of affine-type, where V is a vector space of dimension n over a field $\mathbb{F}_p$ of prime order p. Then $b(G) \leq \log n + 1$. In particular, Theorem 3.0.2 holds for G.*

Proof. By Lemma 3.1.1 we can assume $G = \mathrm{AGL}(V)$. We claim that $b(G) = b(\mathrm{GL}(V)) + 1$. Let $\mathcal{B}$ be a base of minimal size of $\mathrm{GL}(V)$. For every $w \in \mathcal{B}$, if $v \in V \setminus \{0\}$ then $v + w \neq w$, therefore $b(G) \geq b(\mathrm{GL}(V)) + 1$. Now, G_0 be the stabiliser in G of the trivial vector coincides with $\mathrm{GL}(V)$. Hence $\{0\} \cup \mathcal{B}$ is a base for G and $b(G) = b(\mathrm{GL}(V)) + 1$. Let $\mathcal{B} = \{v_1, \ldots, v_n\}$ be a basis of the vector space V. Then $\mathrm{GL}(V)_{(\mathcal{B})} = 1$ and $b(\mathrm{GL}(V)) \leq n$. Now, we show that $\mathrm{GL}(V)_{(\mathcal{A})}$ is nontrivial for every $\mathcal{A} \subset V$ of size $n-1$. Let $g \in \mathrm{GL}(V)$. If g stabilizes w, then $zg = z$, for every $z \in \langle w \rangle$. So, without loss of generality, we can assume that G stabilizes pointwise $\{v_1, \ldots, v_{n-1}\}$. The map fixing pointwise $\{v_1, \ldots, v_{n-1}\}$ and mapping v_n in $v_n + v_1$ is a nontrivial element of $\mathrm{GL}(V)$, hence $b(\mathrm{GL}(V)) \geq n$, and the statement follows. □

3.2 A polynomial bound for the number of maximal systems of imprimitivity of a finite transitive permutation group

3.2.1 Preliminaries

We need some basic terminology, which we borrow from [141, Sections 4.3 and 4.4].

Let κ be a positive integer and let A be a direct product $S_1 \times \cdots \times S_\kappa$, where the S_i are pairwise isomorphic non-abelian simple groups. We denote by $\pi_i : A \to S_i$ the natural projection onto S_i. A subgroup X of A is said to be a *strip*, if $X \neq 1$ and, for each $i \in \{1, \ldots, \kappa\}$, either $X \cap \mathrm{Ker}(\pi_i) = 1$ or $\pi_i(X) = 1$. The support of the strip X is the set $\{i \in \{1, \ldots, \kappa\} \mid \pi_i(X) \neq 1\}$. The strip X is said to be *full* if $\pi_i(X) = S_i$, for all i in the support of X. Two strips X and Y are *disjoint* if their supports are disjoint. A subgroup X of A is said to be a *subdirect* subgroup if $\pi_i(X) = S_i$, for each $i \in \{1, \ldots, \kappa\}$.

Scott's lemma (see for instance [141, Theorem 4.16]) shows (among other things) that if X is a subdirect subgroup of A, then X is a direct product of pairwise disjoint full strips of A.

Lemma 3.2.1. *Let $L_{k'}$ be a crown-based power of L of size k' having non-abelian socle $N^{k'}$ and let H' be a core-free subgroup of $L_{k'}$ contained in $N^{k'}$. Then $|N^{k'} : H'| \geq 5^{k'}$.*

Proof. We argue by induction on k'. If $k' = 1$, then the result is clear because $N^{k'} = N$ has no proper subgroups having index less then 5. Suppose that $k' \geq 2$ and write $N := N_1 \times \cdots \times N_{k'}$, where $N_1, \ldots, N_{k'}$ are the minimal normal subgroups of $L_{k'}$ contained in $N^{k'}$. For each $i \in \{1, \ldots, k'\}$, we denote by $\pi_i : N^{k'} \to N_i$ the natural projection onto N_i.

Suppose that there exists $i \in \{1, \ldots, k'\}$ with $\pi_i(H') < N_i$. Then, $N_i H'/N_i$ is a core-free subgroup of $L_{k'}/N_i \cong L_{k'-1}$ and is contained in $N^{k'}/N_i$. Therefore, by induction, $|N^{k'} : H'N_i| = |N^{k'}/N_i : H'N_i/N_i| \geq 5^{k'-1}$. Furthermore, $|H'N_i : H'| = |N_i : H' \cap N_i| \geq 5$ because N_i has no proper subgroups having index less then 5. Therefore, $|N^{k'} : H'| \geq 5^{k'}$.

Suppose that, for every $i \in \{1, \ldots, k'\}$, $\pi_i(H') = N_i$. Since N is non-abelian, we may write $N_i = S_{i,1} \times \cdots \times S_{i,\ell}$, for some pair-wise isomorphic non-abelian simple groups $S_{i,j}$ of cardinality s. For each $i \in \{1, \ldots, k'\}$ and $j \in \{1, \ldots, \ell\}$, we denote by $\pi_{i,j} : N^{k'} \to S_{i,j}$ the natural projection onto $S_{i,j}$. Since $\pi_i(H') = N_i$, we deduce $\pi_{i,j}(H') = S_{i,j}$, for every $i \in \{1, \ldots, k'\}$ and $j \in \{1, \ldots, \ell\}$. In particular, H' is a subdirect subgroup of $S_{1,1} \times \cdots \times S_{k',\ell}$ and hence (by Scott's lemma) H' is a direct product of pairwise disjoint full strips. Since no N_i is contained in H', there exist two distinct indices $i_1, i_2 \in \{1, \ldots, k'\}$ and $j_1, j_2 \in \{1, \ldots, \ell\}$ such that (i_1, j_1) and (i_2, j_2) are involved in the same full strip of H'. If we now consider the projection $\pi_{i_1,i_2} : N^{k'} \to N_{i_1} \times N_{i_2}$, we obtain $|N_{i_1} \times N_{i_2} : \pi_{i_1,i_2}(H')| \geq s \geq 60 \geq 5^2$. The

inductive hypothesis applied to $\mathrm{Ker}(\pi_{i_1,i_2}) \cap H'$ yields $|\mathrm{Ker}(\pi_{i_1,i_2}) : \mathrm{Ker}(\pi_{i_1,i_2}) \cap H'| \geq 5^{k'-2}$ and hence $|N^{k'} : H'| \geq 5^{k'}$. □

The following Theorem 3.2.2 is an improvement of [115, Corollary 2].

Theorem 3.2.2. [95, Theorem 1.4] *There exists a constant c such that every finite group has at most $cn^{3/2}$ core-free maximal subgroups of index n.*

We warn the reader that the statement of Theorem 3.2.2 is slightly different from that of Theorem 1.4 in [95]: to get Theorem 3.2.2 one should take into account Theorem 1.4 in [95] and the remark following its statement.

3.2.2 Proofs of Theorems 3.0.3 and 3.0.4

In this section we prove Theorems 3.0.3 and 3.0.4. Note that in the proofs of Theorem 3.0.3 and 3.0.4, we use without mention Lemma 1.2.1. Our proofs are inspired from some ideas developed in [42]. Moreover, our proofs have some similarities and hence we start by deducing some general facts holding for both.

We start by defining the universal constant a. Observe that the series $\sum_{u=1}^{\infty} u^{-3/2}$ converges. We write

$$a' := \sum_{u=1}^{\infty} \frac{1}{u^{3/2}}.$$

Let c be the universal constant arising from Theorem 3.2.2. We define

$$a := \frac{11ca'}{1 - 1/2^{3/2}}.$$

Recall that $\max(H, G)$ is the number of maximal subgroups of G containing H. For the proofs of Theorems 3.0.3 and 3.0.4 we argue by induction on $|G : H| + |G|$. The case $|G : H| = 1$ for the proof of Theorem 3.0.3 is clear because $\max(H, G) = 0$. Similarly, the case that H is maximal in G for the proof of Theorem 3.0.4 is clear because $\max(H, G) = 1$. In particular, for the proof of Theorem 3.0.3, we suppose $|G : H| > 1$ and, for the proof of Theorem 3.0.4, we suppose that H is not maximal in G.

Consider

$$\tilde{H} := \bigcap_{\substack{H \leq M < G \\ M \text{ max. in } G}} M.$$

Observe that $\max(H, G) = \max(\tilde{H}, G)$. In particular, when $H < \tilde{H}$, we have $|G : \tilde{H}| < |G : H|$ and hence, by induction, we have $\max(H, G) = \max(\tilde{H}, G) \leq a|G : \tilde{H}|^{3/2} < a|G : H|^{3/2}$. Moreover, when G is soluble, we have $\max(H, G) = \max(\tilde{H}, G) \leq |G : \tilde{H}| - 1 < |G : H| - 1$. Therefore, we may suppose $H = \tilde{H}$, that is,

$$H \text{ is an intersection of maximal subgroups of } G. \tag{3.2.1}$$

Suppose that H contains a non-identity normal subgroup N of G. Since $\max(H, G) = \max(H/N, G/N)$ and $|G/N| < |G|$, by induction, we have $\max(H, G) = \max(H/N, G/N) \leq a|G/N : H/N|^{3/2} = a|G : H|^{3/2}$. Moreover, when G is soluble, we have $\max(H, G) = \max(H/N, G/N) \leq |G/N : G/N| - 1 = |G : H| - 1$. Therefore, we may suppose

$$\mathrm{core}_G(H) = 1. \tag{3.2.2}$$

Let F be the Frattini subgroup of G. From (3.2.1), we have $F \leq H$ and hence, from (3.2.2), $F = 1$. In particular, we may now apply Lemma 1.2.3 to the group G.

Choose I, R and D as in Lemma 1.2.3. By (3.2.1), we may write

$$H = X_1 \cap \cdots \cap X_\rho \cap Y_1 \cap \cdots \cap Y_\sigma,$$

where $X_1, \ldots, X_\rho$ are the maximal subgroups of G not containing D and $Y_1, \ldots, Y_\sigma$ are the maximal subgroups of G containing D. We define

$$X := X_1 \cap \cdots \cap X_\rho \text{ and } Y := Y_1 \cap \cdots \cap Y_\sigma.$$

Thus $H = X \cap Y$.

For every $i \in \{1, \ldots, \rho\}$, since $D \nleq X_i$, we have $G = DX_i$ and hence Lemma 1.2.4 (applied with $K := X_i$) yields $R \leq X_i$. In particular,

$$R \leq X. \tag{3.2.3}$$

Since $R = R_G(A)$ for some chief factor A of G, Section 1.2 yields

$$G/R \cong L_k,$$

for some monolithic primitive group L and for some positive integer k. We let N denote the minimal normal subgroup (a.k.a. the socle) of L. From the definition of I and R, we have $I/R = \mathrm{soc}(G/R) \cong \mathrm{soc}(L_k) = N^k$. Finally, let $T := X \cap I$. In particular,

$$\frac{T}{R} = \frac{X}{R} \cap \frac{I}{R}.$$

We have

$$H \cap D = (X \cap Y) \cap D = X \cap (Y \cap D) = X \cap D = X \cap (I \cap D) = (X \cap I) \cap D = T \cap D.$$

It follows

$$|G : HD| = \frac{|G : H|}{|HD : H|} = \frac{|G : H|}{|D : H \cap D|} = \frac{|G : H|}{|D : T \cap D|}.$$

If $D \leq T$, then $D \leq X$ and hence $D \leq X \cap Y = H$ because $D \leq Y$. However this is a contradiction because $D \neq 1$ and hence, from (3.2.2), $D \nleq H$. Therefore $D \nleq T$ and $|D : T \cap D| > 1$.

Applying our inductive hypothesis, we obtain

$$\begin{aligned} \sigma &= \max(HD/D, G/D) \leq a|G/D : HD/D|^{3/2} = a|G : HD|^{3/2} \\ &= a\left(\frac{|G : H|}{|D : D \cap T|}\right)^{3/2} \leq \frac{a}{2^{3/2}}|G : H|^{3/2}. \end{aligned} \tag{3.2.4}$$

Moreover, when G is soluble and HD is a proper subgroup of G, we obtain

$$\begin{aligned} \sigma &= \max(HD/D, G/D) \leq |G/D : HD/D| - 1 = |G : HD| - 1 \\ &= \frac{|G : H|}{|D : D \cap T|} - 1 \leq \frac{|G : H|}{2} - 1. \end{aligned} \tag{3.2.5}$$

(Observe that, when G is soluble and $G = HD$, we have $\sigma = 0$ and hence the inequality $\sigma \leq |G : H|/2 - 1$ is valid also in this degenerate case.)

From (3.2.3), we deduce $\rho \leq \max(HR, G)$. If $R \nleq H$, then $|G : HR| < |G : H|$ and hence, applying our inductive hypothesis, we obtain

$$\rho \leq \max(HR, G) \leq a|G : HR|^{3/2} = a\left(\frac{|G : H|}{|HR : H|}\right)^{3/2} \leq \frac{a}{2^{3/2}}|G : H|^{3/2}. \tag{3.2.6}$$

Moreover, when G is soluble and HR is a proper subgroup of G, we obtain

$$\rho \leq \max(HR, G) \leq |G : HR| - 1 = \frac{|G : H|}{|HR : H|} - 1 \leq \frac{|G : H|}{2} - 1. \tag{3.2.7}$$

(As above, when G is soluble and $G = HR$, we have $\rho = 0$ and hence the inequality $\rho \leq |G : H|/2 - 1$ is valid also in this degenerate case.)

Now, from (3.2.4) and (3.2.6), we have

$$\max(H, G) = \sigma + \rho \leq \frac{2a}{2^{3/2}} \cdot |G : H|^{3/2} < a|G : H|^{3/2}.$$

Similarly, when G is soluble, from (3.2.5) and (3.2.7), we have

$$\max(H, G) = \sigma + \rho \leq \frac{|G : H|}{2} - 1 + \frac{|G : H|}{2} - 1 < |G : H| - 1.$$

In particular, for the rest of the proof, we may assume that $R \leq H$. Now, (3.2.2) yields $R = 1$ and hence $G \cong L_k$ and $D = I$. Therefore, we may identify G with L_k and D with N^k.

Set

$$\mathcal{C} := \{\mathrm{core}_G(X_i) \mid i \in \{1, \ldots, \rho\}\}$$

and, for every $C \in \mathcal{C}$, set

$$\mathcal{M}_C := \{X_i \mid i \in \{1, \ldots, \rho\}, C = \mathrm{core}_G(X_i)\}.$$

For the rest of our argument for proving Theorems 3.0.3 and 3.0.4, we prefer to keep the proofs separate.

Proof of Theorem 3.0.3. In this proof, we distinguish two cases.

Case 1: Suppose that N is non-abelian.

Since N is non-abelian, the group $G = L_k$ has exactly k minimal normal subgroups. We denote by $N_1, \ldots, N_k$ the minimal normal subgroups of G. In particular, $I = N^k = N_1 \times N_2 \times \cdots \times N_k$.

First, we claim that, for every $i \in \{1, \ldots, \rho\}$, there exist $x, y \in \{1, \ldots, k\}$ such that $N_\ell \leq X_i$, for every $\ell \in \{1, \ldots, k\} \setminus \{x, y\}$, that is, X_i contains all but possibly at most two minimal normal subgroups of G.

We argue by induction on k. The statement is clearly true when $k \leq 2$. Suppose then $k \geq 3$ and let $C := \mathrm{core}_G(X_i)$. If $C = 1$, then X_i is a maximal core-free subgroup of G and hence the action of G on the right cosets of X_i gives rise to a faithful primitive permutation representation. Since a primitive permutation group has at most two minimal normal subgroups [32, Theorem 4.4] and since G has exactly k minimal normal subgroups, we deduce that $k \leq 2$, which is a contradiction. Therefore $C \neq 1$.

Since $N_1, \ldots, N_k$ are the minimal normal subgroups of L_k, we deduce that there exists $\ell \in \{1, \ldots, k\}$ with $N_\ell \leq C$. Now, the proof of the claim follows applying the inductive hypothesis to $G/N_\ell \cong L_{k-1}$ and to its maximal subgroup X_i/N_ℓ.

The previous claim shows that, for every $C \in \mathcal{C}$, C contains all but possibly at most two minimal normal subgroups of $N^k = I$. Therefore,

$$|\mathcal{C}| \leq k^2.$$

Let $C \in \mathcal{C}$ and let $M \in \mathcal{M}_C$. The reader might find it useful to see Figure 3.1, where we have drawn a fragment of the subgroup lattice of G relevant to our argument.

Let k' be the number of minimal normal subgroups of G contained in M. In particular, $I \cap M \cong N^{k'}$. Observe that $I \cap H$ is contained in $I \cap M$ and is core-free in G. Applying

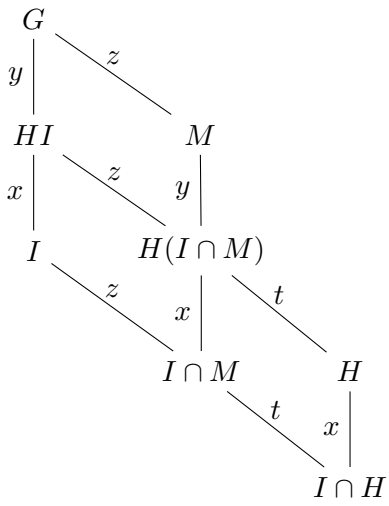

Figure 3.1: Subgroup lattice for G

Lemma 3.2.1 (with H' replaced by $I \cap H$ in a crowned-based group isomorphic to $L_{k'}$), we get $|I \cap M : I \cap H| \geq 5^{k'}$. As $k' \geq k-2$, we deduce $t \geq 5^{k-2}$.

Now, M/C is a core-free maximal subgroup of G/C. From Theorem 3.2.2, when $C = \mathrm{core}_G(M)$ and $z = |G : C|$ are fixed, we have at most $cz^{3/2}$ choices for M. As $t \geq 5^{k-2}$, we have $z \leq |G : H|/5^{k-2}$. Thus

$$\begin{aligned}\rho = \sum_{C \in \mathcal{C}} |\mathcal{M}_C| &\leq \sum_{C \in \mathcal{C}} \sum_{\substack{z||G:H| \\ z \leq |G:H|/5^{k-2}}} cz^{3/2} \leq ck^2 \sum_{\substack{z||G:H| \\ z \leq |G:H|/5^{k-2}}} z^{3/2} \\ &= ck^2 \left(\frac{|G:H|}{5^{k-2}}\right)^{3/2} \sum_{\substack{z||G:H| \\ z \leq |G:H|/5^{k-2}}} \left(\frac{5^{k-2}z}{|G:H|}\right)^{3/2}.\end{aligned}$$

Therefore,

$$\sum_{\substack{z||G:H| \\ z \leq |G:H|/5^{k-2}}} \left(\frac{5^{k-2}z}{|G:H|}\right)^{3/2} \leq \sum_{u=1}^{\infty} \frac{1}{u^{3/2}} = a'.$$

Finally, it is easy to verify that, for every k, $k^2/5^{3(k-2)/2} \leq 11$. Summing up,

$$\rho \leq 11ca'|G:H|^{3/2}. \tag{3.2.8}$$

From (3.2.4), (3.2.8) and from the definition of a, we have

$$\max(H, G) = \sigma + \rho \leq \frac{a}{2^{3/2}}|G:H|^{3/2} + 11ca'|G:H|^{3/2} = a|G:H|^{3/2}.$$

Case 2: Suppose that N is abelian.

As N is abelian, the action of L by conjugation on N endows N with the structure of an L-module. Since L is primitive, N is irreducible. Set $q := |\mathrm{End}_L(N)|$. Now, N is a vector space over the finite field $\mathbb{F}_q$ with q elements, and hence $|N| = q^{k'}$, for some positive integer k'.

Let $C \in \mathcal{C}$ and let $M \in \mathcal{M}_C$. By Lemma 1.2.1, $C \leq I$. Now, the action of G/C on the right cosets of M/C is a primitive permutation group with point stabilizer M/C. Observe

that in this primitive action, I/C is the socle of G/C. In particular, G/C acts irreducibly as a linear group on I/C and hence C is a maximal L-submodule of I. Since I is the direct sum of k pairwise isomorphic irreducible L-modules, we deduce that we have at most $(q^k-1)/(q-1)$ choices for C. Moreover, $|G:M| = |G/C : M/C| = |N| = q^{k'}$. From Theorem 3.2.2, when C is fixed, we have at most $c|G:M|^{3/2} = c(q^{k'})^{3/2}$ choices for $M \in \mathcal{M}_C$. This yields

$$\rho \leq |\mathcal{C}| \cdot \max_{C\in\mathcal{C}} |\mathcal{M}_C| \leq \frac{q^k-1}{q-1} \cdot cq^{3k'/2} < cq^{k+3k'/2}. \tag{3.2.9}$$

As we have observed above, $M \cap I = C$ is an L-submodule of G. Since an intersection of L-submodules is an L-submodule, we deduce that

$$H \cap I = (X_1 \cap \cdots \cap X_\rho) \cap I$$

is an L-submodule of G and hence $H \cap I \trianglelefteq G$. Since H is core-free in G, we deduce $H \cap I = 1$ and hence $|I| = |N|^k = q^{kk'}$ divides $|G:H|$. In particular, $|G:H| \geq q^{kk'}$. Therefore, from (3.2.9), we obtain

$$\rho \leq c|G:H|^{\frac{k+3k'/2}{kk'}}.$$

When $k \neq 1$ or when $(k,k') \neq (2,1)$, we have $\frac{k+3k'/2}{kk'} \leq \frac{3}{2}$. When $k=1$, by refining (3.2.9), we obtain the sharper bound $\rho \leq cq^{3k'/2} \leq c|G:H|^{3/2}$. When $(k,k') = (2,1)$, we may again refine (3.2.9): $\rho \leq c(q+1)q^{3/2} \leq c\cdot 2q\cdot q^{3/2} = 2cq^{5/2} \leq 2c|G:H|^{5/4} \leq 2c|G:H|^{3/2}$. Summing up, in all cases we have

$$\rho \leq 2c|G:H|^{3/2}. \tag{3.2.10}$$

From (3.2.4) and (3.2.10), we have

$$\max(H,G) = \sigma + \rho \leq \frac{a}{2^{3/2}}|G:H|^{3/2} + 2c|G:H|^{3/2} < a|G:H|^{3/2},$$

as desired. □

The rest of the proof of Theorem 3.0.4 follows the same idea as in Case 2 above, but taking in account that the whole group G is soluble.

Proof of Theorem 3.0.4. Since $G = L_k$ and $I = N^k$, we may write $G = I \rtimes K$, where K is a complement of N in L. As in the proof of Theorem 3.0.3 for the case that N is abelian, we have that the action of L by conjugation on N endows N with the structure of an L-module. Since L is primitive, N is irreducible. Set $q := |\mathrm{End}_L(N)|$. Now, N is a vector space over the finite field $\mathbb{F}_q$ with q elements, and hence $|N| = q^{k'}$, for some positive integer k'.

Let $C \in \mathcal{C}$ and let $M \in \mathcal{M}_C$. As we have observed above (for the proof of Case 2), $M \cap I = C$ is a maximal L-submodule of G, $H \cap I = 1$ and $|I| = |N|^k = q^{kk'}$ divides $|G:H|$. In particular, $|G:H| = \ell q^{kk'}$, for some positive integer ℓ.

Since G is soluble and since M is a maximal subgroup of G supplementing I, we have $M = C \rtimes K^x$, for some maximal L-submodule C of I and some $x \in I$. Arguing as in the proof of Theorem 3.0.3 for the case that N is abelian, we deduce that we have at most $(q^k-1)/(q-1)$ choices for C. Moreover, we have at most $|I/C| = |G:M| = |N| = q^{k'}$ choices for x. This yields

$$\rho \leq \frac{q^k-1}{q-1} q^{k'}. \tag{3.2.11}$$

Now, (3.2.5) gives $\sigma \leq |G:H|/|D:D\cap T| - 1$: recall that $D = I = N^k$ and $D \cap T = D \cap H = I \cap H = 1$. Thus $\sigma \leq |G:H|/|D| - 1 = |G:H|/q^{kk'} - 1 = \ell - 1$. Therefore,

$$\max(H,G) = \sigma + \rho \leq \ell - 1 + \frac{q^k-1}{q-1} q^{k'}. \tag{3.2.12}$$

When $\ell \geq 2$, a computation shows that the right-hand side of (3.2.12) is less than or equal to $\ell q^{kk'} - 1 = |G : H| - 1$. In particular, we may suppose that $\ell = 1$. In this case, $|G : H| = q^{kk'} = |I|$ and hence $G = IH = I \rtimes H$. Moreover, $\sigma = 0$. Since H is not a maximal subgroup of G (recall the base case for our inductive argument), $k \geq 2$.

Assume also $k' = 1$. Since $|\mathrm{End}_L(N)| = q = |N|$, we deduce that L/N is isomorphic to a subgroup of the multiplicative group of the field $\mathbb{F}_q$ and hence $|L : N|$ is relatively prime to q. Therefore $|G : I|$ is relatively prime to q and hence so is $|H|$. Therefore, replacing H by a suitable G-conjugate, we may suppose that $K = H$. Using this information, we may now refine our earlier argument bounding ρ. Let $C \in \mathcal{C}$ and let $M \in \mathcal{M}_C$. Since $G = I \rtimes H$ is soluble, M is a maximal subgroup of G supplementing I and $H \leq M$, we have $M = C \rtimes H$, for some maximal L-submodule C of I. We deduce that we have at most $(q^k - 1)/(q - 1)$ choices for C and hence we have at most $(q^k - 1)/(q - 1)$ choices for M. This yields

$$\max(H, G) = \sigma + \rho = \rho \leq \frac{q^k - 1}{q - 1} \leq q^k - 1 = |G : H| - 1,$$

and the result is proved in this case.

Assume $k' \geq 2$. A computation (using $\ell = 1$ and $k, k' \geq 2$) shows that the right-hand side of (3.2.12) is less than or equal to $q^{kk'} - 1 = |G : H| - 1$. □

3.3 Boolean lattices in finite alternating and symmetric groups

3.3.1 Notation, Terminology and basic facts

Since we need fundamental results from the work of Aschbacher [5, 6], we follow the notation and the terminology therein. We let G be the finite alternating group $\mathrm{Alt}(\Omega)$ or the finite symmetric group $\mathrm{Sym}(\Omega)$, where Ω is a finite set of cardinality $n \in \mathbb{N}$. Given a subgroup H of G, we write

$$\mathcal{O}_G(H) := \{K \mid H \leq K \leq G\}$$

for the set of subgroups of G containing H. We let

$$\mathcal{O}_G(H)' := \mathcal{O}_G(H) \setminus \{H, G\},$$

that is, $\mathcal{O}_G(H)'$ consists of the lattice $\mathcal{O}_G(H)$ with its minimum and its maximum elements removed. Given a group X, we denote by $\mathbf{F}^*(X)$ the *generalized Fitting* subgroup of X. Observe that, when X is a primitive subgroup of $\mathrm{Sym}(\Omega)$, $\mathbf{F}^*(X)$ coincides with the *socle* of X. We write

$$\mathcal{O}_G(H)'' := \{M \in \mathcal{O}_G(H) \mid \mathbf{F}^*(G) \not\leq M\}$$

and we denote by

$$\mathcal{M}_G(H) \text{ the set of maximal members of } \mathcal{O}_G(H)''.$$

We start by familiarizing the reader with this terminology.

- When $G = \mathrm{Alt}(\Omega)$, $\mathbf{F}^*(G) = G$ and hence $\mathcal{O}_G(H)''$ is simply $\mathcal{O}_G(H)$ with its maximum element $G = \mathrm{Alt}(\Omega)$ removed. Therefore $\mathcal{M}_G(H)$ consists of the maximal subgroups of $G = \mathrm{Alt}(\Omega)$ containing H.

- When $G = \mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega) \not\leq H$, $\mathcal{O}_G(H)''$ is obtained from $\mathcal{O}_G(H)$ by removing $G = \mathrm{Sym}(\Omega)$ only, because if $M \in \mathcal{O}_G(H)$ and $\mathrm{Alt}(\Omega) = \mathbf{F}^*(G) \leq M$, then $\mathrm{Sym}(\Omega) = H\mathbf{F}^*(G) \leq M$ and $M = \mathrm{Sym}(\Omega)$. Therefore, also in this case $\mathcal{M}_G(H)$ consists simply of the maximal subgroups of $G = \mathrm{Sym}(\Omega)$ containing H.

- When $G = \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Alt}(\Omega)$, $\mathcal{O}_G(H)''$ is obtained from $\mathcal{O}_G(H)$ by removing $\mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$. Therefore $\mathcal{M}_G(H)$ consists of two types of subgroups: the maximal subgroups of $G = \mathrm{Sym}(\Omega)$ containing H and the maximal subgroups M of $\mathrm{Alt}(\Omega)$ containing H and that are not contained in any other maximal subgroup of $\mathrm{Sym}(\Omega)$ other then $\mathrm{Alt}(\Omega)$. For instance, when $H := \mathrm{M}_{12}$ in its transitive action of degree 12, we have $H \leq \mathrm{Alt}(12)$, $\mathcal{O}_{\mathrm{Sym}(12)}(\mathrm{M}_{12}) = \{\mathrm{M}_{12}, \mathrm{Alt}(12), \mathrm{Sym}(12)\}$, $\mathcal{O}_{\mathrm{Sym}(12)}(H)' = \{\mathrm{Alt}(12)\}$, $\mathcal{O}_{\mathrm{Sym}(12)}(\mathrm{M}_{12})'' = \{\mathrm{M}_{12}\}$ and $\mathcal{M}_{\mathrm{Sym}(12)}(\mathrm{M}_{12}) = \{\mathrm{M}_{12}\}$.

Some of the material that follows can be traced back to [5, 6] or [93, 140]. However, we prefer to repeat it here because it helps to set some more notation and terminology. Using the action of $\mathrm{Sym}(\Omega)$ on the domain Ω, we can divide the subgroups X of $\mathrm{Sym}(\Omega)$ into three classes:

Intransitive X is *intransitive* on Ω,

Imprimitive X is *imprimitive* on Ω, that is, X is transitive but it is not primitive on Ω,

Primitive X is *primitive* on Ω.

In particular, every maximal subgroup M of G can be referred to as intransitive, imprimitive or primitive, according to the division above.

In what follows we need detailed information on the overgroups of a primitive subgroup of G. This information was obtained independently by Aschbacher [5, 6] and Liebeck, Praeger and Saxl [93, 140]. Both investigations are important in what follows.

Intransitive subgroups

A maximal subgroup M of G is intransitive if and only if it is the stabilizer in G of a subset Γ of Ω with $1 \leq |\Gamma| < |\Omega|/2$ (see for example [93]), that is,

$$M = G \cap (\mathrm{Sym}(\Gamma) \times \mathrm{Sym}(\Omega \setminus \Gamma)).$$

Following [5, 6], we let $\mathbf{N}_G(\Gamma)$ denote the setwise stabilizer of Γ in G, that is,

$$\mathbf{N}_G(\Gamma) := \{g \in G \mid \gamma^g \in \Gamma, \forall \gamma \in \Gamma\}.$$

More generally, given a subgroup H of G, we let $\mathbf{N}_H(\Gamma) = \mathbf{N}_G(\Gamma) \cap H$ denote the setwise stabilizer of Γ in H.

The case $|\Gamma| = |\Omega|/2$ is special because $\mathbf{N}_G(\Gamma)$ is not maximal. Indeed, $\mathbf{N}_G(\Gamma)$ is a subgroup of the stabilizer in G of the partition $\{\Gamma, \Omega \setminus \Gamma\}$. This is an imprimitive group and we analyze the imprimitive groups later.

Summing up, we have the following fact.

Fact 3.3.1. Let Γ be a subset of Ω with $1 \leq |\Gamma| < |\Omega|/2$. Then, the intransitive subgroup $\mathbf{N}_G(\Gamma)$ of G is a maximal subgroup of G. Moreover, every intransitive maximal subgroup of G is of this form.

Regular partitions and imprimitive subgroups

The collection of all partitions of Ω is a poset, with the reverse refinement order: given two partitions Σ_1 and Σ_2 of Ω, we say that $\Sigma_1 \leq \Sigma_2$ if Σ_2 is a *refinement* of Σ_1, that is, every element in Σ_1 is a union of elements in Σ_2. For instance, when $\Omega := \{1, 2, 3, 4\}$, $\Sigma_1 := \{\{1, 3, 4\}, \{2\}\}$ and $\Sigma_2 := \{\{1\}, \{2\}, \{3, 4\}\}$, we have $\Sigma_1 \leq \Sigma_2$.

A partition Σ of Ω is said to be *regular* or *uniform* if all parts in Σ have the same cardinality. Following [5, 6], we say that the partition Σ is an (a, b)-*regular partition* if Σ consists of b parts each having cardinality a. In particular, $n = |\Omega| = ab$.

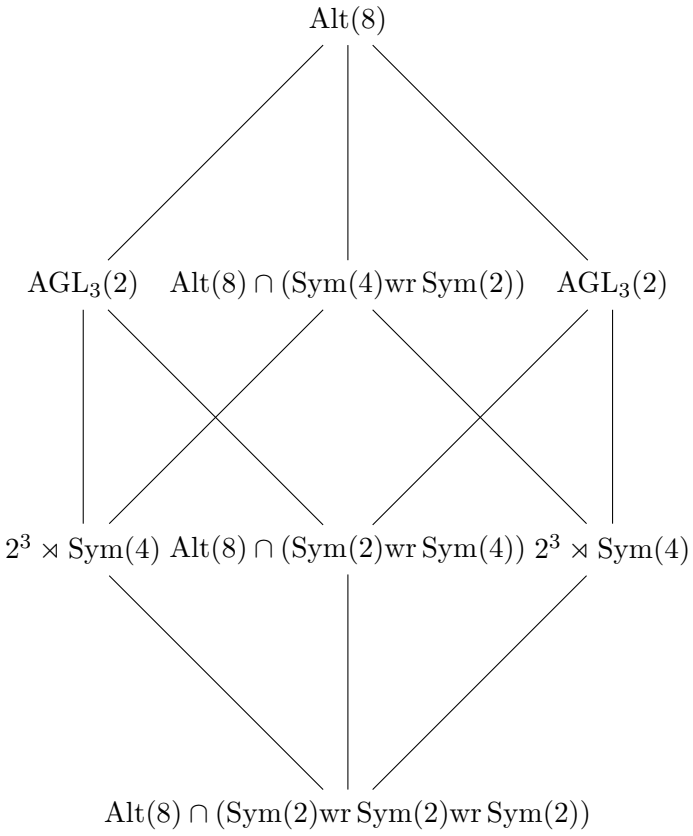

Figure 3.2: The Boolean lattice of largest cardinality in Alt(8)

A partition Σ of Ω is said to be *trivial* if Σ equals the universal relation $\Sigma = \{\Omega\}$ or if Σ equals the equality relation $\Sigma = \{\{\omega\} \mid \omega \in \Omega\}$.

We let

$$\mathbf{N}_G(\Sigma) := \{g \in G \mid \Gamma^g \in \Sigma, \forall\, \Gamma \in \Sigma\}$$

denote the stabilizer in G of the partition Σ. Moreover, when H is a subgroup of G, we write $\mathbf{N}_H(\Sigma) := \mathbf{N}_G(\Gamma) \cap H$.

Let M be a maximal subgroup of G. If M is imprimitive, then M is the stabilizer in G of a non-trivial regular partition. Therefore, there exists an (a, b)-regular partition Σ with $a, b \geq 2$ and with $M = \mathbf{N}_G(\Sigma)$. From [93, 140], we see that when $G = \mathrm{Sym}(\Omega)$ the converse is also true. That is, for every non-trivial (a, b)-regular partition Σ, the subgroup $\mathbf{N}_G(\Sigma)$ is a maximal subgroup of $\mathrm{Sym}(\Omega)$. When $G = \mathrm{Alt}(\Omega)$, the converse is not quite true in general. We summarize what we need in the following fact.

Fact 3.3.2. Let Σ be a non-trivial regular partition of Ω. Except when $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$ and Σ is a $(2, 4)$-regular partition, the imprimitive subgroup $\mathbf{N}_G(\Sigma)$ of G is a maximal subgroup of G.

The case $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$ and Σ is a $(2, 4)$-regular partition is a genuine exception here. Indeed, $\mathbf{N}_G(\Sigma) < \mathrm{AGL}_3(2) < \mathrm{Alt}(\Omega)$, where $\mathrm{AGL}_3(2)$ is the affine general linear group of degree $2^3 = 8$. (This was already observed in [93].) The case $G = \mathrm{Alt}(n)$ and $n = 8$ is combinatorially very interesting: the largest Boolean lattice in $\mathrm{Alt}(8)$ has rank 3 and it is drawn in Figure 3.2.

Regular product structures and primitive subgroups

For what follows it is convenient to use the version of O'Nan-Scott Theorem presented in [140] (see Section 1.5). It follows from the results in [93, 140] that, if M is a maximal subgroup of G and M is primitive, then M has O'Nan-Scott type HA, AS, SD or PA.

Since an overgroup of a primitive group is still primitive, the analogue of Facts 3.3.1 and 3.3.2 is obvious.

Fact 3.3.3. A primitive subgroup M of G is maximal if and only if M is maximal among the primitive subgroups of G.

We recall the definition of a *regular product structure* on Ω from [6, Section 2]. Let m and k be integers with $m \geq 5$ and $k \geq 2$. There are two natural ways to give this definition. First, a regular (m,k)-product structure on Ω is a bijection $f : \Omega \to \Gamma^I$, where $I := \{1,\dots,k\}$ and Γ is an m-set. The function f consists of a family of functions $(f_i : \Omega \to \Gamma \mid i \in I)$ where $f(\omega) = (f_1(\omega),\dots,f_k(\omega))$, for each $\omega \in \Omega$. There is a more intrinsic way to define it. Let $\mathcal{F} := \{\Omega_i \mid i \in I\}$ be a set of partitions Ω_i of Ω into m blocks of size m^{k-1}, let $[\omega]_i$ be the block of Ω_i containing the point ω, and let $\mathcal{F}(\omega) := \{[\omega]_i \mid i \in I\}$. The set $\mathcal{F}$ is a product structure if, for each pair of distinct points $\omega, \omega' \in \Omega$, we have $\mathcal{F}(\omega) \neq \mathcal{F}(\omega')$. Clearly the two definitions are equivalent. Indeed, given a function $f : \Omega \to \Gamma^I$, we let $\mathcal{F}(f)$ be the set of partitions of Ω defined by f, where the i^{th} partition $\Omega_i := \{f_i^{-1}(\gamma) \mid \gamma \in \Gamma\}$ consists of the the fibers of f_i. The product structure $\mathcal{F}$ can also be regarded as a chamber system in the sense of Tits [158].

Following [5], we let $\mathbf{N}_G(\mathcal{F})$ denote the stabilizer of a regular (m,k)-product structure $\mathcal{F} = \{\Omega_1,\dots,\Omega_k\}$ in G, that is,

$$\mathbf{N}_G(\mathcal{F}) := \{g \in G \mid \Omega_i^g \in \mathcal{F}, \forall i \in \{1,\dots,k\}\}.$$

More generally, given a subgroup H of G, we let $\mathbf{N}_H(\mathcal{F}) := \mathbf{N}_G(\mathcal{F}) \cap H$ denote the stabilizer of Γ in H. Clearly,

$$\mathbf{N}_{\mathrm{Sym}(\Omega)}(\mathcal{F}) \cong \mathrm{Sym}(m) \mathrm{wr}\, \mathrm{Sym}(k),$$

where $\mathrm{Sym}(m)\mathrm{wr}\,\mathrm{Sym}(k)$ is endowed of its primitive product action of degree m^k. Moreover, $\mathbf{N}_{\mathrm{Sym}(\Omega)}(\mathcal{F})$ is a typical primitive maximal subgroup of $\mathrm{Sym}(\Omega)$ of PA type according to the O'Nan-Scott theorem.

Let $\boldsymbol{\mathcal{F}}(\Omega)$ be the set of all regular product structures on Ω. The set $\boldsymbol{\mathcal{F}}(\Omega)$ is endowed of a natural partial order. Let $\mathcal{F} := \{\Omega_i \mid i \in I\}$ and $\tilde{\mathcal{F}} := \{\tilde{\Omega}_j \mid j \in \tilde{I}\}$ be regular (m,k)- and $(\tilde{m},\tilde{k})$-product structures on Ω, respectively. Set $I := \{1,\dots,k\}$ and $\tilde{I} := \{1,\dots,\tilde{k}\}$, and define $\mathcal{F} \leq \tilde{\mathcal{F}}$ if there exists a positive integer s with $\tilde{k} = ks$, and a regular (s,k)-partition $\Sigma = \{\sigma_i \mid i \in I\}$ of $\tilde{I}$, such that for each $i \in I$ and each $j \in \sigma_i$, $\tilde{\Omega}_j \leq \Omega_i$, that is, the partition Ω_i is a refinement of the partition $\tilde{\Omega}_j$. From [5, (5.1)], the relation $\leq$ is a partial order on $\boldsymbol{\mathcal{F}}(\Omega)$.

We conclude these preliminary observations on regular product structures by recalling [6, (5.10)].

Lemma 3.3.4. *Let $M = \mathbf{N}_{\mathrm{Sym}(\Omega)}(\mathcal{F})$ be the stabilizer in $\mathrm{Sym}(\Omega)$ of a regular (m,k)-product structure on Ω and let K be the kernel of the action of M on $\mathcal{F}$. Then*

1. *$K \leq \mathrm{Alt}(\Omega)$ if and only if m is even;*
2. *$M \leq \mathrm{Alt}(\Omega)$ if and only if m is even and either $k > 2$, or $k = 2$ and $m \equiv 0 \pmod 4$;*
3. *if $k = 2$ and $m \equiv 2 \pmod 4$, then $M \cap \mathrm{Alt}(\Omega) = K$, so $M \cap \mathrm{Alt}(\Omega)$ is not primitive on Ω (and hence $M \cap \mathrm{Alt}(\Omega)$ is not a maximal subgroup of $\mathrm{Alt}(\Omega)$). Otherwise $M \cap \mathrm{Alt}(\Omega)$ induces $\mathrm{Sym}(\mathcal{F})$ on $\mathcal{F}$.*

Preliminary lemmas

A lattice $\mathcal{L}$ is said to be *Boolean* if $\mathcal{L}$ is isomorphic to the lattice of subsets of a set X, that is, $\mathcal{L} \cong \mathcal{P}(X)$, where $\mathcal{P}(X) := \{Y \mid Y \subseteq X\}$. We also say that $|X|$ is the *rank* of the Boolean lattice $\mathcal{L}$.

Lemma 3.3.5. *Let X be a subgroup of Y. If $\mathcal{O}_Y(X)$ is Boolean of rank ℓ, then every maximal chain from X to Y has length ℓ. In particular, if $|Y : X|$ is divisible by at most ℓ primes (counting these primes with multiplicity), then $\mathcal{O}_Y(X)$ is not Boolean of rank ℓ.*

Proof. This is clear. □

Lemma 3.3.6. *Let H be a subgroup of G with $\mathcal{O}_G(H)$ Boolean. If every maximal element in $\mathcal{O}_G(H)$ is transitive, then either H is transitive or $\mathcal{O}_G(H)$ contains the stabilizer of a $(|\Omega|/2, 2)$-regular partition.*

Proof. Suppose that H is intransitive and let Γ be an orbit of H of smallest possible cardinality. Assume $1 \leq |\Gamma| < |\Omega|/2$. Then $M := G \cap (\mathrm{Sym}(\Gamma) \times \mathrm{Sym}(\Omega \setminus \Gamma))$ is a maximal element of $\mathcal{O}_G(H)$ and M is intransitive, which is a contradiction. This shows that H has two orbits on Ω both having cardinality $|\Omega|/2$. In particular, $M := \mathbf{N}_G(\{\Gamma, \Omega \setminus \Gamma\})$ is a member of $\mathcal{O}_G(H)$. □

Lemma 3.3.7. *Let H be a subgroup of G with $\mathcal{O}_G(H)$ Boolean. If every maximal element in $\mathcal{O}_G(H)$ is primitive, then either H is primitive, or $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$, $H = \mathbf{N}_G(\Sigma)$ for some $(2, 4)$-regular partition Σ and $\mathcal{O}_G(H)$ has rank 2.*

Proof. From Lemma 3.3.6, H is transitive. Suppose that H is imprimitive and let Σ be a non-trivial regular partition with $H \leq \mathbf{N}_G(\Sigma)$. If $\mathbf{N}_G(\Sigma)$ is a maximal subgroup of G, we obtain a contradiction. Thus $\mathbf{N}_G(\Sigma)$ is not maximal in G. This implies $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$, Σ is a $(2, 4)$-regular partition and $\mathcal{O}_G(H)$ has rank 2: see Fact 3.3.2 and Figure 3.2. □

Lemma 3.3.8 is needed in Remark 3.3.11 and Lemma 3.3.9 is needed in Theorem 3.3.26.

Lemma 3.3.8. *Let Ω be the set of all 2-sets from a finite set Δ. Then, in the permutation representation of $\mathrm{Sym}(\Delta)$ on Ω, $\mathrm{Sym}(\Delta) \leq \mathrm{Alt}(\Omega)$ if and only if $|\Delta|$ is even.*

Proof. It is an easy computation to see that, if g is a transposition of $\mathrm{Sym}(\Delta)$ (for its action on Δ), then g is an even permutation in its action on Ω if and only if $|\Delta|$ is even. Therefore, the proof follows. □

Lemma 3.3.9. *Let H be a transitive permutation group on Ω, let $\omega \in \Omega$ and let H_ω be the stabilizer of the point ω in H. Then $\{\omega' \in \Omega \mid \omega'^g = \omega', \forall g \in H_\omega\}$ is a block of imprimitivity for H. In particular, if H is primitive, then either $H_\omega = 1$, or ω is the only point fixed by H_ω.*

Proof. This is an exercise, see [48, Exercise 1.6.5, page 19]. □

3.3.2 Results for almost simple groups

In this section we collect some results from [5, 6] on primitive groups. Our ultimate goal is deducing some structural results on Boolean lattices $\mathcal{O}_G(H)$, when H is an almost simple primitive group

We start with a rather technical result of Aschbacher on the overgroups of a primitive group which is *product indecomposable* and not *octal*. We prefer to give only a broad description of these concepts here and we refer the interested reader to [5, 6]. These deep results have already played an important role in algebraic combinatorics; for instance, they are the key

results for proving that most primitive groups are automorphism groups of edge-transitive hypergraphs [153].

A primitive group $H \leq G$ is said to be *product decomposable* if the domain Ω admits the structure of a Cartesian product (that is, $\Omega \cong \Delta^\ell$, for some finite set Δ and for some $\ell \in \mathbb{N}$ with $\ell \geq 1$) and the group H acts on Ω preserving this Cartesian product structure. We are allowing $\ell = 1$ here, to include the case that H is almost simple. Moreover, for each component L of the socle of H one of the following holds:

(i) $L \cong \mathrm{Alt}(6)$ and $|\Delta| = 6^2$,

(ii) $L \cong M_{12}$ and $|\Delta| = 12^2$,

(iii) $L \cong \mathrm{Sp}_4(q)$ for some $q > 2$ even and $|\Delta| = (q^2(q^2-1)/2)^2$.

We also refer to [141] for a recent thorough investigation on permutation groups admitting Cartesian decompositions, where each of these peculiar examples are thoroughly investigated.

Following [5, 6], a primitive group H is said to be *octal* if each component L of the socle of H is isomorphic to $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$, the orbits of L have order 8 and the action of L on each of its orbits is primitive. For future reference, we report here that a simple computation reveals that, when $H = \mathrm{PSL}_3(2)$ is octal, $\mathcal{O}_{\mathrm{Alt}(8)}(H)$ is Boolean of rank 2, whereas $\mathcal{O}_{\mathrm{Sym}(8)}(H)$ is a lattice of size 6.

Theorem 3.3.10. [6, Theorem A] *Let Ω be a finite set of cardinality n and let H be an almost simple primitive subgroup of $\mathrm{Sym}(\Omega)$ which is product indecomposable and not octal. Then all members of $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ are almost simple, product indecomposable, and not octal, and setting $U := \mathbf{F}^*(H)$, one of the following holds:*

1. *$|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 1$.*
2. *$U = H$, $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 3$, $\mathrm{Aut}(U) \cong \mathbf{N}_{\mathrm{Sym}(\Omega)}(U) \in \mathcal{M}_{\mathrm{Sym}(\Omega)}(U)$, $\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)$ is transitive on $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H) \setminus \{\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)\}$ and U is maximal in V, where $K \in \mathcal{M}_{\mathrm{Sym}(\Omega)}(H) \setminus \{\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)\}$ and $V = \mathbf{F}^*(K)$. Further (U, V, n) is one of the following:*
   - **(a)** *$(HS, \mathrm{Alt}(m), 15400)$, where $m = 176$ and $n = \binom{m}{2}$.*
   - **(b)** *$(\mathrm{G}_2(3), \Omega_7(3), 3159)$.*
   - **(c)** *$(\mathrm{PSL}_2(q), M_n, n)$, where $q \in \{11, 23\}$, $n = q + 1$ and M_n is the Mathieu group of degree n.*
   - **(d)** *$(\mathrm{PSL}_2(17), \mathrm{Sp}_8(2), 136)$.*
3. *$U \cong \mathrm{PSL}_3(4)$, $n = 280$, $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(U)| = 4$, $\mathrm{Aut}(U) \cong \mathbf{N}_{\mathrm{Sym}(\Omega)}(U) \in \mathcal{M}_{\mathrm{Sym}(\Omega)}(U)$, $\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)$ is transitive on $\mathcal{M}_{\mathrm{Sym}(\Omega)}(U) \setminus \{\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)\}$ and $K \in \mathcal{M}_{\mathrm{Sym}(\Omega)}(H) \setminus \{\mathbf{N}_{\mathrm{Sym}(\Omega)}(U)\}$ is isomorphic to $\mathrm{Aut}(\mathrm{PSU}_4(3))$.*
4. *$U \cong \mathrm{Sz}(q)$, $q = 2^k$, $n = q^2(q^2+1)/2$, $\mathcal{M}_{\mathrm{Sym}(\Omega)}(U) = \{K_1, K_2\}$ where $K_i = \mathbf{N}_{\mathrm{Sym}(\Omega)}(V_i) \cong \mathrm{Aut}(V_i)$, $V_1 \cong \mathrm{Alt}(q^2+1)$, $V_2 \cong \mathrm{Sp}_{4k}(2)$ and $\mathbf{N}_{\mathrm{Sym}(\Omega)}(U) \cong \mathrm{Aut}(U)$ is maximal in V_1.*
5. *$H \cong \mathrm{PSL}_2(11)$, $n = 55$, $\mathrm{PGL}_2(11) \cong \mathbf{N}_{\mathrm{Sym}(\Omega)}(H)$ and $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H) = \{\mathbf{N}_{\mathrm{Sym}(\Omega)}(H), K, K^t\}$, $t \in \mathbf{N}_{\mathrm{Sym}(\Omega)}(H) \setminus H$, where $K \cong \mathrm{Sym}(11)$ and $\mathcal{O}_K(H) = \{H < L < V < K\}$, with $L \cong M_{11}$ and $V \cong \mathrm{Alt}(11)$.*

Remark 3.3.11. 1. In Case (1), since $\mathcal{M}_G(H)$ contains only one element, we deduce that the lattice $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean, unless it has rank 1.

2. In Case (2) (a), all elements in $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)$ are maximal subgroups of $\mathrm{Alt}(\Omega)$. This is because the permutation representations of $\mathrm{Aut}(HS) = HS.2$ and of $\mathrm{Sym}(m)$ of degree $\binom{m}{2}$ are the natural permutation representations on the 2-sets of a set of cardinality m. Since $m = 176$ is even, these permutation representations embed in $\mathrm{Alt}(\binom{m}{2}) = \mathrm{Alt}(\Omega)$, see Lemma 3.3.8. From this, we deduce that $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean because $\mathrm{Alt}(\Omega)$ is the only maximal element of $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$. When $G = \mathrm{Alt}(\Omega)$, $\mathcal{O}_G(H)$ has three maximal elements and one of these maximal elements is $\mathrm{Aut}(H) \cong HS.2$. If $\mathcal{O}_G(H)$ is Boolean, then it has rank 3 and hence $\mathcal{O}_{HS.2}(HS)$ is Boolean of rank 2: however this is a contradiction because $|\mathrm{Aut}(HS) : HS| = |HS.2 : HS| = 2$, see Lemma 3.3.5.

   In Case (2) (b), the group $\mathrm{Aut}(\Omega_7(3)) \cong \Omega_7(3).2$ has no faithful permutation representations of degree 3159. Since $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 3$, we deduce $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)$ contains two subgroups isomorphic to $\Omega_7(3)$ which are contained in $\mathrm{Alt}(\Omega)$ and $\mathrm{Aut}(U) \cong \mathrm{G}_2(3).2$ which is not contained in $\mathrm{Alt}(\Omega)$ (the fact that $\mathrm{G}_2(3).2 \not\leq \mathrm{Alt}(\Omega)$ can be easily verified with the computer algebra system MAGMA [19]). When $G = \mathrm{Sym}(\Omega)$, we obtain that $\mathcal{O}_G(H)$ is not Boolean. When $G = \mathrm{Alt}(\Omega)$, we were not able to determine whether $\mathcal{O}_G(H)$ is Boolean, but if it is Boolean, then it has rank 2 having maximal elements two subgroups isomorphic to $\Omega_7(3)$.

   In Case (2) (c) and $n = 12$, we see that $\mathrm{M}_{12}.2$ does not admit a permutation representation of degree 12. Therefore, as above, since $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 3$, we deduce that $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)$ contains two subgroups isomorphic to M_{12} which are contained in $\mathrm{Alt}(\Omega)$ and $\mathrm{Aut}(U) \cong \mathrm{PGL}_2(11)$ which is not contained in $\mathrm{Alt}(\Omega)$. Therefore, $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean. When $G = \mathrm{Alt}(\Omega)$, we have verified with the help of a computer that $\mathcal{O}_G(H)$ is indeed Boolean of rank 2. In Case (2) (c) and $n = 24$, we see that $\mathrm{Aut}(\mathrm{M}_{24}) = \mathrm{M}_{24}$. Therefore, since $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 3$, we deduce $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)$ contains two subgroups isomorphic to M_{24} which are contained in $\mathrm{Alt}(\Omega)$ and $\mathrm{Aut}(U) \cong \mathrm{PGL}_2(23)$ which is not contained in $\mathrm{Alt}(\Omega)$. Therefore, $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean. When $G = \mathrm{Alt}(\Omega)$, we have verified with the help of a computer that $\mathcal{O}_G(H)$ is indeed Boolean of rank 2.

   In Case (2) (d), we see that $\mathrm{Aut}(\mathrm{Sp}_8(2)) = \mathrm{Sp}_8(2)$. Therefore, since $|\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)| = 3$, we deduce that $\mathcal{M}_{\mathrm{Sym}(\Omega)}(H)$ contains two subgroups isomorphic to $\mathrm{Sp}_8(2)$ which are contained in $\mathrm{Alt}(\Omega)$ and $\mathrm{Aut}(U) \cong \mathrm{PGL}_2(17)$ which is not contained in $\mathrm{Alt}(\Omega)$. Therefore, $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean. When $G = \mathrm{Alt}(\Omega)$, we were not able to determine whether $\mathcal{O}_G(H)$ is Boolean, but if it is Boolean, then it has rank 2.

3. In Case (3), we use a computer to deal with this case. None of the four elements in $\mathcal{M}_{\mathrm{Sym}(\Omega)}(U)$ is contained in $\mathrm{Alt}(\Omega)$. Therefore, if $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is Boolean, then it has rank 4. Moreover, the intersection of these four subgroups is H and we see that $|H : U| = 2$. As $|\mathrm{Aut}(\mathrm{PSL}_3(4)) : \mathrm{PSL}_3(4)| = 12$, we deduce $|\mathbf{N}_{\mathrm{Sym}(\Omega)}(U) : H| = 6 = 2 \cdot 3$. Therefore $\mathcal{O}_{\mathbf{N}_{\mathrm{Sym}(\Omega)}(H)}(H)$ cannot be a rank 3 Boolean lattice (see Lemma 3.3.5), contradicting the fact that we assumed $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ to be Boolean. Assume then $G = \mathrm{Alt}(\Omega)$. Define $M_0 := \mathbf{N}_{\mathrm{Alt}(\Omega)}(U)$ and let M_1, M_2, M_3 be the intersections with $\mathrm{Alt}(\Omega)$ of the three maximal subgroups of $\mathrm{Sym}(\Omega)$ isomorphic to $\mathrm{Aut}(\mathrm{PSU}_4(3))$. Assume that $\mathcal{O}_{\mathrm{Alt}(\Omega)}(H)$ is Boolean. If $H < M_0$, then $\mathcal{O}_{\mathrm{Alt}(\Omega)}(H)$ is Boolean of rank 4 and hence $\mathcal{O}_{M_0}(H)$ is Boolean of rank 3. However this is impossible because $|M_0 : U| = 6 = 2 \cdot 3$. Therefore $H = M_0 = \mathbf{N}_{\mathrm{Alt}(\Omega)}(U)$. However this is another contradiction because M_0 is maximal in $\mathrm{Alt}(\Omega)$.

4. In Case (4), k is odd and hence H is a subgroup of $\mathrm{Alt}(\Omega)$. The action under consideration arises using the standard 2-transitive action of $\mathrm{Sz}(q)$ of degree $q^2 + 1$. Now, the action of degree $q^2(q^2+1)/2$ is the action on the 2-sets of the set $\{1, \ldots, q^2+1\}$. Here, $K_1 \not\leq \mathrm{Alt}(\Omega)$ because q^2+1 is odd, see Lemma 3.3.8. Moreover, $\mathrm{Aut}(\mathrm{Sp}_{4k}(2)) = \mathrm{Sp}_{2k}(2)$ and $K_2 = V_2$, hence $V_2 \leq \mathrm{Alt}(\Omega)$. From this we deduce that the maximal elements in

$\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ are $K_1 \cong \mathrm{Sym}(q^2+1)$ and $\mathrm{Alt}(\Omega)$. However this lattice is not Boolean because $H \neq K_1 \cap \mathrm{Alt}(\Omega) = V_1 \cong \mathrm{Alt}(q^2+1)$. When $G = \mathrm{Alt}(\Omega)$, the maximal elements in $\mathcal{O}_G(H)$ are $V_1 \cong \mathrm{Alt}(q^2+1)$ and $V_2 \cong \mathrm{Sp}_{4k}(2)$. Therefore, if $\mathcal{O}_G(H)$ is Boolean, then its rank is 2.

5. In Case (5), $\mathcal{O}_{\mathrm{Sym}(\Omega)}(H)$ is not Boolean because $\mathcal{O}_K(H)$ is not Boolean. When $G = \mathrm{Alt}(\Omega)$, $\mathcal{O}_{\mathrm{Alt}(\Omega)}(H)$ contains two maximal elements V and V^t both isomorphic to $\mathrm{Alt}(11)$. Therefore, if $\mathcal{O}_{\mathrm{Alt}(11)}(H)$ were Boolean, then $\mathcal{O}_{\mathrm{Alt}(\Omega)}(H)$ would have rank 2. However this is not the case because $\mathcal{O}_V(H) = \{H < M < V\}$ and $\mathcal{O}_{V^t} = \{H < M^t < V^t\}$ with $M \cong M^t \cong M_{11}$. Therefore $\mathcal{O}_{\mathrm{Alt}(\Omega)}(H)$ is not Boolean.

Corollary 3.3.12. *Let H be an almost simple primitive subgroup of G which is product indecomposable and not octal. If $\mathcal{O}_G(H)$ is Boolean, then it has rank at most 2.*

Proof. This follows from Theorem 3.3.10 and Remark 3.3.11. □

3.3.3 Boolean intervals $\mathcal{O}_G(H)$ with H primitive

Lemma 3.3.13. *Let M be a maximal subgroup of G of O'Nan-Scott type* SD *and let H be a maximal subgroup of M acting primitively on Ω. Then M and H have the same socle.*

Proof. This follows from [140, Theorem] (using the notation in [140], applied with $G_1 := M$, see also [140, Proposition 8.1]). □

Lemma 3.3.14. *Let H be a primitive subgroup of G with $\mathcal{O}_G(H)$ Boolean of rank ℓ. Suppose that there exists a maximal element $M \in \mathcal{O}_G(H)$ of O'Nan-Scott type* SD*. Then $\ell \leq 2$.*

Proof. Let V be the socle of M. From the structure of primitive groups of SD type, we deduce $V \cong T^\kappa$ and $|\Omega| = |T|^{\kappa-1}$, for some non-abelian simple group T and for some integer $\kappa \geq 2$.

If $\ell = 1$, then we have nothing to prove, therefore we suppose $\ell \geq 2$ and we let $M' \in \mathcal{O}_G(H)$ be a maximal element with $M' \neq M$. Set $H' := M \cap M'$. Since $\mathcal{O}_G(H)$ is Boolean, H' is maximal in M and since $H \leq H'$, H' acts primitively on Ω. From Lemma 3.3.13 applied with H there replaced by H' here, we obtain that H' has socle V. From the O'Nan-Scott theorem and in particular from the structure of the socles of primitive groups, we deduce that H' has type HS or SD, where the type HS can arise only when $\kappa = 2$. Now, from [140, Proposition 8.1], we obtain that either M' is a primitive group of SD type having socle V, or $M' = \mathrm{Alt}(\Omega)$. In the first case, $M' = \mathbf{N}_G(V) = M$, which is a contradiction. Therefore $M' = \mathrm{Alt}(\Omega)$. Thus $G = \mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$ and M are the only maximal members in $\mathcal{O}_G(H)$. This gives $\ell = 2$. □

Lemma 3.3.15. *Let M be a maximal subgroup of G of O'Nan-Scott type* HA *with socle V and let H be a maximal subgroup of M acting primitively on Ω. Then either*

1. *$V \leq H$, or*
2. *$|\Omega| = 8$, $G = \mathrm{Alt}(\Omega)$, $H \cong \mathrm{PSL}_2(7)$ and $M \cong \mathrm{AGL}_3(2)$.*

Proof. Here, $n = |\Omega| = p^d$, for some prime number p and some positive integer d. The result is clear when $n \leq 4$ and hence we suppose $n \geq 5$. In what follows, we assume $V \not\leq H$ and we show that $n = 8$, $G = \mathrm{Alt}(\Omega)$, $H \cong \mathrm{PSL}_2(7)$ and $M \cong \mathrm{AGL}_3(2)$.

The maximality of H in M yields $VH = M$. Since $V \cap H \trianglelefteq \langle V, H\rangle = M$, we deduce $V \cap H = 1$, that is, H is a complement of V in M and hence $H \cong M/V$. Since $\mathbf{N}_{\mathrm{Sym}(n)}(V) \cong \mathrm{AGL}_d(p)$, we deduce M/V and H are isomorphic to $\mathrm{GL}_d(p)$ or to an index 2 subgroup of $\mathrm{GL}_d(p)$.

Since H acts primitively on Ω, we deduce $\mathbf{Z}(H) = 1$ or $\mathbf{Z}(H) = H$. Clearly, the second case cannot arise here because M/V is non-abelian being $n \geq 5$. Suppose then $\mathbf{Z}(H) = 1$.

If $G = \mathrm{Sym}(\Omega)$, then $M/V \cong \mathrm{GL}_d(p)$ has trivial centre only when $p = 2$. It is easy to verify (using the fact that $\mathrm{GL}_d(2)$ is generated by transvections) that $\mathrm{AGL}_d(2)$ is contained in $\mathrm{Alt}(\Omega)$, when $d \geq 3$. Thus $M < \mathrm{Alt}(\Omega) < G$, contradicting the hypothesis that M is maximal in G. This shows that $G = \mathrm{Alt}(\Omega)$. In particular, when $p = 2$, we have $M/V \cong \mathrm{GL}_d(2)$ and when $p > 2$, M/V is isomorphic to a subgroup of $\mathrm{GL}_d(p)$ having index 2.

Since $\mathrm{GL}_d(p)$ has centre of order $p - 1$ and since $\mathbf{Z}(H) = 1$, we deduce that either $p = 2$ or $(p - 1)/2 = 1$, that is, $p \in \{2, 3\}$. In both cases, a simple computation reveals that $M = \mathrm{ASL}_d(p)$ and hence $H \cong M/V \cong \mathrm{SL}_d(p)$. Observe that, when $p = 3$, d is odd because $1 = |\mathbf{Z}(H)| = |\mathbf{Z}(\mathrm{SL}_d(3))| = \gcd(d, 2)$. In particular, in both cases, $H \cong M/V \cong \mathrm{SL}_d(p) \cong \mathrm{PSL}_d(p)$ is a non-abelian simple group. Given $\omega \in \Omega$, $|H : H_\omega| = p^d$ is a power of the prime p and hence, from [61, (3.1)], we deduce $(d, p) = (3, 2)$. Thus $n = p^d = 8$, $H \cong \mathrm{SL}_3(2) \cong \mathrm{PSL}_2(7)$. □

Lemma 3.3.16. *Let H be a primitive subgroup of G with $\mathcal{O}_G(H)$ Boolean of rank ℓ. Suppose that there exists a maximal element $M \in \mathcal{O}_G(H)$ of O'Nan-Scott type* HA. *Then, every maximal element M' in $\mathcal{O}_G(H)$ with $M' \neq M$ is either* $\mathrm{Alt}(\Omega)$ *or the stabilizer in G of a regular product structure on Ω.*

Proof. If $\ell = 1$, then we have nothing to prove, therefore we suppose that $\ell \geq 2$ and we let $M' \in \mathcal{O}_G(H)$ be a maximal element of $\mathcal{O}_G(H)$ with $M' \neq M$. Set $H' := M \cap M'$. Since $\mathcal{O}_G(H)$ is Boolean, H' is maximal in M and since $H \leq H'$, H' acts primitively on Ω. From Lemma 3.3.15 applied with H replaced by H', we obtain that either H' contains the socle V of M, or $n = 8$, $G = \mathrm{Alt}(\Omega)$, $H' \cong \mathrm{PSL}_2(7)$ and $M \cong \mathrm{AGL}_3(2)$. In the second case, a computer computation reveals that the largest Boolean lattice $\mathcal{O}_{\mathrm{Alt}(8)}(H)$ with H primitive has rank 2. Therefore, for the rest of the proof, we suppose $V \leq M'$. In particular, M' is a primitive permutation group containg an abelian regular subgroup. Thus M' is one of the groups classified in [85, Theorem 1.1]: we apply this classification here and the notation therein.

Assume M' is as in [85, Theorem 1.1 (1)], that is, M' is a maximal primitive subgroup of G of O'Nan-Scott type HA. Let V' be the socle of M'. From Lemma 3.3.15, we deduce $V' \leq M$ and hence $VV' \leq H'$. Since $V \trianglelefteq M$ and $V' \trianglelefteq M'$, we deduce that $VV' \trianglelefteq H'$. As H' acts primitively on Ω, we deduce that VV' is the socle of H' and hence $|VV'| = |V|$. Therefore $V = V'$. Thus $M' = \mathbf{N}_G(V) = M$, which is a contradiction. Therefore M' is one of the groups listed in [85, Theorem 1.1 (2)].

Suppose first that $l = 1$ (the positive integer l is defined in [85, Theorem 1.1]). An inspection in the list in [85, Theorem 1.1 (2)] (using the maximality of M' in G) yields

1. $M' \cong \mathrm{M}_{11}$, $n = 11$ and $G = \mathrm{Alt}(\Omega)$, or
2. $M' \cong \mathrm{M}_{23}$, $n = 23$ and $G = \mathrm{Alt}(\Omega)$, or
3. $M' \cong \mathbf{N}_G(\mathrm{PSL}_{d'}(q'))$ for some integer $d' \geq 2$ and some prime power q' with $n = p = (q'^{d'} - 1)/(q' - 1)$, or
4. $M' = \mathrm{Alt}(\Omega)$ and $G = \mathrm{Sym}(\Omega)$.

A computer computation shows that in (1) and (2), $M = \mathbf{N}_G(V) \leq M'$, which is a contradiction. Assume that M' is as in (3). Write $q' = r'^{\kappa'}$, for some prime number r' and for some positive integer κ'. Then V is a Singer cycle in $\mathrm{PGL}_{d'}(q')$. As $H' = M \cap M' = \mathbf{N}_G(V) \cap M' = \mathbf{N}_{M'}(V)$, we obtain

$$|H' : V| = \begin{cases} d'\kappa', & \text{when } \mathbf{N}_{\mathrm{Sym}(p)}(\mathrm{PGL}_{d'}(q')) \leq G, \\ d'\kappa'/2, & \text{when } \mathbf{N}_{\mathrm{Sym}(p)}(\mathrm{PGL}_{d'}(q')) \not\leq G. \end{cases}$$

We claim that d' is prime. If d' is not prime, then $d' = d_1 d_2$, for some positive integers $d_1, d_2 > 1$. Thus $H' < \mathbf{N}_G(\mathrm{PSL}_{d_1}(q'^{d_2})) < M'$, contradicting the fact that H' is maximal in M'. Therefore, d' is a prime number. Moreover, since H' is maximal in M and since M/V is cyclic (of order $p-1$ or $(p-1)/2$), we deduce that $s' := |M : H'|$ is a prime number.

Let M'' be a maximal element in $\mathcal{O}_G(H)$ with $M \neq M'' \neq M'$ and let $H'' := M \cap M''$. Arguing as in the previous paragraph (with M' replaced by M''), M'' cannot be as in (1) or as in (2). Suppose that M'' is as in (3). Thus $M'' \cong \mathbf{N}_G(\mathrm{PSL}_{d''}(q''))$ for some integer $d'' \geq 2$ and some prime power q'' with $n = p = (q''^{d''} - 1)/(q'' - 1)$. Write $q'' = r''^{\kappa''}$, for some prime number r'' and for some positive integer κ''. Arguing as in the previous paragraph, we obtain that d'' and $s'' := |M : H''|$ are prime numbers. Now, $M' \cap M''$ acts primitively on Ω with $n = |\Omega| = p$ prime and hence, from a result of Burnside, $M' \cap M''$ is either solvable (and $V \trianglelefteq M' \cap M''$) or $M' \cap M''$ is 2-transitive. In the first case, $M \cap M' = \mathbf{N}_{M'}(V) \geq M' \cap M''$; however, this contradicts the fact that $\mathcal{O}_G(H)$ is Boolean. Therefore $M' \cap M''$ is 2-transitive and non-solvable. From [76, Theorem 3], we deduce that one of the following holds:

1. $M' \cap M'' = \mathrm{PSL}_2(11)$ and $n = p = 11$, or
2. $M' \cap M'' = \mathrm{M}_{11}$ and $n = p = 11$, or
3. $M' \cap M'' = \mathrm{M}_{23}$ and $n = p = 23$, or
4. $M' \cap M'' \trianglelefteq M'$ and $M' \cap M'' \trianglelefteq M''$.

The last case cannot arise because $M' \cap M'' \trianglelefteq \langle M', M'' \rangle = G$ implies $M' \cap M'' = 1$, which is a contradiction. Also none of the first three cases can arise here because p is not of the form $(q'^{d'} - 1)/(q' - 1)$. This final contradiction shows that, if M'' is a maximal element of $\mathcal{O}_G(H)$ with $M'' \notin \{M, M'\}$, then $M'' = \mathrm{Alt}(\Omega)$. Thus $\ell = 3$, $|\Omega| = p$, $G = \mathrm{Sym}(\Omega)$ and the maximal elements in $\mathcal{O}_G(H)$ are $\mathrm{Alt}(\Omega)$, $\mathrm{AGL}_1(p)$ and $\mathrm{P\Gamma L}_{d'}(q')$.

Since $M \cong \mathrm{AGL}_1(p)$, $|H' : V| = d'\kappa'$ and $|M : H'| = s'$ is prime, we obtain

$$q' \frac{q'^{d'-1} - 1}{q' - 1} = p - 1 = |M : V| = |M : H'||H' : V| = s'd'\kappa'. \tag{3.3.1}$$

Suppose first that $d' = 2$ and hence $p = q' + 1 = r'^{\kappa'} + 1$. We get the equation $r'^{\kappa'} = 2s'\kappa'$ and hence $r' = 2$. Therefore $2^{\kappa'-1} = s'\kappa'$. Therefore, $s' = 2$ and hence $2^{\kappa'-2} = \kappa'$. Thus $\kappa' = 4$ and hence $n = p = 17$. A computer computation shows that this case does not arise because $\mathrm{Alt}(17) \cap \mathrm{AGL}_1(17) = \mathrm{AGL}_1(17) \cap \mathrm{P\Gamma L}_2(16)$. Suppose now $d' > 2$.

Assume $\kappa' = 1$. Then (3.3.1) yields $s' = 2$ because $p - 1$ is even. A computation shows that the equation

$$q' \frac{q'^{d'-1} - 1}{q' - 1} = 2d'$$

has solution only when $d' = 3$ and $q' = 2$. Thus $n = p = 7$. A computer computation shows that this case does not arise because $\mathrm{Alt}(7) \cap \mathrm{AGL}_1(7) \leq \mathrm{Alt}(7) \cap \mathrm{PGL}_2(7)$. Therefore $\kappa' > 1$.

Now, we first show $d' \neq r'$. To this end, we argue by contradiction and we suppose $d' = r'$. Then, (3.3.1) yields

$$\frac{q'}{r'} \frac{q'^{d'-1} - 1}{q' - 1} = s'\kappa'. \tag{3.3.2}$$

Since $q'/r' = r'^{\kappa'-1}$ and $(q'^{d'-1} - 1)/(q' - 1)$ are relatively prime and since s' is prime, we have either $s' = r'$ or s' divides $(q'^{d'-1} - 1)/(q' - 1)$. In the first case,

$$\frac{q'}{r'^2} \frac{q'^{d'-1} - 1}{q' - 1} = \kappa',$$

hence, for $d' > 3$, $\kappa' \geq (q'^{d'-1}-1)/(q'-1) \geq q'^2 = r'^{2\kappa'}$, which is impossible. It is not difficult to observe that (3.3.2) is not satisfied also for $d' = 3$. In the second case, $\kappa' \geq q'/r' = r'^{\kappa'-1}$, which is possible only when $\kappa' = 2$. When $\kappa' = 2$, (3.3.2) becomes

$$r' \frac{(r'^{d-1}-1)(r'^{d-1}+1)}{r'^2-1} = 2s',$$

which has no solution with s' prime. Therefore $d' \neq r'$.

Since d' is a prime number and since $d' \neq r'$, from Fermat's little theorem we have $q'^{d'-1} \equiv 1 \pmod{d'}$, that is, d' divides $q'^{d'-1}-1$. If $q' \equiv 1 \pmod{d'}$, then

$$p = \frac{q'^{d'}-1}{q'-1} = q'^{d'-1} + q'^{d'-2} + \cdots + \cdots + q' + 1 \equiv 0 \pmod{d'}$$

and hence $p = d'$, however this is clearly a contradiction because $p > d'$. Thus d' does not divide $q'-1$. This proves that d' divides $(q'^{d'-1}-1)/(q'-1)$ and hence $(q'^{d'-1}-1)/d'(q'-1)$ is an integer. From (3.3.1), we get

$$q' \frac{q'^{d'-1}-1}{d'(q'-1)} = \kappa' s'.$$

Since s' is prime and $q' > \kappa'$, this equality might admit a solution only when $(q'^{d'-1}-1)/(d'(q'-1)) = 1$, that is, $q'^{d'-1}-1 = d'(q'-1)$. This happens only when $q' = 2$ and $d' = 3$, but this contradicts $\kappa' > 1$.

For the rest of the argument we may suppose $l \geq 2$. In particular, from [85, Theorem 1.1], we obtain that either $M' = \mathrm{Alt}(\Omega)$, or M' is the stabilizer in G of a regular product structure on Ω. Since this argument does not depend upon M', the result follows. □

Lemma 3.3.17. *Let M be a maximal subgroup of G of O'Nan-Scott type* AS *with $M \neq \mathrm{Alt}(\Omega)$ and let H be a maximal subgroup of M acting primitively on Ω. Then*

1. *M and H have the same socle, or*
2. *H has O'Nan-Scott type* AS *and the pair (H, M) appears in Tables* 3–6 *of [93], or*
3. *H has O'Nan-Scott type* HA *and the pair (H, M) appears in Table* 2 *of [140].*

Proof. Suppose that H and M do not have the same socle. It follows from [140, Proposition 6.2] that either H has O'Nan-Scott type AS and the pair (H, M) appears in Tables 3–6 of [93], or H has O'Nan-Scott type HA and the pair (H, M) appears in Table 2 of [140]. □

Lemma 3.3.18. *Let H be a primitive subgroup of G with $\mathcal{O}_G(H)$ Boolean of rank ℓ. Suppose that there exists a maximal element $M \in \mathcal{O}_G(H)$ of O'Nan-Scott type* AS *with $M \neq \mathrm{Alt}(\Omega)$. Then $\ell \leq 2$.*

Proof. If $\ell \leq 2$, then we have nothing to prove, therefore we suppose $\ell \geq 3$. Since M is a maximal element in $\mathcal{O}_G(H)$ of O'Nan-Scott type AS and $M \neq \mathrm{Alt}(\Omega)$, from Lemma 3.3.16, we deduce that no maximal element in $\mathcal{O}_G(H)$ is of O'Nan-Scott type HA. Similarly, from Lemma 3.3.14, no maximal element in $\mathcal{O}_G(H)$ is of O'Nan-Scott type SD. As H acts primitively on Ω, all elements in $\mathcal{O}_G(H)$ are primitive and hence, the maximal elements in $\mathcal{O}_G(H)$ have O'Nan-Scott type AS or PA. Since $\ell \geq 3$, we let $M' \in \mathcal{O}_G(H)$ be a maximal element with $\mathrm{Alt}(\Omega) \neq M' \neq M$. Moreover, we let M'' be any maximal element in $\mathcal{O}_G(H)$ with $M \neq M'' \neq M'$. Set $H' := M \cap M'$ and $H'' := M \cap M' \cap M''$. See Figure 3.3.

Since $\mathcal{O}_G(H)$ is Boolean, H' is maximal in M and hence we are in the position to apply Lemma 3.3.17 with H there replaced by H' here. We discuss the three possibilities in turn.

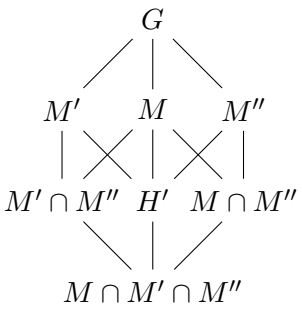

Figure 3.3: The Boolean lattice in the proof of Lemma 3.3.18

Suppose first that H' has O'Nan-Scott type HA and let V' be the socle of H'. Since in $\mathcal{O}_G(H)$ there are no maximal members of HA type, $\mathbf{N}_G(V')$ is not a maximal subgroup of G. It follows from [93, Theorem] that $n \in \{7, 11, 17, 23\}$ and $G = \mathrm{Alt}(\Omega)$. A computer computation shows that none of these cases gives rise to a Boolean lattice of rank 3 or larger.

Suppose now that H' and M have the same socle, or that the pair (H', M) appears in Tables 3–6 of [93]. In these cases, H' has O'Nan-Scott type AS. Since $\mathcal{O}_G(H)$ is Boolean, H'' is maximal in H' and hence, from Lemma 3.3.17, either

- H'' and H' have the same socle,
- or H'' has O'Nan-Scott type AS and the pair (H'', H') appears in Tables 3–6 of [93],
- or H'' has O'Nan-Scott type HA and the pair (H'', H') appears in Table 2 of [140].

Suppose first that H'' has O'Nan-Scott type HA and let V'' be the socle of H''. Since in $\mathcal{O}_G(H)$ there are no maximal members of HA type, $\mathbf{N}_G(V'')$ is not a maximal subgroup of G, as above. It follows from [93, Theorem] that $n \in \{7, 11, 17, 23\}$ and $G = \mathrm{Alt}(\Omega)$. The same computer computation as above shows that none of these cases gives rise to a Boolean lattice of rank 3 or larger. Therefore, H'' has O'Nan-Scott type AS.

As $\mathcal{O}_G(H'')$ has rank 3 and H'' has type AS, Corollary 3.3.12 implies that H'' is either product decomposable or octal. If H'' is octal, then $n = 8$ and $H'' \cong \mathrm{PSL}_2(7)$, however the largest Boolean lattice containing H'' has rank 2. Thus H'' is product decomposable.

From [93, Table II], one of the following holds:

1. $n = 36$, $H'' = \mathrm{Alt}(6).2$,
2. $n = 144$, $H'' = M_{12}.2$,
3. $n = q^4(q^2-1)^2/4$ and $\mathbf{F}^*(H'') = \mathrm{Sp}_4(q)$, where $q > 2$ is even.

When $n = 144$ and $H'' = M_{12}.2$, we see that H' cannot have the same socle as H'' because $H'' \cong \mathrm{Aut}(M_{12})$ and hence (H'', H') is one of the pairs in Tables 3–6 of [93]. However, there is no such pair satisfying $n = 144$ and $\mathbf{F}^*(H'') \cong M_{12}$. When $n = 36$ and $H'' = \mathrm{Alt}(6).2$, we see with a computer computation that $\mathbf{N}_{\mathrm{Sym}(36)}(H'') = H''$ and hence H' cannot have the same socle as H''. Therefore (H'', H') is one of the pairs in Tables 3–6 of [93]. However, there is no such pair satisfying $n = 36$ and $\mathbf{F}^*(H'') \cong \mathrm{Alt}(6)$. Finally, suppose $n = q^4(q^2-1)^2/4$ and $\mathbf{F}^*(H'') = \mathrm{Sp}_4(q)$, where $q > 2$ is even. Since there is no pair (H'', H') in Tables 3–6 of [93] satisfying these conditions for n and $\mathbf{F}^*(H'')$ as above, we deduce that H'' and H' have the same socle. Therefore $\mathbf{F}^*(H') = \mathrm{Sp}_4(q)$, with $q > 2$ even.

Summing up, we have two inclusions $H' \leq M$ and $H' \leq M'$, with H' maximal in both M and M', with $\mathbf{F}^*(H') = \mathrm{Sp}_4(q)$ and with $n = q^4(q^2-1)^2/4$. Using again Tables 3–6 of [93], we deduce that both M and M' must have the same socle of H'. However, this is a contradiction because $G = \langle M, M' \rangle \leq \mathbf{N}_G(\mathbf{F}^*(H'))$. □

Corollary 3.3.19. *Let H be a primitive subgroup of G with $\mathcal{O}_G(H)$ Boolean of rank $\ell \geq 3$ and let $G_1, \ldots, G_\ell$ be the maximal members in $\mathcal{O}_G(H)$. Then one of the following holds:*

1. *$n = |\Omega|$ is odd. For every $i \in \{1, \ldots, \ell\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_\ell$.*

2. *$n = |\Omega|$ is odd and $G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell - 1\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-1}$.*

3. *$n = |\Omega|$ is an odd prime power. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, G_ℓ is maximal subgroup of O'Nan-Scott type HA, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell - 1\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-1}$.*

4. *$n = |\Omega|$ is an odd prime power and $G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$ and $G_{\ell-1}$ is a maximal subgroup of O'Nan-Scott type HA, for every $i \in \{1, \ldots, \ell - 2\}$, there exists a non-trivial regular product structure $\mathcal{F}_i$ with $G_i = \mathbf{N}_G(\mathcal{F}_i)$; moreover, relabeling the index set $\{1, \ldots, \ell - 2\}$ if necessary, $\mathcal{F}_1 < \cdots < \mathcal{F}_{\ell-2}$.*

Proof. As $\ell \geq 3$, from Lemmas 3.3.14, 3.3.16 and 3.3.18, all the elements in $\{G_1, \ldots, G_\ell\}$ are stabilizers of regular product structures, except possibly that one of these elements might be $\mathrm{Alt}(\Omega)$ or a maximal subgroup of type HA. Relabelling the index set $\{1, \ldots, \ell\}$, suppose that $\{G_1, \ldots, G_\kappa\}$ are stabilizers of regular product structures, that is, $G_i := \mathbf{N}_G(\mathcal{F}_i)$. Thus $\kappa \geq \ell - 2$.

Observe that, for every $i, j \in \{1, \ldots, \kappa\}$ with $i \neq j$, $G_i \cap G_j$ is a maximal subgroup of both G_i and G_j. It follows from [6, Section 5] that either $\mathcal{F}_i < \mathcal{F}_j$ or $\mathcal{F}_j < \mathcal{F}_i$. Therefore $\{\mathcal{F}_1, \ldots, \mathcal{F}_\kappa\}$ forms a chain. Relabeling the index set $\{1, \ldots, \kappa\}$ if necessary, we may suppose $\mathcal{F}_1 < \mathcal{F}_2 < \cdots < \mathcal{F}_\kappa$.

Assume that $\mathcal{F}_i$ is a regular (m_i, k_i)-product structure. Since $\mathcal{F}_i \leq \mathcal{F}_{i+1}$, there exists an integer $s_i > 1$ with $m_i = m_{i+1}^{s_i}$ and $k_{i+1} = k_i s_i$. From [6, (5.12)], $\mathcal{O}_G(\mathbf{N}_G(\mathcal{F}_i) \cap \mathbf{N}_G(\mathcal{F}_{i+1}))$ is Boolean of rank 2 only when

$$(\dagger) \quad m_{i+1} \text{ is odd, or } s_i = 2 \text{ and } m_{i+1} \equiv 2 \pmod 4.$$

Suppose that $\kappa \geq 3$. Applying the previous paragraph with $i := \kappa - 1$, we deduce that, if m_κ is even, then $s_{\kappa-1} = 2$ and $m_\kappa \equiv 2 \pmod 4$. In turn, since $m_{\kappa-1} = m_\kappa^{s_{\kappa-1}}$ is even, we have $s_{\kappa-2} = 2$ and $m_{\kappa-1} \equiv 2 \pmod 4$. However, $m_{\kappa-1} = m_\kappa^{s_{\kappa-1}} \equiv 0 \pmod 4$, contradicting the fact that $m_{\kappa-1} \equiv 2 \pmod 4$. Therefore, when $\kappa \geq 3$, m_i is odd, for every $i \in \{1, \ldots, \kappa\}$, that is, $n = |\Omega|$ is odd. In particular, when $\kappa = \ell$, we obtain part (1).

Suppose that $G = \mathrm{Sym}(\Omega)$, $\kappa = \ell - 1$ and $G_\ell = \mathrm{Alt}(\Omega)$. If $|\Omega|$ is odd, we obtain part (2). Suppose then $n = |\Omega|$ is even. In particular, $\kappa = \ell - 1 \leq 2$ and hence $\ell = 3$. Clearly, m_2 is even and hence (†) applied with $i = 1$ yields $s_1 = 2$. Thus $m_1 = m_2^{s_1} = m_2^2 \equiv 0 \pmod 4$. Lemma 3.3.4 (2) yields $G_1 \leq \mathrm{Alt}(\Omega) = G_3$, which is a contradiction.

Suppose that $\kappa = \ell - 1$ and G_ℓ is a primitive group of HA type. If $|\Omega|$ is odd, we obtain part (3). Suppose then $n = |\Omega|$ is even, that is, $n = 2^d$, for some positive integer $d \geq 3$. In particular, $\kappa = \ell - 1 \leq 2$ and hence $\ell = 3$. Clearly, m_2 is even and hence (†) applied with $i = 1$ yields $m_2 \equiv 2 \pmod 4$. Therefore $m_2 = 2$, however this contradicts the fact that in a regular (m, k)-product struction we must have $m \geq 5$.

Finally suppose that $\kappa = \ell - 2$, $G = \mathrm{Sym}(\Omega)$, $G_\ell = \mathrm{Alt}(\Omega)$ and $G_{\ell-1}$ is a primitive group of HA type. If $|\Omega|$ is even, then $|\Omega| = 2^d$ for some $d \geq 3$. As $G_2 \cong \mathrm{AGL}_d(2) \leq \mathrm{Alt}(\Omega) = G_3$, we obtain a contradiction. Therefore $|\Omega|$ is odd and we obtain (4). □

3.3.4 Boolean intervals containing a maximal imprimitive subgroup

The scope of this section is to gather some information on Boolean lattices $\mathcal{O}_G(H)$ containing a maximal element that is imprimitive. Our main tool in this task is a result of Aschbacher and Shareshian [8, Theorem 5.2].

Hypothesis 3.3.20. Let G be either $\mathrm{Sym}(\Omega)$ or $\mathrm{Alt}(\Omega)$ with $n := |\Omega|$, let Σ be a non-trivial regular partition, let $G_1 := \mathbf{N}_G(\Sigma)$, let G_2 be a maximal subgroup of G distinct from $\mathrm{Alt}(\Omega)$ and let $H := G_1 \cap G_2$. Assume that

- $\mathcal{O}_G(H)$ is a Boolean lattice of rank 2 with maximal elements M_1 and M_2, and
- H acts transitively on Ω.

Theorem 3.3.21. [8, Theorem 5.2] *Assume Hypothesis 3.3.20. Then one of the following holds:*

1. *For every $i \in \{1,2\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$; moreover, for some $i \in \{1,2\}$, $\Sigma_i < \Sigma_{3-i}$. Further, $n \geq 8$ and, if $n = 8$, then $G = \mathrm{Sym}(\Omega)$.*
2. *$G = \mathrm{Alt}(\Omega)$, $n = 2^{a+1}$ for some positive integer $a > 1$, G_2 is an affine primitive group, $V = \mathbf{F}^*(G_2) \leq H$, V_Σ is a hyperplane of V, the elements of Σ are the two orbits of V_Σ on Ω, and $H = \mathbf{N}_{G_2}(V_\Sigma)$.*
3. *$G = \mathrm{Alt}(\Omega)$, $n \equiv 0 \pmod 4$, $n > 8$ and, for every $i \in \{1,2\}$, there exists a non-trivial regular partition Σ_i such that*
   - **(a)** *$G_i = \mathbf{N}_G(\Sigma_i)$,*
   - **(b)** *Σ_1 and Σ_2 are lattice complements in the poset of partitions of Ω, and*
   - **(c)** *one of Σ_1, Σ_2 is $(2, n/2)$-regular and the other is $(n/2, 2)$-regular.*

(Observe that two partitions Σ_1 and Σ_2 of Ω are lattice complements if, the smallest partition Σ of Ω with $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$ and the largest partition Σ' of Ω with $\Sigma' \leq \Sigma_1$ and $\Sigma' \leq \Sigma_2$ are the two trivial partitions of Ω. Futher V_Σ denote the poitwise stabilizer of Σ in V.)

Hypothesis 3.3.22. Let G be either $\mathrm{Sym}(\Omega)$ or $\mathrm{Alt}(\Omega)$ with $n := |\Omega|$, let Σ be a non-trivial regular partition, let $G_1 := \mathbf{N}_G(\Sigma)$, let G_2 and G_3 be maximal subgroups of G and let $H := G_1 \cap G_2 \cap G_3$. Assume that

- $\mathcal{O}_G(H)$ is a Boolean lattice of rank 3 with maximal elements G_1, G_2 and G_3, and
- H acts transitively on Ω.

Theorem 3.3.23. *Assume Hypothesis 3.3.22. Then one of the following holds:*

1. *For every $i \in \{1,2,3\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$; moreover, relabeling the index set $\{1,2,3\}$ if necessary, $\Sigma_1 < \Sigma_2 < \Sigma_3$.*
2. *$G = \mathrm{Sym}(\Omega)$. Relabeling the index set $\{1,2,3\}$ if necessary, $G_3 = \mathrm{Alt}(\Omega)$ and, for every $i \in \{1,2\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$, moreover, for some $i \in \{1,2\}$, $\Sigma_i < \Sigma_{3-i}$.*
3. *$G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$ and the Boolean lattice $\mathcal{O}_G(H)$ is in Figure 3.2.*

Proof. If none of G_1, G_2 and G_3 is $\mathrm{Alt}(\Omega)$ and if $G = \mathrm{Sym}(\Omega)$, then the result follows directly from Theorem 3.3.21 and we obtain (1). Suppose $G = \mathrm{Sym}(\Omega)$ and one of G_2 or G_3 is $\mathrm{Alt}(\Omega)$. Without loss of generality we may assume that $G_3 = \mathrm{Alt}(\Omega)$. Now, the result follows directly from Theorem 3.3.21 applied to $\{G_1, G_2\}$; we obtain (2).

It remains to consider the case $G = \mathrm{Alt}(\Omega)$. In particular, we may apply Theorem 3.3.21 to the pairs $\{G_1, G_2\}$ and $\{G_1, G_3\}$. Relabeling the index set $\{1, 2, 3\}$ if necessary, we have to consider in turn one of the following cases:

case A Theorem 3.3.21 part (1) holds for both pairs $\{G_1, G_2\}$ and $\{G_1, G_3\}$;

case B Theorem 3.3.21 part (1) holds for $\{G_1, G_2\}$ and Theorem 3.3.21 part (2) holds for $\{G_1, G_3\}$;

case C Theorem 3.3.21 part (1) holds for $\{G_1, G_2\}$ and Theorem 3.3.21 part (3) holds for $\{G_1, G_3\}$;

case D Theorem 3.3.21 part (2) holds for both pairs $\{G_1, G_2\}$ and $\{G_1, G_3\}$;

case E Theorem 3.3.21 part (2) holds for $\{G_1, G_2\}$ and Theorem 3.3.21 part (3) holds for $\{G_1, G_3\}$;

case F Theorem 3.3.21 part (3) holds for both pairs $\{G_1, G_2\}$ and $\{G_1, G_3\}$.

Case A: In particular, G_2 and G_3 are stabilizers of non-trivial regular partitions and hence we are in the position to apply Theorem 3.3.21 also to the pair $\{G_2, G_3\}$. It is not hard to see that Theorem 3.3.21 part (1) holds for $\{G_2, G_3\}$ and that the conclusion (1) in the statement of Theorem 3.3.23 holds.

Case B: Since G_1 is the stabilizer of a non-trivial regular partition and since $\{G_1, G_3\}$ satisfies Theorem 3.3.21 part (2), we deduce that G_3 is an affine primitive group and Σ_1 is an $(n/2, 2)$-regular partition.

Since G_2 is the stabilizer of the non-trivial regular partition Σ_2, we deduce that we may apply Theorem 3.3.21 to the pair $\{G_2, G_3\}$. In particular, as G_3 is primitive, Theorem 3.3.21 part (2) must hold for $\{G_2, G_3\}$ and hence G_2 is the stabilizer of an $(n/2, 2)$-regular partition. However, this contradicts the fact that $\{G_1, G_2\}$ satisfies Theorem 3.3.21 part (1), that is, $\Sigma_1 < \Sigma_2$ or $\Sigma_2 < \Sigma_1$.

Case C: We have either

(a) $\Sigma_1 < \Sigma_2$, Σ_1 is a $(2, n/2)$-regular partition, Σ_3 is a $(n/2, 2)$-regular partition and Σ_1, Σ_3 are lattice complements, or

(b) $\Sigma_2 < \Sigma_1$, Σ_1 is a $(n/2, 2)$-regular partition, Σ_3 is a $(2, n/2)$-regular partition and Σ_1, Σ_3 are lattice complements.

In case **(b)**, $\Sigma_2 < \Sigma_1$ and hence Σ_1 is a refinement of Σ_2; however, as Σ_1 is a $(n/2, 2)$-regular partition, this is not possible. Therefore, case **(b)** does not arise. As G_2 and G_3 are stabilizers of non-trivial regular partitions of Ω, we are in the position to apply Theorem 3.3.21 also to the pair $\{G_2, G_3\}$. If Theorem 3.3.21 part (1) holds for $\{G_2, G_3\}$, then either $\Sigma_2 < \Sigma_3$ or $\Sigma_3 < \Sigma_2$. However, both possibilities lead to a contradiction. Indeed, if $\Sigma_2 < \Sigma_3$ and **(a)** holds, then $\Sigma_1 < \Sigma_2 < \Sigma_3$, contradicting the fact that Σ_1 and Σ_3 are lattice complements. The argument when $\Sigma_3 < \Sigma_2$ is analogous. Similarly, if Theorem 3.3.21 part (3) holds for $\{G_2, G_3\}$, then Σ_2 and Σ_3 are lattice complements and either

(a)' Σ_2 is a $(2, n/2)$-regular partition and Σ_3 is a $(n/2, 2)$-regular partition, or

(b)' Σ_2 is a $(n/2, 2)$-regular partition and Σ_3 is a $(2, n/2)$-regular partition.

However, an easy case-by-case analysis shows that **(a)'** and **(b)'** are incompatible with **(a)**.

Case D: In particular, G_2 and G_3 are both primitive groups of affine type. Let V_2 be the socle of G_2 and let V_3 be the socle of G_3. From Lemma 3.3.7 applied to $\mathcal{O}_G(G_2 \cap G_3)$, we deduce that either $G_2 \cap G_3$ is primitive, or $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$ and $G_2 \cap G_3$ is the stabilizer of a $(2,4)$-regular partition. In the latter case, we see with a direct computation that part (3) holds. Suppose then that $G_2 \cap G_3$ is primitive. From Lemma 3.3.15 applied to the inclusions $G_2 \cap G_3 < G_2$ and $G_2 \cap G_3 < G_3$, we deduce that either

(a)" $G_2 \cap G_3$, G_2 and G_3 have the same socle, or

(b)" $n = 8$, $G_2 \cap G_3 \cong \mathrm{PSL}_2(7)$ and $G_2 \cong G_3 \cong \mathrm{AGL}_3(2)$.

In the former case, we have $V_2 = V_3$ and hence $G_2 = \mathbf{N}_G(V_2) = \mathbf{N}_G(V_3) = G_3$, contradicting the fact that $G_2 \neq G_3$. In the latter case, we have checked with the invaluable help of the computer algebra system MAGMA [19] that $\mathcal{O}_{\mathrm{Alt}(8)}(\mathrm{PSL}_2(7)) = \{\mathrm{PSL}_2(7) < \mathrm{AGL}_3(2) < \mathrm{Alt}(8)\}$, contradicting the fact that it is a Boolean lattice.

Case E: In this case, Σ_1 is a $(n/2,2)$-regular partition, Σ_3 is a $(2,n/2)$-regular partition and Σ_1, Σ_3 are lattice complements. As G_3 is the stabilizer of a non-trivial regular partition, we are in the position to apply Theorem 3.3.21 to the pair $\{G_2, G_3\}$. As G_2 is primitive, we see that Theorem 3.3.21 part (2) holds for $\{G_2, G_3\}$ and hence Σ_3 is a $(n/2,2)$-regular partition, which implies $(n/2,2) = (2,n/2)$, that is, $n = 4$. However this contradicts $a > 1$ in Theorem 3.3.21 part (2).

Case F: In particular, both Σ_2 and Σ_3 are either $(n/2,2)$-regular partitions or $(2,n/2)$-regular partitions. As G_2 and G_3 are stabilizers of non-trivial regular partitions, we may apply Theorem 3.3.21 also to the pair $\{G_2, G_3\}$. Clearly, none of parts (1), (2) and (3) in Theorem 3.3.21 holds for $\{G_2, G_3\}$, which is a contradiction. □

Corollary 3.3.24. *Let H be a transitive subgroup of G and suppose that $\mathcal{O}_G(H)$ is Boolean of rank $\ell \geq 3$ and that $\mathcal{O}_G(H)$ contains a maximal element which is imprimitive. Let $\{G_1, \ldots, G_\ell\}$ be the maximal elements of $\mathcal{O}_G(H)$. Then one of the following holds:*

1. *For every $i \in \{1, \ldots, \ell\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$; moreover, relabeling the index set $\{1, \ldots, \ell\}$ if necessary, $\Sigma_1 < \cdots < \Sigma_\ell$.*
2. *$G = \mathrm{Sym}(\Omega)$. Relabeling the indexed set $\{1, \ldots, \ell\}$ if necessary, $G_\ell = \mathrm{Alt}(\Omega)$, for every $i \in \{1, \ldots, \ell - 1\}$, there exists a non-trivial regular partition Σ_i with $G_i = \mathbf{N}_G(\Sigma_i)$, and $\Sigma_1 < \cdots < \Sigma_{\ell-1}$.*
3. *$G = \mathrm{Alt}(\Omega)$, $|\Omega| = 8$, $\ell = 3$ and the Boolean lattice $\mathcal{O}_G(H)$ is in Figure 3.2.*

Proof. It follows arguing inductively on ℓ; the base case $\ell = 3$ is Theorem 3.3.23. □

3.3.5 Boolean intervals containing a maximal intransitive subgroup

The scope of this section is to gather some information on Boolean lattices $\mathcal{O}_G(H)$ containing a maximal element that is intransitive. Some of the material in this section can be also traced back to the PhD thesis [14].

Hypothesis 3.3.25. Let G be either $\mathrm{Sym}(\Omega)$ or $\mathrm{Alt}(\Omega)$ with $n := |\Omega|$, let Γ be a subset of Ω with $1 \leq |\Gamma| < |\Omega|/2$, let $G_1 := \mathbf{N}_G(\Gamma)$, let G_2 be a maximal subgroup of G and let $H := G_1 \cap G_2$. Assume that $\mathcal{O}_G(H)$ is Boolean of rank 2 with maximal elements G_1 and G_2.

Theorem 3.3.26. *Assume Hypothesis 3.3.25. Then one of the following holds:*

1. *$G = \mathrm{Sym}(\Omega)$ and $G_2 = \mathrm{Alt}(\Omega)$.*

2. *G_2 is an imprimitive subgroup having Γ as a block of imprimitivity.*

3. *$G = \mathrm{Alt}(\Omega)$, $n = 7$, $|\Gamma| = 3$ and $G_2 \cong \mathrm{SL}_3(2)$ acts primitively on Ω.*

4. *$|\Gamma| = 1$ and one of the following holds:*

   (a) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{AGL}_d(2)$ with $d \geq 3$;*

   (b) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{Sp}_{2m}(2)$ and $|\Omega| \in \{2^{m-1}(2^m+1), 2^{m-1}(2^m-1)\}$;*

   (c) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong HS$ and $|\Omega| = 176$;*

   (d) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong Co_3$ and $|\Omega| = 276$;*

   (e) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{M}_{12}$ and $|\Omega| = 12$;*

   (f) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{M}_{24}$ and $|\Omega| = 24$;*

   (g) *$G = \mathrm{Sym}(\Omega)$, $G_2 \cong \mathrm{PGL}_2(p)$ with p prime and $|\Omega| = p+1$;*

   (h) *$G = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{PSL}_2(p)$ with p prime and $|\Omega| = p+1$.*

Proof. Suppose that G_2 is intransitive. Thus $G_2 = G \cap (\mathrm{Sym}(\Gamma') \times \mathrm{Sym}(\Omega \setminus \Gamma'))$, for some subset $\Gamma' \subseteq \Omega$ with $1 \leq |\Gamma'| < |\Omega|/2$. In particular,

$$H = G_1 \cap G_2 = G \cap (\mathrm{Sym}(\Gamma \cap \Gamma') \times \mathrm{Sym}(\Gamma \setminus \Gamma') \times \mathrm{Sym}(\Gamma' \setminus \Gamma) \times \mathrm{Sym}(\Omega \cup (\Gamma \cup \Gamma'))).$$

Thus H is contained in

- $G \cap (\mathrm{Sym}(\Gamma \cap \Gamma') \times \mathrm{Sym}(\Omega \setminus (\Gamma \cap \Gamma')))$,
- $G \cap (\mathrm{Sym}(\Gamma \setminus \Gamma') \times \mathrm{Sym}(\Omega \setminus (\Gamma \setminus \Gamma')))$,
- $G \cap (\mathrm{Sym}(\Gamma' \setminus \Gamma) \times \mathrm{Sym}(\Omega \setminus (\Gamma' \setminus \Gamma)))$,
- $G \cap (\mathrm{Sym}(\Gamma \cup \Gamma') \times \mathrm{Sym}(\Omega \setminus (\Gamma \cup \Gamma')))$.

Since the only overgroups of H are H, G_1, G_2 and G, each of the previous four subgroups must be one of H, G_1, G_2 and G. This immediately implies $G = G \cap (\mathrm{Sym}(\Gamma \cap \Gamma') \times \mathrm{Sym}(\Omega \setminus (\Gamma \cap \Gamma')))$, that is, $\Gamma \cap \Gamma' = \varnothing$. However, $G \cap (\mathrm{Sym}(\Gamma \cup \Gamma') \times \mathrm{Sym}(\Omega \setminus (\Gamma \cup \Gamma')))$ is neither H, nor G_1, nor G_2, nor G, because $1 \leq |\Gamma|, |\Gamma'| < |\Omega|/2$.

Suppose that G_2 is imprimitive. In particular, G_2 is the stabilizer of a non-trivial (a,b)-regular partition of Ω, that is, G_2 is the stabilizer of a partition $\Sigma_2 := \{X_1, \ldots, X_b\}$ of the set Ω into b parts each having cardinality a, for some positive integers a and b with $a, b \geq 2$. Thus

$$G_2 = \mathbf{N}_G(\Sigma_2) \text{ and } \mathbf{N}_{\mathrm{Sym}(\Omega)}(\Sigma_2) \cong \mathrm{Sym}(a) \mathrm{wr}\, \mathrm{Sym}(b).$$

The group $H = G_1 \cap G_2$ is intransitive. Since G_1 is the only proper overgroup of H that is intransitive, we deduce that H has only two orbits on Ω, namely Γ and $\Omega \setminus \Gamma$. From this it follows that, for every $i \in \{1, \ldots, b\}$, either $X_i \subseteq \Gamma$ or $X_i \subseteq \Omega \setminus \Gamma$. Let $\Sigma_2' := \{X \in \Sigma_2 \mid X \subseteq \Gamma\}$ and $\Sigma_2'' := \{X \in \Sigma_2 \mid X \subseteq \Omega \setminus \Gamma\}$. Therefore

$$\begin{aligned} H = G_1 \cap G_2 &= G \cap (\mathbf{N}_{\mathrm{Sym}(\Gamma)}(\Sigma_2') \times \mathbf{N}_{\mathrm{Sym}(\Omega\setminus\Gamma)}(\Sigma_2'')), \\ \mathbf{N}_{\mathrm{Sym}(\Gamma)}(\Sigma_2') &\cong \mathrm{Sym}(a) \mathrm{wr}\, \mathrm{Sym}(b_1), \\ \mathbf{N}_{\mathrm{Sym}(\Omega\setminus\Gamma)}(\Sigma_2'') &\cong \mathrm{Sym}(a) \mathrm{wr}\, \mathrm{Sym}(b_2), \end{aligned}$$

where b_1 is the number of parts in Σ_2' and b_2 is the number of parts in Σ_2''. Therefore, H is contained in subgroups isomorphic to

$$(\dagger) \qquad G \cap (\mathrm{Sym}(\Gamma) \times \mathbf{N}_{\mathrm{Sym}(\Omega\setminus\Gamma)}(\Sigma_2'')) \quad \text{and} \quad G \cap (\mathbf{N}_{\mathrm{Sym}(\Gamma)}(\Sigma_2') \times \mathrm{Sym}(\Omega \setminus \Gamma)).$$

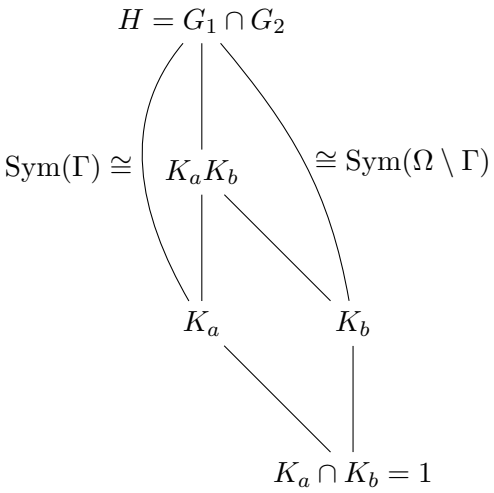

Figure 3.4: Structure of $H = G_1 \cap G_2$

Since H and G_1 are the only intransitive overgroup of H, we deduce that the two subgroups in (†) are H or G_1. However this happens if and only if $b_1 = 1$. In other words, this happens if and only if $\Gamma \in \Sigma_2$ and we obtain part (2).

Suppose that G_2 is primitive. We divide our analysis in various cases.

Case 1: $|\Gamma| \geq 3$, or $|\Gamma| = 2$ and $G = \mathrm{Sym}(\Omega)$.

Now, $H = G_1 \cap G_2$ is a maximal subgroup of G_1. Moreover, $G_1 = \mathrm{Sym}(\Gamma) \times \mathrm{Sym}(\Omega \setminus \Gamma)$ when $G = \mathrm{Sym}(\Omega)$ and $G_1 = \mathrm{Alt}(\Omega) \cap (\mathrm{Sym}(\Gamma) \times \mathrm{Sym}(\Omega \setminus \Gamma))$ when $G = \mathrm{Alt}(\Omega)$. Consider $\pi_a : G_1 \to \mathrm{Sym}(\Gamma)$ and $\pi_b : G_1 \to \mathrm{Sym}(\Omega \setminus \Gamma)$ the natural projections. Oberve that these projections are surjective.

Assume $\pi_a(G_1 \cap G_2)$ is a proper subgroup of $\mathrm{Sym}(\Gamma)$. Then, from the maximality of $G_1 \cap G_2$ in G_1, we have

$$G_1 \cap G_2 = G \cap (\pi_a(G_1 \cap G_2) \times \mathrm{Sym}(\Omega \setminus \Gamma)).$$

As $|\Omega \setminus \Gamma| \geq 3$, we deduce that $G_1 \cap G_2$ contains a 2-cycle or a 3-cycle. In particular, the primitive group G_2 contains a 2-cycle or a 3-cycle. By a celebrated result of Jordan [48, Theorem 3.3A], we obtain $\mathrm{Alt}(\Omega) \leq G_2$. Thus $G = \mathrm{Sym}(\Omega)$ and $G_2 = \mathrm{Alt}(\Omega)$ and we obtain part (1). Suppose then $\pi_a(G_1 \cap G_2) = \mathrm{Sym}(\Gamma)$ and let $K_a := \mathrm{Ker}(\pi_a) \cap G_1 \cap G_2$.

If $\pi_b(G_1 \cap G_2)$ is a proper subgroup of $\mathrm{Sym}(\Omega \setminus \Gamma)$, using the same argument of the previous paragraph we obtain part (1).

Suppose then $\pi_b(G_1 \cap G_2) = \mathrm{Sym}(\Omega \setminus \Gamma)$ and let $K_b := \mathrm{Ker}(\pi_b) \cap G_1 \cap G_2$. In the rest of the proof of this case the reader might find useful to see Figure 3.4.

Now, K_aK_b is a subgroup of $G_1 \cap G_2$, moreover $(G_1 \cap G_2)/(K_aK_b)$ is an epimorphic image of both $\mathrm{Sym}(\Gamma)$ and $\mathrm{Sym}(\Omega \setminus \Gamma)$. Assume $|\Omega \setminus \Gamma| \geq 5$. Then the only epimorphic image of both $\mathrm{Sym}(\Gamma)$ and $\mathrm{Sym}(\Omega \setminus \Gamma)$ is either the identity group or the cyclic group of order 2. Therefore $|G_1 \cap G_2 : K_aK_b| \leq 2$. Moreover, $K_aK_b/K_b \cong K_a/(K_a \cap K_b) = K_a$ is isomorphic to either $\mathrm{Alt}(\Omega \setminus \Gamma)$ or to $\mathrm{Sym}(\Omega \setminus \Gamma)$. In both cases, $\mathrm{Alt}(\Omega \setminus \Gamma) \leq K_a \leq G_2$ and hence G_2 contains a 3-cycle. As above, this implies $G = \mathrm{Sym}(\Omega)$ and $G_2 = \mathrm{Alt}(\Omega)$ and part (1) holds. Assume $|\Omega \setminus \Gamma| \leq 4$. As $1 \leq |\Gamma| < |\Omega|/2$, we deduce $|\Omega| \leq 7$. When $|\Gamma| = 3$, we obtain $|\Omega| = 7$ and we can verify with a direct analysis that part (1) holds when $G = \mathrm{Sym}(\Omega)$ and part (3) holds when $G = \mathrm{Alt}(\Omega)$. Finally, if $|\Gamma| = 2$, we have $|\Omega| \in \{5, 6\}$ and $G = \mathrm{Sym}(\Omega)$. A direct inspection in each of these cases reveals that every maximal subgroup of G_1 contains either a 2-cycle or a 3-cycles. Therefore $G_2 = \mathrm{Alt}(\Omega)$ and part (1) holds.

Case 2: $|\Gamma| = 2$ and $G = \mathrm{Alt}(\Omega)$.

In this case, $G_1 = \mathrm{Alt}(\Omega) \cap (\mathrm{Sym}(\Gamma) \times \mathrm{Sym}(\Omega \setminus \Gamma)) \cong \mathrm{Sym}(\Omega \setminus \Gamma)$.

Assume that $H = G_1 \cap G_2$ acts intransitively on $\Omega \setminus \Gamma$ and let Δ be one of its smallest orbits. In particular, H fixes setwise Γ, Δ and $\Omega \setminus (\Gamma \cup \Delta)$. Now, $\mathrm{Alt}(\Omega) \cap (\mathrm{Sym}(\Gamma \cup \Delta) \times \mathrm{Sym}(\Omega \setminus (\Gamma \cup \Delta)))$ is a proper overgroup of H which is intransitive and is different from G_1, which is a contradiction. Therefore H acts transitively on $\Omega \setminus \Gamma$. Suppose that H acts imprimitively on $\Omega \setminus \Gamma$. Since H is maximal in $G_1 \cong \mathrm{Sym}(\Omega \setminus \Gamma)$, we deduce $H = \mathbf{N}_{G_1}(\Sigma)$, where Σ is a non-trivial (a, b)-regular partition of $\Omega \setminus \Gamma$. If $a \geq 3$, then H contains a 3-cycle and hence so does G_2. Since G_2 is primitive, we deduce from [48, Theorem 3.3A] that $G_2 = \mathrm{Alt}(\Omega) = G$, which is a contradiction. If $a = 2$, then H contains a permutation that is the product of two disjoint transpositions. Since G_2 is primitive, we deduce from [48, Theorem 3.3D and Example 3.3.1] that either $G_2 = \mathrm{Alt}(\Omega) = G$ or $|\Omega| \leq 8$. The first possibility is clearly impossible and hence $|\Omega| \in \{6, 8\}$. However, a computation in $\mathrm{Alt}(6)$ and in $\mathrm{Alt}(8)$ reveals that no case arises. Therefore H acts primitively on $\Omega \setminus \Gamma$.

Let $\Gamma = \{\gamma, \gamma'\}$. As $|\Gamma| = 2$, the group $(G_1 \cap G_2)_\gamma = H_\gamma$ has index at most 2 in $G_1 \cap G_2 = H$ and hence $H_\gamma \trianglelefteq H$. Since H acts primitively on $\Omega \setminus \Gamma$ and $H_\gamma \trianglelefteq H$, H_γ acts transitively on $\Omega \setminus \Gamma$ or H_γ is trivial. The second possibility is clearly a contradiction because it implies $|H| = 2$ and hence $|\Omega| = 4$. Thus H_γ acts transitively on $\Omega \setminus \Gamma$ and the orbits of H_γ on Ω are $\{\gamma\}, \{\gamma'\}, \Omega \setminus \Gamma$ and have cardinality $1, 1, |\Omega| - 2$. Since G_2 is primitive and not regular, from Lemma 3.3.9, we deduce that γ is the only fixed point of $(G_2)_\gamma$. Since H_γ is a subgroup of $(G_2)_\gamma$ from the cardinality of the orbits of H_γ, we deduce that $(G_2)_\gamma$ acts transitively on $\Omega \setminus \{\gamma\}$, that is, G_2 is 2-transitive. Similarly, since $H_\gamma \leq (G_2)_\gamma \cap (G_2)_{\gamma'}$, we deduce also that G_2 is 3-transitive.

From the classification of the finite 3-transitive groups, we deduce that

1. G_2 equals the Mathieu group M_n and $n = |\Omega| \in \{11, 12, 22, 23, 24\}$, or
2. $G_2 = M_{11}$ and $|\Omega| = 12$, or
3. $\mathbf{F}^*(G_2) = \mathrm{PSL}_2(q)$ and $|\Omega| = q + 1$.

Using this information, a computation with the computer algebra system MAGMA shows that the cases (1) and (2) do not arise because $\mathcal{O}_G(H)$ is not Boolean of rank 2. In case (3), from the structure of $\mathrm{PSL}_2(q)$, we deduce that $G_1 \cap G_2$ is solvable and hence $G_1 \cap G_2$ is a solvable group acting primitively on $|\Omega| - 2$ points. This yields that $q - 1$ is a prime power, say $q - 1 = x^y$, for some prime x and for some positive integer y. Write $q = p^f$, for some prime power p and some positive integer f. Since $p^f - 1$ is a power of a prime, we deduce that $p^f - 1$ has no primitive prime divisors. Zsigmondy's theorem 1.3.2 yields

(a) $f = 1$, $x = 2$ and $q - 1 = 2^y$, or

(b) $q = 9$, $x = 2$ and $y = 3$ or

(c) $p = 2$, f is prime and $q - 1 = 2^f - 1 = x$ is a prime.

We can now refine further our argument above. Indeed, recall that $G_1 \cap G_2$ is a maximal subgroup of $G_1 \cong \mathrm{Sym}(\Omega \setminus \Gamma)$. Since $G_1 \cap G_2$ is solvable, we deduce that $G_1 \cap G_2$ is isomorphic to the general linear group $\mathrm{AGL}_y(x)$ and hence $|G_1 \cap G_2| = x^y |\mathrm{GL}_y(x)| = (q - 1)|\mathrm{GL}_y(x)|$. Since $G_2 = \mathbf{N}_{\mathrm{Alt}(q+1)}(\mathrm{PSL}_2(q))$ and $|\mathrm{Aut}(\mathrm{PSL}_2(q))| = fq(q^2 - 1)$, we deduce that $|G_1 \cap G_2|$ divides $2f(q - 1)$. Therefore $|\mathrm{GL}_y(x)|$ divides $2f$. Cases **(a)** and **(b)** are readily seen to be impossible and in case **(c)** we have $|\mathrm{GL}_1(x)| = 2^f - 2 = 2(2^{f-1} - 1)$ divides $2f$, which is possible only when $f = 3$. A computation reveals that in this latter case $\mathcal{O}_G(H)$ has 5 elements and hence it is not Boolean.

Case 3: $|\Gamma| = 1$.

We assume that the conclusion in part (1) of this lemma does not hold and hence G_2 is a primitive subgroup of G with $\mathrm{Alt}(\Omega) \not\leq G_2$.

Assume that $H = G_1 \cap G_2$ acts intransitively on $\Omega \setminus \Gamma$ and let Δ be one of its smallest orbits. In particular, H fixes setwise Γ, Δ and $\Omega \setminus (\Gamma \cup \Delta)$. Now, $\mathrm{Alt}(\Omega) \cap (\mathrm{Sym}(\Gamma \cup \Delta) \times \mathrm{Sym}(\Omega \setminus (\Gamma \cup \Delta)))$ is a proper overgroup of H which is intransitive and is different from G_1, which is a contradiction. Therefore H acts transitively on $\Omega \setminus \Gamma$. Suppose that H acts imprimitively on $\Omega \setminus \Gamma$. Since H is maximal in $G_1 \cong \mathrm{Sym}(\Omega \setminus \Gamma)$, we deduce $H = \mathbf{N}_{G_1}(\Sigma)$, where Σ is a non-trivial (a, b)-regular partition of $\Omega \setminus \Gamma$. If $a \geq 3$, then H contains a 3-cycle and hence so does G_2. Since G_2 is primitive, we deduce from [48, Theorem 3.3A] that $\mathrm{Alt}(\Omega) \leq G_2$, which is a contradiction. If $a = 2$, then H contains a permutation that is the product of two disjoint transpositions. Since G_2 is primitive, we deduce from [48, Theorem 3.3D and Example 3.3.1] that either $\mathrm{Alt}(\Omega) \leq G_2$ or $|\Omega| \leq 8$. The first possibility is clearly impossible. In the second case, as $a = 2$, we have that $|\Omega \setminus \Gamma|$ is even and hence $|\Omega| \in \{5, 7\}$. However, a computation in Alt(5), Sym(5), Alt(7) and Sym(7) reveals that no case arises. Therefore

$$H \text{ acts primitively on } \Omega \setminus \Gamma.$$

In particular, G_2 is 2-transitive on Ω. One of the first main applications on the Classification of the Finite Simple Groups is the classification of the finite 2-transitive groups, see [32]. These groups are either affine or almost simple. For the rest of the proof we go through this classification to investigate G_2 further; we assume that the reader is broadly familiar with this classification and for this part we refer the reader to Section 7.7 in [48].

Case 3A: G_2 is affine.

Since G_2 is a maximal subgroup of G, we deduce that $G_2 \cong G \cap \mathrm{AGL}_d(p)$, for some prime number p and some positive integer d. Now, $G_1 \cap G_2 \cong G \cap \mathrm{GL}_d(p)$ and the action of $G_1 \cap G_2$ on $\Omega \setminus \Gamma$ is permutation isomorphic to the natural action of a certain subgroup of index at most 2 of the linear group $\mathrm{GL}_d(p)$ acting on the non-zero vectors of a d-dimensional vector space over the field with p-elements. Clearly, this action is primitive if and only if $d = 1$ and $p - 1$ is prime, or $p = 2$. Indeed, if V is the d-dimensional vector space over the field $\mathbb{F}_p$ with p elements, then $\mathrm{GL}_d(p)$ preserves the partition $\{\{av \mid a \in \mathbb{F}_p, a \neq 0\} \mid v \in V, v \neq 0\}$ of $V \setminus \{0\}$. This partition is the trivial partition only when $p = 2$ or $d = 1$. When $d = 1$, the group $\mathrm{GL}_1(p)$ is cyclic of order $p - 1$ and it acts primitively on $V \setminus \{0\}$ if and only if $p - 1$ is a prime number. Since the only two consecutive primes are 2 and 3, in the latter case we obtain $|\Omega| = 3$ and no case arises here. Thus $p = 2$.

If $d \leq 2$, then $\mathrm{Alt}(\Omega) \leq G_2$, which is a contradiction. Therefore $d \geq 3$. With a computation (using the fact that $\mathrm{GL}_d(2)$ is generated by transvectoins for example) we see that, when $d \geq 3$, the group $\mathrm{AGL}_d(2)$ consists of even permutations and hence $\mathrm{AGL}_d(2) \leq \mathrm{Alt}(\Omega)$. This implies $G = \mathrm{Alt}(\Omega)$ and we obtain one of the examples stated in the theorem, namely part (4) **(a)**.

Case 3B: $G_2 \cong \mathrm{Sp}_{2m}(2)$ and $|\Omega| = 2^{m-1}(2^m + 1)$ or $|\Omega| = 2^{m-1}(2^m - 1)$.

The group $G_1 \cap G_2$ is isomorphic to either $\mathrm{O}^+_{2m}(2)$ or to $\mathrm{O}^-_{2m}(2)$ depending on whether $|\Omega| = 2^{m-1}(2^m+1)$ or $|\Omega| = 2^{m-1}(2^m-1)$. Since G_2 is a simple group, we deduce $G_2 \leq \mathrm{Alt}(\Omega)$ and hence $G = \mathrm{Alt}(\Omega)$. We obtain part (4) **(b)**.

Case 3C: $\mathbf{F}^*(G_2) \cong \mathrm{PSU}_3(q)$ and $|\Omega| = q^3 + 1$.

Let $q = p^f$, for some prime number p and for some positive integer f. Observe that $G_1 \cap G_2$ is solvable, it is a maximal subgroup of G_1 and it acts primitively on $\Omega \setminus \Gamma$. From this we deduce that $G_1 \cap G_2$ is isomorphic to $G \cap \mathrm{AGL}_{3f}(p)$. Since $|\mathrm{Aut}(\mathrm{PSU}_3(q))| = 2f(q^3 + 1)q^3(q^2 - 1)$ and $|\Omega| = q^3 + 1$, we deduce that $G_1 \cap G_2$ has order a divisor of $2fq^3(q^2 - 1)$. Therefore $|\mathrm{AGL}_{3f}(p)| = q^3|\mathrm{GL}_{3f}(p)|$ divides $4fq^3(q^2-1)$ (observe that the extra "2" in front of $2fq^3(q^2-1)$ takes in account the case that $G = \mathrm{Alt}(\Omega)$ and $G \cap \mathrm{AGL}_{3f}(p)$ has index 2 in $\mathrm{AGL}_{3f}(p)$). Therefore $|\mathrm{GL}_{3f}(p)|$ divides $4f(q^2 - 1)$. However the inequality $|\mathrm{GL}_{3f}(p)| \leq 4f(p^{2f} - 1)$ is never satisfied.

Case 3D: $\mathbf{F}^*(G_2) \cong \mathrm{Sz}(q)$, $q = 2^f$ for some odd positive integer $f \geq 3$ and $|\Omega| = q^2 + 1$.

Since $\mathrm{Aut}(\mathrm{Sz}(q)) \cong \mathrm{Sz}(q).f$ and since f is odd, we deduce $G_2 \leq \mathrm{Alt}(\Omega)$. In particular, $G = \mathrm{Alt}(\Omega)$. As in the case above, $G_1 \cap G_2$ is solvable, $G_1 \cap G_2$ is a maximal subgroup of G_1 and $G_1 \cap G_2$ acts primitively on $\Omega \setminus \Gamma$. From this we deduce that $G_1 \cap G_2$ is isomorphic to $G \cap \mathrm{AGL}_{2f}(2)$. Since $|\mathrm{Aut}(\mathrm{Sz}(q))| = f(q^2+1)q^2(q-1)$ and $|\Omega| = q^2+1$, we deduce that $G_1 \cap G_2$ has order a divisor of $fq^2(q-1)$. Therefore $|\mathrm{AGL}_{2f}(2)| = q^2|\mathrm{GL}_{2f}(2)|$ divides $4fq^2(q-1)$. Therefore $|\mathrm{GL}_{2f}(2)|$ divides $4f(q-1)$. However the inequality $|\mathrm{GL}_{2f}(2)| \leq 4f(2^f-1)$ is never satisfied.

Case 3E: $\mathbf{F}^*(G_2) \cong \mathrm{Ree}(q)$, $q = 3^f$ for some odd positive integer $f \geq 1$ and $|\Omega| = q^3+1$.

Since $\mathrm{Aut}(\mathrm{Ree}(q)) \cong \mathrm{Ree}(q).f$ and since f is odd, we deduce $G_2 \leq \mathrm{Alt}(\Omega)$. In particular, $G = \mathrm{Alt}(\Omega)$. As in the case above, $G_1 \cap G_2$ is solvable, $G_1 \cap G_2$ is a maximal subgroup of G_1 and $G_1 \cap G_2$ acts primitively on $\Omega \setminus \Gamma$. From this we deduce that $G_1 \cap G_2$ is isomorphic to $G \cap \mathrm{AGL}_{3f}(3)$. Since $|\mathrm{Aut}(\mathrm{Ree}(q))| = f(q^3+1)q^3(q-1)$ and $|\Omega| = q^3+1$, we deduce that $G_1 \cap G_2$ has order a divisor of $fq^3(q-1)$. Therefore $|\mathrm{AGL}_{3f}(3)| = q^3|\mathrm{GL}_{3f}(3)|$ divides $4fq^3(q-1)$. Therefore $|\mathrm{GL}_{3f}(3)|$ divides $4f(q-1)$. However the inequality $|\mathrm{GL}_{3f}(3)| \leq 4f(3^f-1)$ is never satisfied.

Case 3F: $(G_2, |\Omega|) \in \{(HS, 176), (Co_3, 276), (\mathrm{Alt}(7), 15), (\mathrm{PSL}_2(11), 11), (M_{11}, 12)\}$.

Since $\mathrm{PSL}_2(11) < M_{11}$ in their degree 11 actions, $\mathrm{Alt}(7) < \mathrm{PSL}_4(2)$ in their degree 15 actions and $M_{11} < M_{12}$ in their degree 12 actions, we see that $\mathrm{PSL}_2(11)$, $\mathrm{Alt}(7)$ and M_{12} are not maximal in G and hence cannot be G_2. Therefore, we are left with $(G_2, |\Omega|) \in \{(HS, 176), (Co_3, 276)\}$. We obtain part (4) **(c)** and **(d)**.

Case 3G: $(G_2, |\Omega|) \in \{(\mathrm{M}_{11}, 11), (\mathrm{M}_{12}, 12), (\mathrm{M}_{22}, 22), (\mathrm{M}_{22}.2, 22), (\mathrm{M}_{23}, 23), (\mathrm{M}_{24}, 24)\}$.

With a computer computation we see that when $G_2 \cong M_{11}$ the lattice $\mathcal{O}_G(H)$ is not Boolean. The cases M_{22} and $M_{22}.2$ do not arise because in these two cases $G_1 \cap G_2$ is isomorphic to either $\mathrm{PSL}_3(4)$ (when $G = \mathrm{Alt}(\Omega)$) or to $\mathrm{P\Sigma L}_3(4)$ (when $G = \mathrm{Sym}(\Omega)$). However, these two groups are not maximal subgroups of G_1 because they are contained respectively in $\mathrm{PGL}_3(4)$ and in $\mathrm{P\Gamma L}_3(4)$. Therefore, we are left with $(G_2, |\Omega|) \in \{(\mathrm{M}_{12}, 12), (\mathrm{M}_{23}, 23), (\mathrm{M}_{24}, 24)\}$. The case $(G_2, |\Omega|) = (\mathrm{M}_{23}, 23)$ also does not arise because with a computation we see that $\mathcal{O}_G(H)$ consists of five elements. Thus we are only left with part (4) **(e)** and **(f)**.

Case 3I: $\mathbf{F}^*(G_2) \cong \mathrm{PSL}_d(q)$ for some prime power q and some positive integer $d \geq 2$ and $|\Omega| = (q^d-1)/(q-1)$.

Since the group G_2 is acting on the points of a $(d-1)$-dimensional projective space, we deduce that $G_1 \cap G_2$ acts primitively on $\Omega \setminus \Gamma$ only when G_2 is acting on the projective line, that is, $d = 2$. (Indeed, consider the action of $X := \mathrm{P\Gamma L}_d(q)$ on the points of the projective space $\mathcal{P}$, consider a point p of $\mathcal{P}$ and consider the stabilizer Y of the point p in X. Then Y preserves a natural partition on $\mathcal{P} \setminus \{p\}$, where two points p_1 and p_2 are declared to be in the same part if the lines $\langle p, p_1\rangle$ and $\langle p, p_2\rangle$ are equal. This partition is trivial only when $\mathcal{P}$ is a line, that is, $d = 2$.) Let $q = p^f$, for some prime number p and for some positive integer f. Observe that $G_1 \cap G_2$ is solvable, it is a maximal subgroup of G_1 and it acts primitively on $\Omega \setminus \Gamma$. From this we deduce that $G_1 \cap G_2$ is isomorphic to $G \cap \mathrm{AGL}_f(p)$. Since $|\mathrm{Aut}(\mathrm{PSL}_2(q))| = f(q^2-1)q$ and $|\Omega| = q+1$, we deduce that $G_1 \cap G_2$ has order a divisor of $f(q-1)q$. Therefore $|\mathrm{AGL}_f(p)| = q|\mathrm{GL}_f(p)|$ divides $2f(q-1)q$ (observe that the extra "2" in front of $fq(q-1)$ takes in account the case that $G = \mathrm{Alt}(\Omega)$ and $G \cap \mathrm{AGL}_f(p)$ has index 2 in $\mathrm{AGL}_f(p)$). Therefore $|\mathrm{GL}_f(p)|$ divides $2f(q-1)$. The inequality $|\mathrm{GL}_f(p)| \leq 2f(p^f-1)$ is satisfied only when $f = 1$ or $p = f = 2$. When $p = f = 2$, we have $|\Omega| = 5$ and hence $G_2 = \mathrm{Alt}(\Omega)$, which is not the case. Thus $q = p$ and $f = 1$. In particular, $\mathbf{F}^*(G_2) = \mathrm{PSL}_2(p)$, for some prime number p. Now, we obtain part **(g)** and **(h)** depending on whether $G = \mathrm{Sym}(\Omega)$ or $G = \mathrm{Alt}(\Omega)$. □

Hypothesis 3.3.27. Let G be either $\mathrm{Sym}(\Omega)$ or $\mathrm{Alt}(\Omega)$, let Γ be a subset of Ω with $1 \leq |\Gamma| < |\Omega|/2$, let $G_1 := \mathbf{N}_G(\Gamma)$, let G_2 and G_3 be maximal subgroups of G and let $H := G_1 \cap G_2 \cap G_3$. Assume that $\mathcal{O}_G(H)$ is Boolean of rank 3 with maximal elements G_1, G_2 and G_3.

Theorem 3.3.28. *Assume Hypothesis 3.3.27. Then, relabeling the indexed set* $\{1,2,3\}$ *if necessary, one of the following holds:*

1. $G = \mathrm{Sym}(\Omega)$, G_2 *is an imprimitive group having* Γ *as a block of imprimitivity and* $G_3 = \mathrm{Alt}(\Omega)$.
2. $G = \mathrm{Sym}(\Omega)$, $|\Gamma| = 1$, $G_3 = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{PGL}_2(p)$ *for some prime* p *and* $|\Omega| = p+1$.
3. $G = \mathrm{Alt}(\Omega)$, $|\Gamma| = 1$, $G_2 \cong G_3 \cong \mathrm{M}_{24}$ *and* $|\Omega| = 24$.

Proof. A computation shows that the largest Boolean lattice in $\mathrm{Alt}(\Omega)$ when $|\Omega| = 7$ has rank 2. Hence, in the rest of our argument we suppose that $|\Omega| \neq 7$; in particular, part (3) in Theorem 3.3.26 does not arise.

We apply Theorem 3.3.26 to the pairs $\{G_1, G_2\}$ and $\{G_1, G_3\}$. Relabeling the indexed set $\{2,3\}$ if necessary, we have to consider in turn each of the following cases:

case A G_2 and G_3 are imprimitive (hence G_2 and G_3 are stabilizers of non-trivial regular partitions having Γ as one block);

case B G_2 is imprimitive and G_3 is primitive;

case C G_2 and G_3 are primitive.

Case A: Since $\mathcal{O}_G(G_2 \cap G_3)$ is Boolean of rank 2, from Lemma 3.3.6, we deduce that either $G_2 \cap G_3$ is transitive or G_2 or G_3 is the stabilizer of a $(|\Omega|/2, 2)$-regular partition. As $|\Gamma| \neq |\Omega|/2$, we deduce that $G_2 \cap G_3$ is transitive. Therefore, we are in the position to apply Theorem 3.3.21 to the pair $\{G_2, G_3\}$. However, none of the possibilities there can arise here because both G_2 and G_3 have Γ as a block of imprimitivity and $1 \leq |\Gamma| < |\Omega|/2$.

Case B: From Theorem 3.3.26, we have that Γ is a block of imprimitivity for G_2. If $G_3 = \mathrm{Alt}(\Omega)$, then we obtain (1). Suppose then $G_3 \neq \mathrm{Alt}(\Omega)$. As $|\Gamma| \neq |\Omega|/2$, Lemma 3.3.6 implies that $G_2 \cap G_3$ is transitive and hence we may apply Theorem 3.3.21 to the pair $\{G_2, G_3\}$. In particular, Theorem 3.3.21 part (2) holds and hence G_3 is an affine primitive group and G_2 is the stabilizer of a $(n/2, 2)$-regular partition. Thus $|\Gamma| = |\Omega|/2$, which is a contradiction.

Case C: Suppose that either G_2 or G_3 equals $\mathrm{Alt}(\Omega)$. Relabeling the indexed set $\{2,3\}$ if necessary, we may suppose that $G_3 = \mathrm{Alt}(\Omega)$. In particular, $G = \mathrm{Sym}(\Omega)$. Now, Theorem 3.3.26 implies that $|\Gamma| = 1$, $G_2 \cong \mathrm{PGL}_2(p)$ for some prime p and $|\Omega| = p+1$. Therefore, we obtain (2).

It remains to consider the case that G_2 and G_3 are both primitive and both different from $\mathrm{Alt}(\Omega)$. As $|\Omega| \neq 7$, Theorem 3.3.26 implies that $|\Gamma| = 1$, G_2 and G_3 are one of the groups described in part (4). Now, $G_1 \cong \mathrm{Sym}(\Omega \setminus \Gamma)$ or $G_1 \cong \mathrm{Alt}(\Omega \setminus \Gamma)$, depending on whether $G = \mathrm{Sym}(\Omega)$ or $G = \mathrm{Alt}(\Omega)$. Moreover, $\mathcal{O}_G(G_2 \cap G_3)$ is a Boolean lattice of rank 2 having G_2 and G_3 as maximal elements. From Lemma 3.3.7, we deduce that either $G_2 \cap G_3$ acts primitively on Ω, or $G = \mathrm{Alt}(\Omega)$, $G_2 \cap G_3 = \mathbf{N}_G(\Sigma)$ for some $(2,4)$-regular partition Σ. In the latter case, we see with a computation that the lattice $\mathcal{O}_G(G_1 \cap G_2 \cap G_3)$ is not Boolean (see also Figure 3.2). Therefore

$$G_2 \cap G_3 \text{ acts primitively on } \Omega.$$

Consider then $H := G_1 \cap G_2 \cap G_3$ and suppose that H is intransitive on $\Omega \setminus \Gamma$. Since $|\Omega \setminus \Gamma| = |\Omega| - 1$, H has an orbit $\Delta \subseteq \Omega \setminus \Gamma$ with $1 \leq |\Delta| < |\Omega|/2$. Then $\mathbf{N}_G(\Delta) \in \mathcal{O}_G(H)$ and $\mathbf{N}_G(\Delta)$ is a maximal element of $\mathcal{O}_G(H)$, contradicting the fact that G_1 is the only intransitive element in $\mathcal{O}_G(H)$. Thus H is transitive on $\Omega \setminus \Gamma$. Therefore

$$G_2 \cap G_3 \text{ acts 2-transitively on } \Omega. \tag{3.3.3}$$

Suppose that G_2 is as in Theorem 3.3.26 (4) **(a)**, that is, $G_2 \cong \mathrm{AGL}_d(2)$ for some $d \geq 3$. Let V_2 be the socle of G_2. From Lemma 3.3.15 applied with applied with H there replaced by $G_2 \cap G_3$ here , we have either $V_2 \leq G_2 \cap G_3$ or $|\Omega| = 8$, $G = \mathrm{Alt}(\Omega)$ and $G_2 \cap G_3 \cong \mathrm{PSL}_2(7)$. In the second case, $G_1 \cap G_2 \cap G_3 \cong C_7 \rtimes C_3$; however, a computation yields that $\mathcal{O}_{\mathrm{Alt}(8)}(C_7 \rtimes C_3)$ is not Boolean of rank 3. Therefore, $V_2 \leq G_2 \cap G_3$. The only primitive groups in Theorem 3.3.26 (4) with $|\Omega|$ a power of a prime are $\mathrm{AGL}_d(2)$ or $\mathrm{PSL}_2(p)$ when $p+1 = 2^d$. In particular, either $G_3 \cong \mathrm{AGL}_d(2)$, or $G_3 \cong \mathrm{PSL}_2(p)$ and $p+1 = 2^d$. In the second case, since the elementary abelian 2-group V_2 is contained in $G_2 \cap G_3$, we deduce that $\mathrm{PSL}_2(p)$ contains an elementary abelian 2-group of order 2^d, which is impossible. Therefore, $G_3 \cong \mathrm{AGL}_d(2)$. Let V_3 be the socle of G_3. From Lemma 3.3.15, we deduce $V_3 \leq G_2 \cap G_3$. In particular, $V_2 \trianglelefteq G_2 \cap G_3$ and $V_3 \trianglelefteq G_2 \cap G_3$. Since $G_2 \cap G_3$ is primitive, we infer $V_2 = V_3$ and hence $G_2 = \mathbf{N}_G(V_2) = \mathbf{N}_G(V_3) = G_3$, which is a contradiction.

Suppose that G_2 is as in Theorem 3.3.26 (4) **(b)**, that is, $G_2 \cong \mathrm{Sp}_{2m}(2)$. To deal with both actions simultaneously we set $\Omega^+ := \Omega$ when $|\Omega| = 2^{m-1}(2^m+1)$ and $\Omega^- := \Omega$ when $|\Omega| = 2^{m-1}(2^m-1)$. We can read off from [95, Table 1], the maximal subgroups of G_2 transitive on either Ω^+ or Ω^- (this is our putative $G_2 \cap G_3$). Comparing these candidates with the list of 2-transitive groups, we see that none of these groups is 2-transitive, contradicting (3.3.3).

Suppose that G_2 is as in Theorem 3.3.26 (4) **(c)**, that is, $G_2 \cong HS$. The only maximal subgroup of G_2 primitive on Ω is M_{22} in its degree 176 action. Thus $G_2 \cap G_3 \cong M_{22}$ in its degree 176 action. However, this action is not 2-transitive, contradicting (3.3.3).

Suppose that G_2 is as in Theorem 3.3.26 (4) **(d)**, that is, $G_2 \cong Co_3$. From [95, Table 6], we see that Co_3 has no proper subgroup acting primitively on Ω. Therefore this case does not arise in our investigation.

Suppose that G_2 is as in Theorem 3.3.26 (4) **(e)**, that is, $G_2 \cong M_{12}$. In particular, $G_1 \cap G_2 \cong M_{11}$. Up to conjugacy, there are five maximal subgroups of M_{11} (see [40]): one of them is our putative $G_1 \cap G_2 \cap G_3$. For each of these five subgroups, with the help of a computer, we have computed the orbits on Ω. Observe that one of this orbit is Γ. If $G_1 \cap G_2 \cap G_3$ was intransitive on $\Omega \setminus \Gamma$, then $\mathcal{O}_G(H)$ contains a maximal intransitive subgroup which is not G_1, contradicting our assumptions. Among the five choices, there is only one (isomorphic to $\mathrm{PSL}_2(11)$) which is transitive on $\Omega \setminus \Gamma$. Thus $G_1 \cap G_2 \cap G_3 \cong \mathrm{PSL}_2(11)$. Next, we have computed $\mathcal{O}_{\mathrm{Alt}(12)}(\mathrm{PSL}_2(11))$ and we have checked that it is not Boolean (it is a lattice of size 6).

Suppose that G_2 is as in Theorem 3.3.26 (4) **(f)**, that is, $G_2 \cong M_{24}$. The only maximal subgroup of M_{24} acting primitively is $\mathrm{PSL}_2(23)$. Thus $G_2 \cap G_3 \cong \mathrm{PSL}_2(23)$, and $G_1 \cap G_2 \cap G_3 \cong C_{23} \rtimes C_{11}$. Now, $\mathcal{O}_{G_1}(G_1 \cap G_2 \cap G_3) \cong \mathcal{O}_{\mathrm{Alt}(23)}(C_{23} \rtimes C_{11})$. Since $\mathcal{O}_{G_1}(G_1 \cap G_2 \cap G_3)$ is Boolean of rank 2, so is $\mathcal{O}_{\mathrm{Alt}(23)}(C_{23} \rtimes C_{11})$. We have checked with the help with a computer that $\mathcal{O}_{\mathrm{Alt}(24)}(C_{23} \rtimes C_{11})$ is Boolean of rank 3 and this gives rise to the marvellous example in (3).

Using the subgroup structure of $\mathrm{PSL}_2(p)$ and $\mathrm{PGL}_2(p)$ with p prime, we see that $\mathrm{PSL}_2(p)$ does not contain a proper subgroup acting primitively on the $p+1$ points of the projective line, whereas the only proper primitive subgroup of $\mathrm{PGL}_2(p)$ acting primitively on the projective line is $\mathrm{PSL}_2(p)$. Thus part (4) **(h)** in Theorem 3.3.26 does not arise and if part (4) **(g)** in Theorem 3.3.26 does arise, then $G_2 \cap G_3 \cong \mathrm{PSL}_2(p)$. However this is impossible because this implies that $G_2 \cap G_3 \leq \mathrm{Alt}(\Omega)$ and hence $\mathrm{Alt}(\Omega)$ must be a maximal element of $\mathcal{O}_G(H)$, but we have dealt with this situation already. □

Corollary 3.3.29. *Let H be a subgroup of G and suppose that $\mathcal{O}_G(H)$ is Boolean of rank $\ell \geq 3$ and that $\mathcal{O}_G(H)$ contains a maximal element which is intransitive. Then $\ell = 3$; moreover, relabeling the indexed set $\{1,2,3\}$ if necessary, $G_1 = \mathbf{N}_G(\Gamma)$ for some $\Gamma \subseteq \Omega$ with $1 \leq |\Gamma| < |\Omega|/2$ and one of the following holds:*

1. $G = \mathrm{Sym}(\Omega)$, G_2 *is an imprimitive group having* Γ *as a block of imprimitivity and* $G_3 = \mathrm{Alt}(\Omega)$.
2. $G = \mathrm{Sym}(\Omega)$, $|\Gamma| = 1$, $G_3 = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{PGL}_2(p)$ *for some prime* p *and* $|\Omega| = p + 1$.
3. $G = \mathrm{Alt}(\Omega)$, $|\Gamma| = 1$, $G_2 \cong G_3 \cong M_{24}$ *and* $|\Omega| = 24$.

Proof. Let $G_1, G_2, \ldots, G_\ell$ be the maximal elements of $\mathcal{O}_G(H)$. Relabeling the indexed set if necessary, we may suppose that $G_1 = \mathbf{N}_G(\Gamma)$, for some $\Gamma \subseteq \Omega$ with $1 \leq |\Gamma| < |\Omega|/2$. From Theorem 3.3.28 applied to $\mathcal{O}_G(G_1 \cap G_2 \cap G_3)$, we obtain that G_1, G_2, G_3 satisfy one of the cases listed there. We consider these cases in turn. Suppose $G_3 = \mathrm{Alt}(\Omega)$ and G_2 is an imprimitive group having Γ as a block of imprimitivity. If $\ell \geq 4$, then we may apply Theorem 3.3.28 to $\{G_1, G_2, G_4\}$ and we deduce that $G_4 = \mathrm{Alt}(\Omega) = G_3$, which is a contradiction. Suppose then $|\Gamma| = 1$, $G_3 = \mathrm{Alt}(\Omega)$, $G_2 \cong \mathrm{PGL}_2(p)$ for some prime p and $|\Omega| = p + 1$. If $\ell \geq 4$, then we may apply Theorem 3.3.28 to $\{G_1, G_2, G_4\}$ and we deduce that $G_4 = \mathrm{Alt}(\Omega) = G_3$, which is a contradiction.

Finally, suppose that $G = \mathrm{Alt}(\Omega)$, $|\Omega| = 24$, $|\Gamma| = 1$, $G_2 \cong G_2 \cong M_{24}$. If $\ell \geq 4$, then we may apply Theorem 3.3.28 to $\{G_1, G_2, G_4\}$ and we deduce that $G_4 \cong M_{24}$. In particular, $\mathcal{O}_{G_1}(G_1 \cap G_2 \cap G_3 \cap G_4)$ is a Boolean lattice of rank 3 having three maximal subgroups $G_1 \cap G_2, G_1 \cap G_3, G_1 \cap G_4$ all isomorphic to M_{23}. Arguing as usual $G_1 \cap G_2 \cap G_3 \cap G_4$ acts transitively on $\Omega \setminus \Gamma$. Therefore, M_{23} has a chain $M_{23} > A > B > C$ with C maximal in B, B maximal in A, A maximal in M_{23}, with C transitive. However, there is no such a chain. □

3.3.6 Proof of Theorem 3.0.5

We use the notation and the terminology in the statement of Theorem 3.0.5. If, for some $i \in \{1, \ldots, \ell\}$, G_i is intransitive, then the proof follows from Corollary 3.3.29. In particular, we may assume that G_i is transitive, for every $i \in \{1, \ldots, \ell\}$. If, for some $i \in \{1, \ldots, \ell\}$, G_i is imprimitive, then the proof follows from Corollary 3.3.24. In particular, we may assume that G_i is primitive, for every $i \in \{1, \ldots, \ell\}$. Now, the proof follows from Corollary 3.3.19.

3.3.7 Large Boolean lattices arising from imprimitive maximal subgroups

In this section, we prove that G admits Boolean lattices $\mathcal{O}_G(H)$ of arbitrarily large rank, arising from Theorem 3.0.5 part (1). Let ℓ be a positive integer with $\ell \geq 2$ and let $\Sigma_1, \ldots, \Sigma_\ell$ be a family of non-trivial regular partitions of Ω with

$$\Sigma_1 < \Sigma_2 < \cdots < \Sigma_\ell.$$

For each $i \in \{1, \ldots, \ell\}$, we let

$$M_i := \mathbf{N}_G(\Sigma_i) = \{g \in G \mid X^g \in \Sigma_i, \forall X \in \Sigma_i\}$$

be the stabiliser of the partition Σ_i in G. More generally, for every $I \subseteq \{1, \ldots, \ell\}$, we let

$$M_I := \bigcap_{i \in I} M_i.$$

When $I = \{i\}$, we have $M_{\{i\}} = M_i$. Moreover, when $I = \varnothing$, we are implicitly setting $G = M_\varnothing$. We let $H := M_{\{1,\ldots,\ell\}}$.

Here we show that, except when $|\Omega| = 8$ and $G = \mathrm{Alt}(\Omega)$,

$$\mathcal{O}_G(H) = \{M_I \mid I \subseteq \{1, \ldots, \ell\}\} \tag{3.3.4}$$

and hence $\mathcal{O}_G(H)$ is isomorphic to the Boolean lattice of rank ℓ. As usual, the case $|\Omega| = 8$ and $G = \mathrm{Alt}(\Omega)$ is exceptional because of Figure 3.2. To prove (3.3.4), it suffices to show that, if $M \in \mathcal{O}_G(H)$, then there exists $I \subseteq \{1, \ldots, \ell\}$ with $M = M_I$.

We start by describing the structure of the groups M_I, for each $I \subseteq \{1,\dots,\ell\}$. Let $i \in \{1,\dots,\ell\}$. Since M_i is the stabilizer of a non-trivial regular partition Σ_i, we have

$$M_i \cong G \cap (\mathrm{Sym}(n/n_i) \mathrm{wr}\, \mathrm{Sym}(n_i)),$$

where Σ_i is a $(n/n_i, n_i)$-regular partition. (Strictly speaking, we are abusing our notation in the displayed equation above: indeed, the group $\mathrm{Sym}(n/n_i)\mathrm{wr}\,\mathrm{Sym}(n_i)$ is only defined as an abstract group and it is not defined as a subgroup of $\mathrm{Sym}(\Omega)$. In order to be mathematically rigorous we pay the price of having to use cumbersome notation. Therefore, for this proof and for the of this Subsection, we have preferred to adopt a less precise notation when it should not cause any misunderstanding or confusion.) Since $\{\Sigma_i\}_{i=1}^{\ell}$ forms a chain, we deduce that n_i divides n_{i+1}, for each $i \in \{1,\dots,\ell-1\}$. Now, let $i,j \in \{1,\dots,\ell\}$ with $i<j$. The group $M_{\{i,j\}} = \mathbf{N}_G(\Sigma_i) \cap \mathbf{N}_G(\Sigma_j)$ is the stabiliser in G of Σ_i and Σ_j. Since $\Sigma_i < \Sigma_j$, we deduce that

$$M_{\{i,j\}} \cong G \cap (\mathrm{Sym}(n/n_j) \mathrm{wr}\, \mathrm{Sym}(n_j/n_i) \mathrm{wr}\, \mathrm{Sym}(n_i)) .$$

The structure of an arbitrary element M_I is analogous. Let $I = \{i_1,\dots,i_\kappa\}$ be a subset of I with $i_1 < i_2 < \ldots < i_\kappa$. Since $\Sigma_{i_1} < \Sigma_{i_2} < \cdots < \Sigma_\kappa$, we deduce that

$$M_I \cong G \cap (\mathrm{Sym}(n/n_{i_\kappa}) \mathrm{wr}\, \mathrm{Sym}(n_{i_\kappa}/n_{i_{\kappa-1}}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(n_{i_2}/n_{i_1}) \mathrm{wr}\, \mathrm{Sym}(n_{i_1})) .$$

In particular,

$$H \cong G \cap (\mathrm{Sym}(n/n_\ell) \mathrm{wr}\, \mathrm{Sym}(n_\ell/n_{\ell-1}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(n_2/n_1) \mathrm{wr}\, \mathrm{Sym}(n_1)) .$$

Before proceeding with our general argument we prove a preliminary lemma.

Lemma 3.3.30. *The only non-trivial systems of imprimitivity for H are $\Sigma_1,\dots,\Sigma_\ell$, or $G = \mathrm{Alt}(\Omega)$ and $|\Omega| = 4$.*

Proof. Let $\Sigma := \{X_1,\dots,X_\kappa\}$ be a non-trivial system of imprimitivity for H. Set $\Sigma_\ell = \{Y_1,\dots,Y_\iota\}$. From the structure of H, it is clear that the action induced by $\mathbf{N}_H(Y_i)$ on Y_i is that of $\mathrm{Sym}(Y_i)$, for each $i \in \{1,\dots,\iota\}$. Let $i \in \{1,\dots,\iota\}$ and let $j \in \{1,\dots,\kappa\}$ with $Y_i \cap X_j \neq \varnothing$. Since Σ and Σ_ℓ are H-invariant, we have $|X_j \cap Y_i| = 1$ or $Y_i \subseteq X_j$. We investigate a little further the first alternative. Since Σ is non-trivial and since $|Y_i| \geq 2$, there exists $j' \in \{1,\dots,\kappa\} \setminus \{j\}$ with $X_{j'} \cap Y_i \neq \varnothing$. Therefore, we again have the two alternatives: $|X_{j'} \cap Y_i| = 1$ or $Y_i \subseteq X_{j'}$. Suppose that $Y_i \subseteq X_{j'}$. It is readily seen from the structure of H that $\mathbf{N}_H(X_j) \cap \mathbf{N}_H(X_{j'})$ acts transitively on X_j. However, since Σ is H-invariant and $Y_i \subseteq X_{j'}$, we deduce that $\mathbf{N}_H(X_j) \cap \mathbf{N}_H(X_{j'})$ fixes setwise Y_i. Therefore, $\mathbf{N}_H(X_j) \cap \mathbf{N}_H(X_{j'})$ fixes the singleton $X_j \cap Y_i$, contradicting the fact that $\mathbf{N}_H(X_j) \cap \mathbf{N}_H(X_{j'})$ is transitive on X_j or the fact that Σ_ℓ is non-trivial.

Therefore $|X_{j'} \cap Y_i| = 1$. Write $X_j \cap Y_i = \{x\}$. Now, let $(\mathbf{N}_H(X_j))_x$ be the stabilizer of the point x in $\mathbf{N}_H(X_j)$. If $G = \mathrm{Sym}(\Omega)$, or $\kappa \geq 3$, or $|X_j| \geq 3$, then from the structure of H we deduce that $(\mathbf{N}_H(X_j))_x$ is transitive on $X_{j'}$. However, since Σ_ℓ is H-invariant, $x \in Y_i \in \Sigma_\ell$, we deduce that $(\mathbf{N}_H(X_j))_x$ fixes setwise Y_j, contradicting the fact that $|X_{j'} \cap Y_i| = 1$. Therefore, $G = \mathrm{Alt}(\Omega)$, $\iota = 2$ and $|X_j| = 2$, that is, $|\Omega| = 4$ and we have the first possibility in the statement of this lemma.

The previous paragraph shows that, for every $j \in \{1,\dots,\kappa\}$ and for every $i \in \{1,\dots,\iota\}$ with $X_j \cap Y_i \neq \varnothing$, we have $Y_i \subseteq X_j$. That is $\Sigma \leq \Sigma_\ell$. Now, the proof follows by induction on ℓ: replacing Ω with Σ_ℓ, G with $\mathrm{Sym}(\Sigma_\ell)$ and H with the permutation group induced by H on Σ_ℓ. □

We now continue with our construction and we show (3.3.4) arguing by induction on ℓ. When $\ell = 1$, $H = M_1 = \mathbf{N}_G(\Sigma_1)$ and $\mathcal{O}_G(H) = \{H, G\}$ because H is a maximal subgroup

of G by Fact 3.3.2 (recall that we are excluding the case $G = \mathrm{Alt}(\Omega)$ and $|\Omega| = 8$ in the discussion here). For the rest of the proof, we suppose $|\Omega| > 4$ and $\ell \geq 2$.

Let $M \in \mathcal{O}_G(H)$. Suppose M is primitive. As $H \leq M$, we deduce that M contains a 2-cycle or a 3-cycle (when $G = \mathrm{Sym}(\Omega)$ or when $n/n_1 \geq 3$), or a product of two transpositions (when $G = \mathrm{Alt}(\Omega)$ and $n/n_1 = 2$). From [48, Theorem 3.3D and Example 3.3.1], either $\mathrm{Alt}(\Omega) \leq M$ or $|\Omega| \leq 8$. In the first case, $M = M_{\varnothing}$. When $|\Omega| \in \{6, 8\}$, we see with a direct inspection that no exception arises (recall that we are excluding the case $G = \mathrm{Alt}(\Omega)$ and $|\Omega| = 8$ in the discussion here). Therefore, M is not primitive.

Since M is imprimitive, $H \leq M$ and $\Sigma_1, \ldots, \Sigma_\ell$ are the only systems of imprimitivity left invariant by H, we deduce that M leaves invariant one of these systems of imprimitivity. Let $i \in \{1, \ldots, \ell\}$ be maximum such that M leaves invariant Σ_i, that is, $M \leq M_i$. Fix $X \in \Sigma_i$ and consider $\mathbf{N}_M(X) = \{g \in M \mid X^g = X\}$. Consider also the natural projection

$$\pi : \mathbf{N}_{M_i}(X) \to \mathrm{Sym}(X) \cong \mathrm{Sym}(n/n_i).$$

This projection is surjective. For each $j \in \{1, \ldots, \ell\}$ with $i < j$ consider $\Sigma'_j := \{Y \in \Sigma_j \mid Y \subseteq X\}$. By construction Σ'_j is a non-trivial regular partition of X and

$$\Sigma'_{i+1} < \Sigma'_{i+2} < \cdots < \Sigma'_\ell.$$

Moreover,

$$\pi(\mathbf{N}_{M_j}(X)) = \mathbf{N}_{\mathrm{Sym}(X)}(\Sigma'_j).$$

In particular, as $\cap_{j=i+1}^{\ell} \mathbf{N}_{\mathrm{Sym}(X)}(\Sigma'_j) = \pi(\mathbf{N}_H(X)) \leq \pi(\mathbf{N}_M(X))$, by induction on ℓ,

$$\pi(\mathbf{N}_M(X)) = \bigcap_{j \in I'} \mathbf{N}_{\mathrm{Sym}(X)}(\Sigma'_j),$$

for some $I' \subseteq \{i+1, \ldots, \ell\}$. Now, if $I' \neq \varnothing$, then the action of $\mathbf{N}_M(X)$ on X leaves invariant some Σ'_j, for some $j \in I'$. Since $\Sigma_i < \Sigma_j$ and since M leaves invariant Σ_i, it is not hard to see that M leaves invariant Σ_j. However, as $i < j$, we contradict the maximality of i. Therefore $I' = \varnothing$ and hence

$$\pi(\mathbf{N}_M(X)) = \mathrm{Sym}(X).$$

Let $H_{(\Omega \setminus X)}$ and $M_{(\Omega \setminus X)}$ be the pointwise stabilizer of $\Omega \setminus X$ in H and in M, respectively. Thus $H_{(\Omega \setminus X)} \leq M_{(\Omega \setminus X)} \leq \mathrm{Sym}(X)$. From the definition of H and from the fact that X is a block of Σ_i, we deduce

$$H_{(\Omega \setminus X)} \cong \begin{cases} \mathrm{Sym}(n/n_\ell) \mathrm{wr}\, \mathrm{Sym}(n_\ell/n_{\ell-1}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(n_{i+1}/n_i) & \text{when } G = \mathrm{Sym}(\Omega), \\ \mathrm{Alt}(n/n_i) \cap (\mathrm{Sym}(n/n_\ell) \mathrm{wr}\, \mathrm{Sym}(n_\ell/n_{\ell-1}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(n_{i+1}/n_i)) & \text{when } G = \mathrm{Alt}(\Omega). \end{cases}$$

We claim that

$$\mathrm{Alt}(X) \leq M_{(\Omega \setminus X)}. \tag{3.3.5}$$

When $i = \ell$, this is clear because in this case $\mathrm{Alt}(X) \leq H_{(\Omega \setminus X)}$ from the structure of $H_{(\Omega \setminus X)}$. Suppose then $i \leq \ell - 1$. Assume first that either $n/n_\ell \geq 3$ or $n/n_i = |X| \geq 5$. From the description of $H_{(\Omega \setminus X)}$ and from $i \leq \ell - 1$, it is clear that $H_{(\Omega \setminus X)}$ contains a permutation g which is either a cycle of length 3 or the product of two transpositions. Define $V := \langle g^m \mid m \in \mathbf{N}_M(X) \rangle$. As $H \leq M$, we deduce that $g \in M_{(\Omega \setminus X)}$ and hence $V \leq M_{(\Omega \setminus X)}$. Since $\pi(\mathbf{N}_M(X)) = \mathrm{Sym}(X)$, we get $V \trianglelefteq \mathrm{Sym}(X)$ and hence $V = \mathrm{Alt}(X)$. In particular, our claim is proved in this case. It remains to consider the case that $n/n_\ell = 2$ and $|X| < 5$. As $i \leq \ell - 1$, this yields $i = \ell - 1$, $n/n_\ell = n_\ell/n_{\ell-1} = 2$ and $|X| = 4$. Observe that in this case, the group V has order 4 and is the Klein subgroup of $\mathrm{Alt}(X)$. When $G = \mathrm{Sym}(\Omega)$, $H_{(\Omega \setminus X)}$ contains a transposition and hence we may repeat this argument replacing g with this transposition; in this case, we deduce $M_{(\Omega \setminus X)} = \mathrm{Sym}(X)$ and hence our claim is proved

also in this case. Assume then $G = \mathrm{Alt}(\Omega)$, $i = \ell - 1$, $n/n_\ell = n_\ell/n_{\ell-1} = 2$ and $|X| = 4$. Among all elements $h \in \mathbf{N}_M(X)$ with $\pi(h)$ a cycle of length 3, choose h with the maximum number of fixed points on Ω. Assume that h fixes pointwise X', for some $X' \in \Sigma_i$. From the structure of H, we see that H contains a permutation g normalizing both X and X', acting on both sets as a transposition and fixing pointwise $\Omega \setminus (X \cup X')$. Now, a computation shows that $g^{-1}h^{-1}gh$ acts as a cycle of length 3 on X and fixes pointwise $\Omega \setminus X$, that is, $g^{-1}h^{-1}gh \in M_{(\Omega\setminus X)}$. In particular, $\mathrm{Alt}(X) \leq M_{(\Omega\setminus X)}$ in this case. Therefore, we may suppose that h fixes pointwise no block $X' \in \Sigma_i$. Assume that h acts as a cycle of length 3 on three blocks $X_1, X_2, X_3 \in \Sigma_i$, that is, $X_1^h = X_2$, $X_2^h = X_3$ and $X_3^h = X_1$. From the structure of H, we see that H contains a permutation g normalizing both X and X_1, acting on both sets as a transposition and fixing pointwise $\Omega \setminus (X \cup X_1)$. Now, a computation shows that $g^{-1}h^{-1}gh$ acts as a cycle of length 3 on X, as a transposition on X_1, and fixes pointwise $\Omega \setminus (X \cup X_1)$. In particular, $(g^{-1}h^{-1}gh)^2$ acts as a cycle of length 3 and fixes pointwise $\Omega \setminus X$. Thus $(g^{-1}h^{-1}gh)^2 \in M_{(\Omega\setminus X)}$ and $\mathrm{Alt}(X) \leq M_{(\Omega\setminus X)}$ also in this case. Finally, suppose that h fixes set-wise but not pointwise each block in Σ_i. In particular, for each $X' \in \mathbf{N}_M(X)$, we have $X'^h = X'$ and h acts as a cycle of length 3 on X'. Let $X' \in \Sigma_i$ with $X' \neq X$. From the structure of H, we see that H contains a permutation g normalizing both X and X', acting on both sets as a transposition and fixing pointwise $\Omega \setminus (X \cup X')$. Now, a computation shows that $g^{-1}h^{-1}gh$ acts as a cycle of length 3 on X and on X' and fixes pointwise $\Omega \setminus (X \cup X')$. As h was choosen with the maximum number of fixed points with $\pi(h)$ having order 3, we deduce that $\Omega = X \cup X'$, that is, $n = 8$. In particular, we end up with the exceptional case in Figure 3.2, which we are excluding in our discussion. Therefore, (3.3.5) is now proved.

Let K_i be the kernel of the action of M_i on Σ_i. Thus

$$K_i = G \cap \prod_{X \in \Sigma_i} \mathrm{Sym}(X).$$

From (3.3.5), we deduce

$$\mathrm{Alt}(n/n_i)^{n_i} \cong \prod_{X \in \Sigma_i} \mathrm{Alt}(X) \leq M.$$

As $H \leq M$, we obtain $K_i = H(\prod_{X\in\Sigma_i} \mathrm{Alt}(X)) \leq M$.

Since $\Sigma_1 < \Sigma_2 < \cdots < \Sigma_i$, for every $j \in \{1, \ldots, i\}$, we may consider Σ_j as a regular partition of Σ_i. More formally, define $\Omega'' := \Sigma_i$ and define $\Sigma_j'' := \{\{Y \in \Sigma_i \mid Y \subseteq Z\} \mid Z \in \Sigma_j\}$. Thus Σ_j'' is the quotient partition of Σ_j via Σ_i. Clearly, $M_j/K_i = \mathbf{N}_{M_i}(\Sigma_j'')$. Applying our induction hypothesis to the chain $\Sigma_1'' < \cdots < \Sigma_i''$, we have $M/K_i = M_I/K_i$, for some subset I of $\{1, \ldots, i\}$. Since $K_i \leq M$, we deduce $M = M_I$.

3.3.8 Large Boolean lattices arising from primitive maximal subgroups

Lemma 3.3.31. *Let Σ be a (c, d)-regular partition of Ω. Given a transitive subgroup U of $\mathrm{Sym}(d)$, we identify the group $X = \mathrm{Sym}(c)\mathrm{wr}\, U$ with a subgroup of $\mathbf{N}_{\mathrm{Sym}(\Omega)}(\Sigma)$. If X normalizes a regular partition $\tilde{\Sigma}$ of Ω, then $\tilde{\Sigma} \leq \Sigma$.*

Proof. Let A and $\tilde{A}$ be blocks, respectively, of Σ and $\tilde{\Sigma}$ with $A \cap \tilde{A} \neq \varnothing$ and let $a \in A \cap \tilde{A}$. Then, for every $z \in A \setminus \{a\}$, the transposition $(a, z) \in X$ fixes at least one element of $\tilde{A}$ and therefore (a, z) normalizes $\tilde{A}$ and consequently $z \in \tilde{A}$. Therefore, either $A \subseteq \tilde{A}$ or $\tilde{A} \subseteq A$. From this, it follows that either $\Sigma \leq \tilde{\Sigma}$ or $\tilde{\Sigma} \leq \Sigma$. We can exclude the first possibility, because $\mathbf{N}_X(A)$ acts on A as the symmetric group $\mathrm{Sym}(A)$. □

Since we aim to prove that there exist Boolean lattices of arbitrarily large rank of the type described in Thereom 3.0.5 (3), we suppose $n = |\Omega|$ is odd. Let ℓ be an integer with $\ell \geq 3$ and let

$$\mathcal{F}_1 < \cdots < \mathcal{F}_\ell$$

be a chain of regular product structures on Ω. In particular, $\mathcal{F}_\ell$ is a regular (a,b)-product structure for some integers $a \geq 5$ and $b \geq 2$ with a odd and $n = a^b$. From the partial order in the poset of regular product structures, we deduce that we may write $b = b_1 \cdots b_\ell$ such that, if we set $d_i := b_i \cdots b_\ell$ and $c_i := b/d_i$, then $\mathcal{F}_{\ell+1-i}$ is a regular (a^{c_i}, d_i)-product structure, for every $i \in \{1, \ldots, \ell\}$.

Let $M_i := \mathbf{N}_{\mathrm{Sym}(\Omega)}(\mathcal{F}_i) \cong \mathrm{Sym}(a^{c_i}) \mathrm{wr}\, \mathrm{Sym}(d_i)$ and let $H := M_1 \cap \cdots \cap M_\ell$. We have

$$H := \mathrm{Sym}(a) \mathrm{wr}\, \mathrm{Sym}(b_1) \mathrm{wr}\, \mathrm{Sym}(b_2) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(b_\ell)$$

as a permutation group of degree n. Moreover, if I is a subset of $\{1, \ldots, \ell\}$, we let $M_I := \cap_{i \in I} M_i$, where we are implicitly setting $M_\varnothing = \mathrm{Sym}(n)$. In particular, if $I = \{r_1, \ldots, r_s\}$, then M_I is isomorphic to

$$\mathrm{Sym}(a^{b_1 \cdots b_{r_1 - 1}}) \mathrm{wr}\, \mathrm{Sym}(b_{r_1} \cdots b_{r_2 - 1}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(b_{r_s} \cdots b_\ell).$$

For proving that $\mathcal{O}_G(H)$ is Boolean of rank ℓ, we need to show that, for every $K \in \mathcal{O}_G(H)$, there exists $I \subseteq \{1, \ldots, \ell\}$ with $K = M_I$.

We may identity H with the wreath product $\mathrm{Sym}(a) \mathrm{wr}\, X$ with

$$X = \mathrm{Sym}(b_1) \mathrm{wr}\ \mathrm{Sym}(b_2) \mathrm{wr} \cdots \mathrm{wr}\ \mathrm{Sym}(b_\ell),$$

where X has degree b and is endowed of the imprimitive action of the itereted wreath product and $\mathrm{Sym}(a) \mathrm{wr}\, X$ is primitive of degree $n = a^b$ and is endowed of the primitive action of the wreath product.

Lemma 3.3.32. *If H normalizes a regular product structure $\mathcal{F}$, then $\mathcal{F} \in \{\mathcal{F}_1, \ldots, \mathcal{F}_\ell\}$.*

Proof. The group $H = \mathrm{Sym}(a) \mathrm{wr}\, X$ is semisimple and not almost simple. Since the components of H are isomorphic to $\mathrm{Alt}(a)$ and a is odd, according with the definition in [6, Section 2], H is product indecomposable. From [6, Proposition 5.9 (5)], we deduce $\boldsymbol{\mathcal{F}}(H)$ is isomorphic to the dual of $\mathcal{O}_H(J) \setminus \{H\}$, where $J := \mathbf{N}_H(L)$ is the normalizer of a component L of H. Since $\mathbf{F}^*(H) = (\mathrm{Alt}(a))^b$, we have

$$J = \mathrm{Sym}(a) \times (\mathrm{Sym}(a) \mathrm{wr}\, Y) = \mathrm{Sym}(a) \times (\mathrm{Sym}(a)^{b-1} \rtimes Y),$$

with Y the stabilizer of a point in the imprimitive action of X of degree b. In particular $\mathcal{O}_H(J) \setminus \{H\} \cong \mathcal{O}_X(Y) \setminus \{X\}$.

The proper subgroups of X containing the point-stabilizer Y are in one-to-one correspondence with the regular partitions Σ of $\{1, \ldots, b\}$ normalized by X and with at least two blocks. Notice that, for any $i \in \{1, \ldots, \ell\}$, there is an embedding of X in $\mathrm{Sym}(c_i) \mathrm{wr}\ \mathrm{Sym}(d_i)$, and therefore X normalizes a regular (c_i, d_i)-partition, which we call it $\Sigma_{\ell+1-i}$. An iterated application of Lemma 3.3.31 implies that $\Sigma_1 < \cdots < \Sigma_\ell$ are the unique non-trivial regular partitions normalized by X. □

Theorem 3.3.33. *If $H \leq K \leq \mathrm{Sym}(n)$, then $K = M_I$ for some subset I of $\{1, \ldots, \ell\}$.*

Proof. Clearly, without loss of generality we may suppose that $H < K < \mathrm{Sym}(n)$. We apply [140, Proposition 7.1] to the inclusion (H, K). Since H has primitive components isomorphic to $\mathrm{Alt}(a)$, with a odd, only cases (ii,a) and (ii,b) can occur.

Assume that (H, K) is an inclusion of type (ii,a). In this case we have $H < K \leq \mathrm{Sym}(a) \mathrm{wr}\ \mathrm{Sym}(b)$. Since $\mathrm{Sym}(a)^b \leq H \leq K$ we deduce that $K = \mathrm{Sym}(a) \mathrm{wr}\, Y$; with $X \leq Y \leq \mathrm{Sym}(b)$. So it suffices to notice that the only subgroups of $\mathrm{Sym}(b)$ containing X are those of the kind $\mathrm{Sym}(b_1 \cdots b_{t_1}) \mathrm{wr}\ \mathrm{Sym}(b_{t_1+1} \cdots b_{t_2}) \mathrm{wr} \cdots \mathrm{wr}\ \mathrm{Sym}(b_{t_s+1} \cdots b_\ell)\}$, for some subset $\{t_1, \ldots, t_s\}$ of $\{1, \ldots, \ell\}$. Indeed, this fact follows from Subsection 3.3.7.

Assume that (H, K) is an inclusion of type (ii,b). (In what follows, the precise meaning of the term "blow up" can be found in [140, Section 2] and we refer the reader to that paper for details. Here we do not give a full account because we are only interested in a particular consequence.) In this case, following the terminology in [140, Section 2 and 7], $n = a^b = \alpha^{\gamma\delta}$, H is a blow-up of a subgroup Z of $\mathrm{Sym}(\alpha^\gamma)$ and (H, K) is a blow up of a natural inclusion (Z, L) where $\mathrm{Alt}(\alpha^\gamma) \leq L \leq \mathrm{Sym}(\alpha^\gamma)$. From this we immediately deduce that H normalizes a regular (α^γ, δ)-product structure $\mathcal{F}$. By Lemma 3.3.32, we have $\mathcal{F} \in \{\mathcal{F}_1, \ldots, \mathcal{F}_\ell\}$. In particular, $\alpha^\gamma = a^{c_i}$ and $\delta = d_i$ and $Z = \mathrm{Sym}(a)\mathrm{wr}\ \mathrm{Sym}(b_1)\mathrm{wr}\ \mathrm{Sym}(b_2)\mathrm{wr} \cdots \mathrm{wr}\ \mathrm{Sym}(b_i)$. Since a is odd, $Z \not\leq \mathrm{Alt}(a^{c_i})$ so $L = \mathrm{Sym}(a^{c_i})$ and $(\mathrm{Sym}(a^{c_i}))^{d_i} \leq K \leq \mathrm{Sym}(a^{c_i})\mathrm{wr}\ \mathrm{Sym}(d_i)$. If H is maximal in K, then $i = 1$ and $K = \mathrm{Sym}(a^{b_1})\mathrm{wr}\ \mathrm{Sym}(b_2)\mathrm{wr} \cdots \mathrm{wr}\ \mathrm{Sym}(b_\ell) = M_{\{1,\ldots,\ell-1\}}$; otherwise, we can proceed by induction on ℓ. □

3.3.9 Application to Brown's problem

In this section we will prove Theorem 3.0.6 (where (4) is a direct application of Theorem 3.0.5) which, in these cases, proves Conjecture 6.

Some general lemmas

Let G be a finite group and H a subgroup such that the overgroup lattice $\mathcal{O}_G(H)$ is Boolean of rank ℓ, and let $M_1, \ldots, M_\ell$ be its coatoms. For any K in $\mathcal{O}_G(H)$, let us note $K^{\complement}$ its *lattice-complement*, i.e. $K \wedge K^{\complement} = H$ and $K \vee K^{\complement} = G$.

Lemma 3.3.34. *If $\mathcal{O}_G(H)$ is Boolean of rank 2 and if H is normal in M_i $(i = 1, 2)$, then $|M_1 : H| \neq |M_2 : H|$.*

Proof. As an immediate consequence of the assumption, H is normal in $M_1 \vee M_2 = G$, but then G/H is a group and $\mathcal{L}(G/H)$ is Boolean, so distributive, and G/H is cyclic by Ore's theorem, thus $|M_1/H| \neq |M_2/H|$. □

Lemma 3.3.35. *If $\mathcal{O}_G(H)$ is Boolean of rank 2 then $(|M_1 : H|, |M_2 : H|) \neq (2, 2)$.*

Proof. If $(|M_1 : H|, |M_2 : H|) = (2, 2)$ then H is normal in M_i $(i = 1, 2)$. This contradicts Lemma 3.3.34. □

Lemma 3.3.36. *If $\mathcal{O}_G(H)$ is Boolean of rank $\ell \leq 2$. Then $\hat{\varphi}(H, G) \geq 2^{\ell-1}$.*

Proof. If $\ell = 1$ then

$$\hat{\varphi}(H, G) = |G : H| - |G : G| \geq 2 - 1 = 2^{\ell-1}.$$

If $\ell = 2$, by Lemma 3.3.35, there is i with $|M_i : H| \geq 3$. Then

$$\begin{aligned}\hat{\varphi}(H, G) &= |G : H| - |G : M_1| - |G : M_2| + |G : G| \\ &= |G : H|(1 - |M_1 : H|^{-1} - |M_2 : H|^{-1}) + 1 \\ &\geq 6(1 - 1/3 - 1/2) + 1 = 2^{\ell-1}.\end{aligned}$$

□

Remark 3.3.37 (Product Formula)**.** *Let A be a finite group and let B, C be two subgroups. Then $|B| \cdot |C| = |BC| \cdot |B \cap C|$, so*

$$|B| \cdot |C| \leq |B \vee C| \cdot |B \wedge C| \quad \text{and} \quad |B : B \wedge C| \leq |B \vee C : C|.$$

Lemma 3.3.38. *Let A be a finite group and let B, C be two subgroups. If $|A : C| = 2$ and $B \not\subseteq C$ then $|B : B \wedge C| = 2$.*

Proof. By Product Formula, $2 \leq |B : B \wedge C| \leq |A : C| = 2$ because $A = B \vee C$. □

Lemma 3.3.39. *Let A be an atom of $\mathcal{O}_G(H)$. If $K_1, K_2 \in \mathcal{O}_{A^{\complement}}(H)$ with $K_1 < K_2$, then*

$$|K_1 \vee A : K_1| \leq |K_2 \vee A : K_2|.$$

Equivalently, if $K_1, K_2 \in \mathcal{O}_G(A)$ with $K_1 < K_2$, then

$$|K_1 : K_1 \wedge A^{\complement}| \leq |K_2 : K_2 \wedge A^{\complement}|.$$

Moreover if $|G : A^{\complement}| = 2$ then $|K \vee A : K| = 2$, for all K in $\mathcal{O}_{A^{\complement}}(H)$.

Proof. By Product Formula,

$$|K_1 \vee A| \cdot |K_2| \leq |(K_1 \vee A) \vee K_2| \cdot |(K_1 \vee A) \wedge K_2|$$

but $K_1 \wedge K_2 = K_1$, $K_1 \vee K_2 = K_2$ and $A \wedge K_2 = H$, so by distributivity

$$|K_1 \vee A| \cdot |K_2| \leq |K_2 \vee A| \cdot |K_1|.$$

Finally, $A^{\complement} \vee A = G$, so if $H \leq K \leq A^{\complement}$ and $|G : A^{\complement}| = 2$, then

$$2 \leq |K \vee A : K| \leq |A^{\complement} \vee A : A^{\complement}| = 2.$$

It follows that $|K \vee A : K| = 2$. □

Lemma 3.3.40. *If $\mathcal{O}_G(H)$ is Boolean of rank 2, then $|M_1 : H| = 2$ if and only if $|G : M_2| = 2$.*

Proof. If $|G : M_2| = 2$ then $|M_1 : H| = 2$ by Lemma 3.3.38. Now if $|M_1 : H| = 2$ then $H \lhd M_1$ and $M_1 = H \sqcup H\tau$ with $\tau H = H\tau$ and $(H\tau)^2 = H$, so $H\tau^2 = H$ and $\tau^2 \in H$. Now $M_2 \in (H, G)$, then $\tau M_2 \tau^{-1} \in (\tau H \tau^{-1}, \tau G \tau^{-1}) = (H, G)$, so by assumption $\tau M_2 \tau^{-1} \in \{M_1, M_2\}$. If $\tau M_2 \tau^{-1} = M_1$, then $M_2 = \tau^{-1} M_1 \tau = M_1$, contradiction. So $\tau M_2 \tau^{-1} = M_2$. Now $\tau^2 \in H < M_2$, so $M_2 \tau^2 = M_2$. It follows that $G = \langle M_2, \tau \rangle = M_2 \sqcup M_2 \tau$, and $|G : M_2| = 2$. □

Lemma 3.3.41. *If there are $K, L \in \mathcal{O}_G(H)$ such that $K < L$ and $|L : K| = 2$, then there is an atom A such that $L = K \vee A$ and $|G : A^{\complement}| = 2$.*

Proof. By the Boolean structure and because K is a maximal subgroup of L, there is an atom A of $\mathcal{O}_G(H)$ such that $L = K \vee A$. Let

$$K = K_1 < K_2 < \cdots < K_r = A^{\complement}$$

be a maximal chain from K to $A^{\complement}$. Let $L_i = K_i \vee A$, then the overgroup lattice $\mathcal{O}_{L_{i+1}}(K_i)$ is Boolean of rank 2, now $|L_1 : K_1| = 2$, so by Lemma 3.3.40

$$2 = |L_1 : K_1| = |L_2 : K_2| = \cdots = |L_r : K_r| = |G : A^{\complement}|.$$ □

Note that for an index 2 subgroup B of A, if $|B|$ is odd then $A = B \rtimes C_2$, but this is not true in general if $|B|$ is even.

Lemma 3.3.42. *If there is i such that for all K in $\mathcal{O}_{M_i}(H)$, $|K \vee M_i^{\complement} : K| = |M_i^{\complement} : H|$ then*

$$\hat{\varphi}(H, G) = (|M_i^{\complement} : H| - 1)\hat{\varphi}(H, M_i).$$

Proof. By assumption we deduce that $\hat{\varphi}(H, M_i) = \hat{\varphi}(M_i^{\complement}, G)$, but by definition, $\hat{\varphi}(H, G) = |M_i^{\complement} : H|\hat{\varphi}(H, M_i) - \hat{\varphi}(H, M_i)$. The result follows. □

Lemma 3.3.43. *If there is i such that $|M_i^{\complement} : H| = 2$ then $\hat{\varphi}(H, G) = \hat{\varphi}(H, M_i)$.*

Proof. By assumption and Lemma 3.3.41, $|G : M_i| = 2$, so by Lemma 3.3.39, if $H \leq K \leq M_i$ then $|K \vee M_i^{\mathfrak{C}} : K| = 2$. Thus, by Lemma 3.3.42, $\hat{\varphi}(H, G) = (2-1)\hat{\varphi}(H, M_i)$. □

Lemma 3.3.44. *Let G be a finite group and H a subgroup such that the overgroup lattice $\mathcal{O}_G(H)$ is Boolean of rank ℓ, and let $A_1, \ldots, A_\ell$ be its atoms. If $|A_i : H| \geq 2^i$ then $\hat{\varphi}(H, G) \geq 2^{\ell-1}$.*

Proof. Let I be a subset of $\{1, \ldots, \ell\}$ and let A_I be $\bigvee_{i \in I} A_i$. Then $\mathcal{O}_G(H) = \{A_I \mid I \subseteq \{1, \ldots, \ell\}\}$ and

$$\hat{\varphi}(H, G) = \sum_{I \subseteq \{1,\ldots,\ell\}} (-1)^{|I|} |G : A_I|.$$

By assumption and Lemma 3.3.39, if $j \notin I$ then $|G : A_I| \geq 2^j |G : A_I \vee A_j|$. It follows that

$$|G : A_J| \leq \frac{1}{|J|} \sum_{j \in J} 2^{-j} |G : A_{J \setminus \{j\}}|$$

from which we get that

$$\begin{aligned}
\hat{\varphi}(H, G) &\geq \sum_{|I| \text{ even}} |G : A_I| - \sum_{|I| \text{ odd}} \frac{1}{|I|} \sum_{i \in I} 2^{-i} |G : A_{I \setminus \{i\}}| \\
&= \sum_{|I| \text{ even}} |G : A_I| \left(1 - \frac{\sum_{i \notin I} 2^{-i}}{|I| + 1}\right) \\
&= \sum_{|I| \text{ even}} |G : A_I| \frac{|I| + 2^{-\ell} + \sum_{i \in I} 2^{-i}}{|I| + 1} \\
&\geq |G : A_\varnothing| 2^{-\ell} = 2^{-\ell} |G : H| \\
&\geq 2^{-\ell} \prod_{i=1}^{\ell} 2^i = 2^{\ell(\ell-1)/2} \geq 2^{\ell-1}.
\end{aligned}$$

□

Lemma 3.3.45. *Let G be a finite group and H a subgroup such that the overgroup lattice $\mathcal{O}_G(H)$ is Boolean of rank ℓ, and let $A_1, \ldots, A_\ell$ be its atoms. If $|A_i : H| \geq a_i > 0$ then $\hat{\varphi}(H, G) \geq (1 - \sum_i a_i^{-1}) \prod_i a_i$.*

Proof. It works exactly as for the proof of Lemma 3.3.44. □

Proof of Theorem 3.0.6 (1)

Proof. The case $\ell \leq 2$ is precisely Lemma 3.3.36. It remains to consider the case $\ell = 3$.

If there is i such that $|M_i^{\mathfrak{C}} : H| = 2$, then by Lemma 3.3.35 and the Boolean structure, for all $j \neq i$, $|M_j^{\mathfrak{C}} : H| \geq 3$, and by Lemma 3.3.43, $\hat{\varphi}(H, G) = \hat{\varphi}(H, M_i)$. As in the proof of Lemma 3.3.36, we have that

$$\hat{\varphi}(H, M_i) \geq 9(1 - 1/3 - 1/3) + 1 = 2^{\ell-1}.$$

Otherwise, for all i we have $|M_i^{\mathfrak{C}} : H| \geq 3$. Then (using Lemma 3.3.39)

$$\begin{aligned}
\hat{\varphi}(H, G) &= |G : H| - \sum_i |G : M_i^{\mathfrak{C}}| + \sum_i |G : M_i| - |G : G| \\
&\geq |G : H| \left(1 - \sum_i |M_i^{\mathfrak{C}} : H|^{-1}\right) + \sum_i |M_i^{\mathfrak{C}} : H| - 1 \\
&\geq 27 \left(1 - \sum_i 1/3\right) + \sum_i (3) - 1 = 8 > 2^{\ell-1}.
\end{aligned}$$

□

Proof of Theorem 3.0.6 (2)(3)

Let $M_1, \dots, M_\ell$ be the coatoms of $\mathcal{O}_G(H)$.
The Boolean lattice $\mathcal{O}_G(H)$ is called *group-complemented* if $KK^{\complement} = K^{\complement}K$ for every $K \in \mathcal{O}_G(H)$.

Lemma 3.3.46. *If the Boolean lattice $\mathcal{O}_G(H)$ is group-complemented then $\hat{\varphi}(H,G) = \prod_i(|G : M_i| - 1)$.*

Proof. By assumption, $KK^{\complement} = K^{\complement}K$ which means that $KK^{\complement} = K \vee K^{\complement} = G$. Further, by Product Formula, it follows that $|G : K| = |K^{\complement} : H|$. Then by Lemma 3.3.39, for all i and for all K in $\mathcal{O}_G(M_i^{\complement})$, $|K : K \wedge M_i| = |G : M_i|$. Now, for all K in $\mathcal{O}_G(H)$ there is $I \subseteq \{1, \dots, \ell\}$ such that $K = M_I = \bigwedge_{i\in I} M_i$, it follows that $|G : K| = \prod_{i\in I} |G : M_i|$ and then

$$\hat{\varphi}(H,G) = (-1)^\ell \sum_{I\subseteq\{1,\dots,\ell\}} (-1)^{|I|}|G : M_I| = (-1)^\ell \sum_{I\subseteq\{1,\dots,\ell\}} \prod_{i\in I}(-|G : M_i|) = \prod_i(|G : M_i|-1). \quad \square$$

Theorem 3.0.6 (2) follows from Lemmas 3.3.46 and 3.3.35. Moreover, if G is solvable and if $\mathcal{O}_G(H)$ is Boolean then it is also group-complemented by [102, Theorem 1.5] and the proof of Lemma 3.3.46, hence Theorem 3.0.6 (3) follows.

Proof of Theorem 3.0.6 (4)

Proof. By Theorem 3.0.6 (1), we are reduced to consider $\ell \geq 4$ on the cases (1)-(6) of Theorem 3.0.5.

1. Let $G = Sym(\Omega)$. By Subsection 3.3.7, the rank ℓ Boolean lattice $\mathcal{O}_G(H)$ is made of

$$M_I \cong \mathrm{Sym}(n/n_{i_1}) \mathrm{wr}\, \mathrm{Sym}(n_{i_1}/n_{i_2}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(n_{i_{\kappa-1}}/n_{i_\kappa}) \mathrm{wr}\, \mathrm{Sym}(n_{i_\kappa}),$$

with $I = \{i_1, i_2, \dots, i_\kappa\} \subseteq \{1, \dots, \ell\}$. Now,

$$|M_I| = \left(\frac{n}{n_{i_1}}!\right)^{n_{i_1}} \left(\frac{n_{i_1}}{n_{i_2}}!\right)^{n_{i_2}} \cdots \left(\frac{n_{i_{\kappa-1}}}{n_{i_\kappa}}!\right)^{n_{i_\kappa}} n_{i_\kappa}!$$

In particular, with $n_0 = n$, $n_{\ell+1} = 1$, $H = M_{\{1,\dots,\ell\}}$ and $A_i = M_i^{\complement}$, we have that

$$|H| = \prod_{i=0}^{\ell} \left(\frac{n_i}{n_{i+1}}!\right)^{n_{i+1}}, \quad |A_j| = \left(\frac{n_{j-1}}{n_{j+1}}!\right)^{n_{j+1}} \prod_{i\neq j,j+1} \left(\frac{n_i}{n_{i+1}}!\right)^{n_{i+1}}.$$

It follows that

$$|A_j : H| = \frac{\left(\frac{n_{j-1}}{n_{j+1}}!\right)^{n_{j+1}}}{\left(\frac{n_{j-1}}{n_j}!\right)^{n_j} \left(\frac{n_j}{n_{j+1}}!\right)^{n_{j+1}}} = \left[\frac{\left(\frac{n_{j-1}}{n_{j+1}}!\right)}{\left(\frac{n_{j-1}}{n_j}!\right)^{\frac{n_j}{n_{j+1}}} \left(\frac{n_j}{n_{j+1}}!\right)}\right]^{n_{j+1}} \geq 3^{n_{j+1}}.$$

Take the atom $B_i := A_{\ell+1-i}$ and $m_i := n_{\ell+1-i}$, then

$$|B_i : H| \geq 3^{m_{i+1}} \geq 3^{2^{i-1}} > 2^i.$$

It follows by Lemma 3.3.44 that $\hat{\varphi}(H,G) \geq 2^{\ell-1}$.

Next, if $B_i \subseteq \mathrm{Alt}(\Omega)$ then $H \subseteq \mathrm{Alt}(\Omega)$. Clearly $|\mathrm{Alt}(\Omega) \cap B_i : \mathrm{Alt}(\Omega) \cap H| = |B_i : H|$. Otherwise, by Lemma 3.3.38, $|B_i : \mathrm{Alt}(\Omega) \cap B_i| = 2$. Now, $|H : \mathrm{Alt}(\Omega) \cap H| = 1$ or 2 whether $H \subseteq \mathrm{Alt}(\Omega)$ or not. In any case,

$$|\mathrm{Alt}(\Omega) \cap B_i : \mathrm{Alt}(\Omega) \cap H| \geq |B_i : H|/2 > 3^{2^{i-1}-1},$$

and we can also apply Lemma 3.3.44.

2. Let $A_\ell = M_\ell^{\mathfrak{C}}$, then $|A_\ell : H| = 2$. Next, we can order, as above, the remaining atoms $A_1, \ldots, A_{\ell-1}$ such that $|A_i : H| \geq 3^{2^{i-1}}$ because by assumption $|A_\ell : \mathrm{Alt}(\Omega) \cap A_\ell| = 2$. The result follows by Lemma 3.3.45 because

$$1 - (\frac{1}{2} + \sum_{i=1}^{\ell-1} 3^{-2^{i-1}}) \geq \frac{1}{2} - \sum_{i=1}^{\ell-1} 3^{-i} = \sum_{i=\ell}^{\infty} 3^{-i} = \frac{3}{2} 3^{-\ell}.$$

3. Following the notations of Subsection 3.3.8, for $I = \{r_1, r_2, \ldots, r_s\}$ we have that

$$|M_I| = (a^{b_1 \cdots b_{r_1 - 1}}!)^{b_{r_1} \cdots b_\ell} \prod_{i=1}^{s} ((b_{r_i} \cdots b_{r_{i+1}-1})!)^{b_{r_{i+1}} \cdots b_\ell}.$$

   The atom $A_i = M_i^{\mathfrak{C}}$ is of the form $M_{\{i\}^{\mathfrak{C}}}$, whereas, $H = M_{\{1,\ldots,\ell\}}$, then (with $b_0 = 1$)

$$|H| = (a!)^{b_1 \cdots b_\ell} \prod_{i=1}^{\ell} (b_i!)^{b_{i+1} \cdots b_\ell} \text{ and } A_j = (a^{b_1^{\delta_{1,j}}}!)^{b_1^{-\delta_{1,j}} \prod_i b_i} ((b_{j-1} b_j)!)^{\delta_{1,j} b_{j+1} \cdots b_\ell} \prod_{i \neq j-1, j} (b_i!)^{b_{i+1} \cdots b_\ell}.$$

   Let $j > 1$, it follows that

$$|A_j : H| = \left[\frac{(b_{j-1} b_j)!}{((b_{j-1})!)^{b_j} b_j!} \right]^{b_{j+1} \cdots b_\ell} \text{ and } |A_1 : H| = \left[\frac{a^{b_1}!}{(a!)^{b_1} b_1!} \right]^{b_2 \cdots b_\ell}.$$

   The rest is similar to (1).

4. Similar to (2).

5. Here $n = a^b$ is a prime power p^d so that $a = p^{d'}$ with $bd' = d$, $b = b_1 \cdots b_{\ell-1}$ and $G_\ell = AGL_d(p)$. We can deduce, by using [5, Theorem 13 (3)], that

$$AGL_d(p) \cap (\mathrm{Sym}(a^{b_1 \cdots b_{r_1}}) \mathrm{wr}\, \mathrm{Sym}(b_{r_1+1} \cdots b_{r_2}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(b_{r_s+1} \cdots b_{\ell-1}))$$

$$= AGL_{d' b_1 \cdots b_{r_1}}(p) \mathrm{wr}\, \mathrm{Sym}(b_{r_1+1} \cdots b_{r_2}) \mathrm{wr} \cdots \mathrm{wr}\, \mathrm{Sym}(b_{r_s+1} \cdots b_{\ell-1}).$$

   But $|AGL_k(p)| = p^k \prod_{i=0}^{k-1} (p^k - p^i)$. The rest is similar to (3).

6. Similar to (2). □

Chapter 4

Asymptotic enumeration of Cayley graphs

In this chapter, we consider only finite groups and graphs. A graph (digraph) Γ is an ordered pair (V, E) with V a finite non-empty set of vertices, and E a set of unordered (ordered) pairs from V, representing the edges. An automorphism of a graph (digraph) is a permutation on V that preserves the set E.

Definition 4.0.1. *Let R be a group and let S be a subset of R. The* Cayley digraph $\Gamma(R, S)$ *with connection set S, is the digraph with with $V = R$ and $\{r, t\} \in E$ if and only if $tr^{-1} \in S$. When $S = S^{-1}$ is an inverse-closed subset of R, then $\Gamma(R, S)$ is the* Cayley graph *with connection set S.*

The problem of finding graphical regular representations (GRRs) for groups has a long history. Mathematicians have studied graphs with specified automorphism groups at least as far back as the 1930s, and in the 1970s there were many papers devoted to the topic of finding GRRs (see for example [9, 68, 71, 72, 73, 124, 125, 126, 161]), although the "GRR" terminology was coined somewhat later.

Definition 4.0.2. *A* graphical (respectively, digraphical) regular representation*, GRR (respectively DRR) for short, for a group R is a graph whose full automorphism group is the group R acting regularly on the vertices of the graph.*

It is an easy observation that when $\Gamma(R, S)$ is a Cayley graph (digraph), the group R acts regularly on the vertices as a group of graph (digraph) automorphisms. A GRR (DRR) for R is therefore a Cayley graph (digraph) on R that admits no other automorphisms.

The main thrust of much of the work through the 1970s was to determine which groups admit GRRs. This question was ultimately answered by Godsil in [57].

Theorem 4.0.3 (Godsil, [57])**.** *A group has a graphical regular representation if and only if it is not one of:*

- *a generalised dicyclic group (see Definition 4.0.8);*
- *an abelian group of exponent greater than 2; or*
- *one of 13 small groups (of order at most 32).*

A corresponding result for DRRs by Babai was much simpler, requiring no excluded families and finding only 5 exceptional small groups.

Babai and Godsil made the following conjecture.

Conjecture 7 ([10]; Conjecture 3.13, [58])**.** *If R is not generalised dicyclic or abelian of exponent greater than 2, then for almost all inverse-closed subsets S of R, $\Gamma(R, S)$ is a GRR.*

The details of this conjecture are somewhat imprecise; we are interested in the following more specific formulation:

$$\lim_{r\to\infty} \min\left\{ \frac{|\{S \subseteq R : S = S^{-1}, \mathrm{Aut}(\Gamma(R,S)) = R\}|}{2^{\mathbf{c}(R)}} : R \text{ admits a GRR and } |R| = r \right\} = 1,$$

where $2^{\mathbf{c}(R)}$ is the number of inverse-closed subsets of R. (The value $\mathbf{c}(R)$ is defined explicitly in Definition 4.0.7.)

From Godsil's theorem, as $r \to \infty$, the condition "R admits a GRR" is equivalent to "R is neither a generalised dicyclic group, nor abelian of exponent greater than 2."

The corresponding result for Cayley digraphs (which does not require any families of groups to be excluded) was proved by Morris and Spiga in [120].

The strategy used in [120] (which was based on previous work in [10] by Babai and Godsil) to prove that almost every Cayley digraph is a DRR, involved three major pieces. One piece was to show that there are not many Cayley digraphs admitting digraph automorphisms that are also group automorphisms. A second piece of the proof involved considering the possibility that the group R has a proper nontrivial normal subgroup N, and there is a digraph automorphism that fixes every orbit of N setwise. This piece itself naturally divides into two parts. If $|N|$ is relatively small in comparison with $|R|$, then showing that roughly $2^{|R|/|N|}$ digraphs do not admit a particular type of automorphism is significant, while if $|N|$ is relatively large (for example if $|N| = |R|/c$ for some constant c) this sort of bound is not useful for our purposes. Conversely, if $|N|$ is relatively large then showing that roughly $2^{|N|}$ digraphs do not admit a particular type of automorphism is significant, but such a bound is not useful if $|N|$ is relatively small. So we need to combine bounds of each type to come up with an overall bound. The third and final piece of the proof involved considering the possible existence of digraph automorphisms that do not fix all orbits of any normal subgroup N of R.

While the second piece may not seem entirely natural, it is important to consider because it covers a possibility that does not readily succumb to induction. If a graph only admits automorphisms that fix every orbit of N setwise, then the quotient graph on the orbits of N may be in fact a GRR. The induced subgraph on a single orbit may very well also be a GRR, so an inductive argument will reduce a non-GRR to two smaller GRRs, making induction virtually impossible to use effectively.

Similarly to the results about existence of GRRs and DRRs, the requirement that a connection set for a graph must be inverse-closed creates complications that make the proof of the Babai-Godsil conjecture more difficult for graphs than for digraphs.

The first piece of the proof of the Babai-Godsil conjecture for graphs, showing that there are not many Cayley graphs admitting graph automorphisms that are also group automorphisms (unless the group is generalised dicyclic or abelian of exponent greater than 2) was accomplished by Spiga in [154]. Some of the main results from that work are also used in here, and we have included them as Theorem 4.0.12 and Proposition 4.0.13.

The goal of [119] was to complete the second piece of the proof: that is, to show that the number of Cayley graphs on R that admit nontrivial graph automorphisms that fix the vertex 1 and normalise some proper nontrivial normal subgroup N of R, is vanishingly small as a proportion of all Cayley graphs on R.

As in the work on DRRs, this problem naturally divides into the cases where the normal subgroup N is "large" or "small" relative to $|R|$. Our main results are Theorem 4.0.4 and Theorem 4.0.5, which we prove in Sections 4.2 and 4.3, respectively. In the case of graphs, it emerges that we also need to consider separately graph automorphisms that fix or invert every element of the group. We deal with these in Section 4.1, and this piece of our work applies whether or not R admits any proper nontrivial normal subgroup.

Theorem 4.0.4. [119, Theorem 1.5] *Let R be a finite group and let N be a non-identity proper normal subgroup of R. Then, the set*

$$\{S \subseteq R \mid S = S^{-1},\, R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R),\, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1\},$$

has cardinality at most $2^{\mathbf{c}(R)-\frac{|N|}{96}+2\log_2|R|+(\log_2|R|)^2+3}$. Moreover, if R is neither abelian of exponent greater than 2 nor generalised dicyclic, we may drop the condition "$R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$" in the definition of the set.

Theorem 4.0.5. [119, Theorem 1.6] *Let R be a finite group and let N be a non-identity proper normal subgroup of R. Then, the set*

$$\{S \subseteq R \,|S = S^{-1},\, R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R),\, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1, f \text{ fixes each } N\text{-orbit setwise}\}$$

has cardinality at most $2^{\mathbf{c}(R)-\frac{|R|}{192|N|}+(\log_2|R|)^2+3}$. Moreover, if R is neither abelian of exponent greater than 2 nor generalised dicyclic, we may drop the condition "$R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$" in the definition of the set.

By distinguishing the cases that $|N| \geq \sqrt{|R|}$ and $|R:N| \geq \sqrt{|R|}$, we obtain the following corollary.

Corollary 4.0.6. [119, Corollary 1.7] *Let R be a finite group and let N be a non-identity proper normal subgroup of R. Then, the set*

$$\{S \subseteq R \,|S = S^{-1},\, R = \mathbf{N}_{\mathrm{Aut}(R,S)}(R),\, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1, f \text{ fixes each } N\text{-orbit setwise}\}$$

has cardinality at most $2^{\mathbf{c}(R)-\frac{\sqrt{|R|}}{192}+2\log_2|R|+(\log_2|R|)^2+3}$. Moreover, if R is neither abelian of exponent greater than 2 nor generalised dicyclic, we may drop the condition "$R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$" in the definition of the set.

Prior to launching into the pieces of the proof mentioned above, we provide some additional background and introductory material.

4.0.1 General notation

Definition 4.0.7. Given a finite group R and $x \in R$, we let $o(x)$ denote the order of the element x and we let

$$\mathbf{I}(R) := \{x \in R \mid o(x) \leq 2\}$$

be the set of elements of R having order at most 2. Given a subset X of R, we write $\mathbf{I}(X) := X \cap \mathbf{I}(R)$. Given an inverse-closed subset X of R, we let

$$\mathbf{c}(X) := \frac{|X| + |\mathbf{I}(X)|}{2}.$$

Definition 4.0.8. Let A be an abelian group of even order and of exponent greater than 2, and let y be an involution of A. The *generalised dicyclic group* $\mathrm{Dic}(A,y,x)$ is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A\rangle$. A group is called generalised dicyclic if it is isomorphic to some $\mathrm{Dic}(A,y,x)$. When A is cyclic, $\mathrm{Dic}(A,y,x)$ is called a *dicyclic* or *generalised quaternion group*.

We let $\bar{\iota}_A : \mathrm{Dic}(A,y,x) \to \mathrm{Dic}(A,y,x)$ be the mapping defined by $(ax)^{\bar{\iota}_A} = ax^{-1}$ and $a^{\bar{\iota}_A} = a$, for every $a \in A$. In particular, $\bar{\iota}_A$ is an automorphism of $\mathrm{Dic}(A,y,x)$. The role of

the label "A" in $\bar{\iota}_A$ seems unnecessary, however we use this label to stress one important fact. An abstract group R might be isomorphic to $\mathrm{Dic}(A, y, x)$, for various choices of A. Therefore, since the automorphism $\bar{\iota}_A$ depends on A and since we might have more than one choice of A, we prefer a notation that emphasizes this fact.

It follows from [121, Section 2.1 and 4] that, if $D = \mathrm{Dic}(A, x, y)$ is generalized dicyclic over A, then either A is characteristic in D, or $D \cong Q_8 \times C_2^\ell$ for some $\ell \in \mathbb{N}$. In particular, when D is not isomorphic to $Q_8 \times C_2^\ell$, the automorphism $\bar{\iota}_A$ is uniquely determined by D.

When $D = Q_8 \times C_2^\ell$, the group D is generalized dicyclic over three distinct abelian subgroups; namely, if $Q_8 = \langle i, j\rangle$, then D is generalized dicyclic over $\langle i\rangle \times C_2^\ell$, $\langle j\rangle \times C_2^\ell$ and $\langle ij\rangle \times C_2^\ell$. In particular, we have three distinct options for the automorphism $\bar{\iota}_A$: one for each of these abelian subgroups. For simplicity, we denote by $\bar{\iota}_i, \bar{\iota}_j$ and $\bar{\iota}_k$ the corresponding automorphisms. It is not hard to check that $\bar{\iota}_k = \bar{\iota}_i\bar{\iota}_j$ and hence $\langle \bar{\iota}_i, \bar{\iota}_j\rangle$ is elementary abelian of order 4.

Definition 4.0.9. Let A be an abelian group. We let $\iota_A : A \to A$ denote the automorphism of A defined by $x^{\iota_A} = x^{-1}\ \forall x \in A$. Very often, we drop the label A from ι_A because this should cause no confusion.

In what follows we use the following facts repeatedly.

Remark 4.0.10. Let X be a finite group. Since a chain of subgroups of X has length at most $\log_2(|X|)$, X has a generating set of cardinality at most $\lfloor \log_2(|X|)\rfloor \leq \log_2(|X|)$.

Any automorphism of X is uniquely determined by its action on the elements of a generating set for X. Therefore $|\operatorname{Aut}(X)| \leq |X|^{\lfloor \log_2(|X|)\rfloor} \leq 2^{(\log_2(|X|))^2}$.

Lemma 4.0.11. *Let R be a finite group and let X be an inverse-closed subset of X. The number of inverse-closed subsets S of X is $2^{\mathbf{c}(X)}$. In particular, R has $2^{\mathbf{c}(R)}$ inverse-closed subsets.*

Proof. Given an arbitrary inverse-closed subset S of X, $S \cap \mathbf{I}(X)$ is an arbitrary subset of $\mathbf{I}(X)$ whereas in $S \cap (X \setminus \mathbf{I}(X))$ the elements come in pairs, where each element is paired up to its inverse. Thus the number of inverse-closed subsets of X is

$$2^{|\mathbf{I}(X)|} \cdot 2^{\frac{|X\setminus \mathbf{I}(X)|}{2}} = 2^{\mathbf{c}(X)}.$$

The last statement follows using $X = R$. □

The following important results by the third author deal with the case where there is a graph automorphism that is also a group automorphism of R.

Theorem 4.0.12 ([154], Lemma 2.7)**.** *Let R be a finite group and let φ be a non-identity automorphism of R. Then, one of the following holds*

1. *the number of φ-invariant inverse-closed subsets of R is at most $2^{\mathbf{c}(R)-\frac{|R|}{96}}$,*
2. *$\mathbf{C}_R(\varphi)$ is abelian of exponent greater than 2 and has index 2 in R, R is a generalized dicyclic group over $\mathbf{C}_R(\varphi)$ and $\varphi = \bar{\iota}_{\mathbf{C}_R(\varphi)}$,*
3. *R is abelian of exponent greater than 2 and φ is the automorphism of R mapping each element to its inverse.*

Proposition 4.0.13 ([154], Proposition 2.8)**.** *Let R be a finite group and suppose that R is not an abelian group of exponent greater than 2 and that R is not a generalized dicyclic group. Then the set*

$$\{S \subseteq R \mid S = S^{-1}, R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\}$$

has cardinality at most $2^{\mathbf{c}(R)-|R|/96+(\log_2|R|)^2}$.

Notation 2. *With R a finite group that is neither abelian of exponent greater than 2 nor generalised dicyclic, we define*

$$\mathcal{S}_N = \{S \subseteq R \mid S = S^{-1}, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1\},$$

so that $|\mathcal{S}_N|$ is a value we aim to bound to prove Theorem 4.0.4. We divide $\mathcal{S}_N$ into three subsets:

$$\mathcal{S}_N^1 := \{S \in \mathcal{S}_N \mid R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\},$$
$$\mathcal{T}_N := \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \mid \exists x \in R \text{ and } \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ and } x^f \notin \{x, x^{-1}\}\},$$
$$\mathcal{U}_N := \mathcal{S}_N \setminus \mathcal{S}_N^1 \setminus \mathcal{T}_N.$$

so

$$\mathcal{S}_N = \mathcal{S}_N^1 \cup \mathcal{T}_N \cup \mathcal{U}_N.$$

Observe that

$$\mathcal{U}_N = \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \mid \forall f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ we have } x^f \in \{x, x^{-1}\} \forall x \in R\}.$$

Proposition 4.0.13 already provides us with a bound for $|\mathcal{S}_N^1|$. In the next section, we will show that $|\mathcal{U}_N| = 0$.

4.1 Graph automorphisms that fix or invert every group element

The bulk of this section consists of a long lemma in which we show that if a nontrivial permutation that fixes or inverts every element of a group exists, then the normaliser of R in the appropriate group is in fact larger than R. This means that any connection sets that could arise in $\mathcal{U}_N$ have actually already arisen in $\mathcal{S}_N^1$, and therefore do not appear in $\mathcal{U}_N$.

Lemma 4.1.1. *Let G be a subgroup of $\mathrm{Sym}(R)$ with $R < G$ and with the property that $r^g \in \{r, r^{-1}\}$, for every $r \in R$ and for every $g \in G_1$. Then $\mathbf{N}_G(R) > R$.*

Proof. We argue by contradiction and, among all groups satisfying the hypothesis of this lemma, we choose G with $|R||G|$ as small as possible and with

$$R = \mathbf{N}_G(R).$$

In this proof, we denote by r^g the image of the point $r \in R$ via the permutation g and we denote by $r^{\iota_g} := g^{-1}rg$ the conjugation of r via g.

Let M be a subgroup of G with $R < M$. For every $r \in R$ and for every $x \in M_1 = M \cap G_1$, $r^x \in \{r, r^{-1}\}$, and, from the modular law,

$$R = M \cap R = M \cap \mathbf{N}_G(R) = \mathbf{N}_M(R).$$

Therefore, by the minimality of our counterexample, we get $M = G$. As M was an arbitrary subgroup of G with $R < M$, we deduce

$$R \text{ is a maximal subgroup of } G. \tag{4.1.1}$$

Let K be the core of R in G, that is, $K := \bigcap_{g \in G} R^g$.

We claim that

$$\text{the core of } R \text{ in } G \text{ is } 1. \tag{4.1.2}$$

To prove this claim we argue by contradiction and we suppose that $K \neq 1$. Let $\bar{G}$ be the permutation group induced by G on the action on K-orbits. Moreover, we let $^- \colon G \to \bar{G}$ denote the natural projection.

Let H be the kernel of $^-$. Thus H is the largest subgroup of G fixing each K-orbit setwise and $H \leq G_1K$. Since R is a maximal subgroup of G and $R \leq RH \leq G$, we have that either $R = RH$ or $G = RH$.

In the first case, $H \leq R$ and, since $H \leq G_1K$, from the modular law we obtain $H \leq R \cap G_1K = (R \cap G_1)K = K$, that is, $H = K$. Moreover, as $H = K \leq R$, we have $\bar{R} = \mathbf{N}_{\bar{G}}(\bar{R})$. Now, $\bar{R}$ is a regular subgroup of $\bar{G} \leq \mathrm{Sym}(\bar{R})$ and, for every $\bar{r} \in \bar{R}$ and for every $\bar{g} \in \bar{G}_1$, we have $\bar{r}^{\bar{g}} \in \{\bar{r}, \bar{r}^{-1}\}$. Using our assumption that $K \neq 1$, we get that $|\bar{R}| < |R|$, and by the minimality of our couterexample we have that $\bar{G} = G/K = R/K = \bar{R}$. That is, $G = R$ contradicting the fact that R is a proper subgroup of G.

So the second case holds, and $G = RH$, so G_1 acts trivially on K-orbits. In other words, G_1 fixes each K-orbit setwise. Thus $H = KG_1$, and consequently

$$KG_1 \trianglelefteq G. \tag{4.1.3}$$

Suppose there exist $x \in G_1$ and $r \in R$ such that $r^x = r^{-1}$ and $o(rK) \geq 3$. Then $r^x = r^{-1} \in r^{-1}K = (rK)^{-1} \neq rK$, contradicting the fact that G_1 fixes each K-orbit. This shows that,

$$\text{for every } x \in G_1 \text{ and for every } r \in R \text{ either } r^x = r \text{ or } o(rK) \leq 2. \tag{4.1.4}$$

Let L be the subgroup of R fixed pointwise by G_1, that is, $L := \{r \in R \mid G_r = G_1\}$. (The set L is indeed a subgroup of R, because it is a block of imprimitivity for the action of G on R containing the point 1.) Clearly, $L < R$, because $G_1 \neq 1$. Now, from (4.1.4), we deduce that, for every $r \in R \setminus L$, $o(rK) \leq 2$. Hence,

$$\text{every element in } \frac{R}{K} \setminus \frac{KL}{K} \text{ is an involution.} \tag{4.1.5}$$

Now, by (4.1.5), we must have $\langle xK \in R/K \mid x^2 \notin K\rangle \leq L/K$. Since either $|R/K : \langle xK \in R/K \mid x^2 \notin K\rangle| = 2$ or R/K is a 2-group, we deduce that one of the following holds

1. R/K is an elementary abelian 2-group,
2. $R = KL$,
3. $|R : KL| = 2$ and every element in $R/K \setminus KL/K$ is an involution.

In what follows, we analyze these three alternatives.

Case (1)

Since R/K and G_1 are elementary abelian 2-groups, we deduce that G/K is a 2-group. From $R/K < G/K$, it follows that $\mathbf{N}_{G/K}(R/K) > R/K$. So $\mathbf{N}_G(R) > R$, but this contradicts our choice of G and R.

Case (2)

Let $f \in G_1$ with $f \neq 1$. Now, as G_1 normalizes K, the action of f on the points in K coincides with the action of f by conjugation on K. Thus, $k^{\iota_f} = k^f \in \{k, k^{-1}\}$, for every $k \in K$. In particular, ι_f is a non-trivial automorphism of K with the property that it maps each element to itself or to its inverse (so every inverse-closed subset of K is invariant under ι_f). Therefore using Theorem 4.0.12 only one of the following holds true:

- K is abelian of exponent greater than 2 and $\iota_f = \iota$ is the automorphism inverting each element of K,

- K is generalised dicyclic over an abelian subgroup A of exponent greater than 2 and $\iota_f = \bar{\iota}_A$,
- $K \cong Q_8 \times C_2^\ell$, for some $\ell \geq 0$, and $\iota_f \in \{\bar{\iota}_i, \bar{\iota}_j, \bar{\iota}_k\}$.

Since $R = KL$ and since G_1 fixes L pointwise, the action of $g \in G_1$ on R is uniquely determined once the action of g on K is determined. Since we have at most four choices for the action of $g \in G_1$ on K, we deduce that $|G_1|$ divides 4. If $|G_1| = 2$, then $|G : R| = 2$ and hence $R \trianglelefteq G$, which contradicts $R = \mathbf{N}_G(R)$. Thus $4 = |G_1| = |G : R|$ and $K \cong Q_8 \times C_2^\ell$, for some $\ell \geq 0$.

Since $|G : R| = 4$, the transitive action of G on the right cosets of R gives rise to a permutation group of degree 4 and hence G/K is isomorphic to a transitive subgroup of Sym(4). As $R/K = \mathbf{N}_{G/K}(R/K)$, we deduce that G/K is isomorphic to either Sym(4) or Alt(4).

If R/K were a 2-group, we reach a contradiction using the same argument as in Case (1). So R/K is a maximal subgroup of G/K which is not a 2-group, hence R/K isomorphic to either Sym(3) or Alt(3).

Let C be a Sylow 3-subgroup of R. Thus $C = \langle c \rangle$ is a cyclic group of order 3. Since K is a 2-group and $R = KL$, replacing C by a suitable R-conjugate, from Sylow's theorem, we can assume that $C \leq L$. Let $k \in K$ with $k \notin L$. As k is not fixed by each element of G_1, there exists $x \in G_1$ such that $k^x = k^{-1} \neq k$. Now, as $c^{x^{-1}} = c$, we obtain

$$(ck)^x = c^{kx} = c^{x^{-1}kx} = c^{k^{\iota_x}} = c^{k^{-1}} = ck^{-1}. \tag{4.1.6}$$

On the other hand, $(ck)^x \in \{ck, (ck)^{-1}\}$. If $(ck)^x = ck$, then we deduce $k = k^{-1}$, contradicting the fact that $k^x \neq k$. If $(ck)^x = (ck)^{-1}$, we deduce $k^{-1}c^{-1} = ck^{-1}$ and hence $k^{-1} = ck^{-1}c = c^2(k^{-1})^{\iota_c}$. Again we obtain a contradiction because k and k^{ι_c} belong to K but $c^2 \notin K$.

Case (3)

Before proceeding with this case, we collect some information on G/K. Observe that in this case, R/K is a generalized dihedral group over the abelian group KL/K. Consider the set Ω of the right cosets of R/K in G/K. By (4.1.1) R/K is a maximal subgroup of G/K. So G/K is a primitive permutation with generalised dihedral point stabilisers.

These groups were classified in [49, Lemma 2.2]. Using this and the fact that G_1 is 2-elementary abelian group, the only possibility that can occur is that G/K is a primitive group of affine type of degree $|R : K| = |G_1|$. Since $G = G_1R$ and $R \cap G_1 = 1$, G_1K/K acts regularly on Ω. Moreover, as $KG_1 \trianglelefteq G$ by (4.1.3), G_1K/K is the socle of G/K. Since every element of G_1 is an involution (it fixes or inverts each element of R), then G_1K/K is an elementary abelian 2-group.

Now, R/K acts by conjugation irreducibly as a linear group over the elementary abelian 2-group G_1K/K. Let $\ell K \in LK/K \setminus \{K\}$. Since LK/K is abelian, then $\mathbf{C}_{G_1K/K}(\ell K) = \{aK \in G_1K/K \mid \ell^{-1}a\ell K = aK\}$ is stable under the conjugation by uK, for every $uK \in LK/K$. Further, since $R/K = \langle rK, LK/K \rangle$, where $rK = r^{-1}K$, and $r^{-1}\ell rK = \ell^{-1}K$, for every $\ell K \in LK/K$, then $\mathbf{C}_{G_1K/K}(\ell K)$ is stable under the conjugation by xK. In other words, we proved that $\mathbf{C}_{G_1K/K}(\ell K)$ is a proper R-submodule of the irruducible R-module G_1K/K, and consequently $\mathbf{C}_{G_1K/K}(\ell K)$ is trivial. Summing up, KL/K is abelian and $\mathbf{C}_{G_1K/K}(\ell K)$ is trivial for every $\ell K \in LK/K \setminus \{K\}$. Thus KL/K is a cyclic group of odd order. Moreover, as the socle G_1K/K has even order, $|KL/K|$ must be odd. We let $t := |KL/K|$. At this point, the reader might find it useful to consider Figure 4.1. Since KL/K is cyclic, there exists $c \in L$ with $\langle c \rangle K = KL$ and with $o(cK) = t$.

Suppose now that $K \not\leq L$ and let $k \in K \setminus L$. As k is not fixed by each element of G_1, there exists $x \in G_1$ with $k^x = k^{-1} \neq k$. Now, since x fixes c, we are in position to use the same argument as in Case (2). That is (4.1.6) holds, and consequently either $k = k^{-1}$ or $c^2 \in K$. Since $k \neq k^{-1}$ and $o(cK) = t$ is odd, in both cases we get a contradiction.

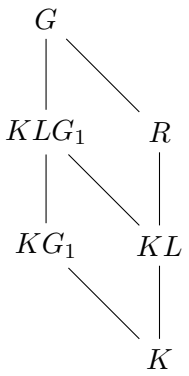

Figure 4.1: Local structure of $\bar{G}$

We conclude that $K \leq L$. (For the proof here, it might be useful again considering Figure 4.1.) In particular, $KL = L$. Fix $r \in R \setminus L$. As $|R : L| = 2$, we have $R = L \cup rL$. Now, LG_1 fixes L and rL setwise. The action induced by LG_1 on L is the regular action of L because G_1 fixes L pointwise. As $LG_1 \trianglelefteq G$, we must also have that the action of LG_1 on rL is simply the regular action of L. In particular, for every $x \in G_1$, there exists $\ell_x \in L$ with the property that

$$(r\ell)^x = r\ell\ell_x, \ \forall \ell \in L.$$

The set $\{\ell_x \mid x \in G_1\}$ forms a subgroup of L, which we denote by T. As G_1 is elementary abelian, so is T.

Summing up, we have

$$\ell^x = \ell, \quad (r\ell)^x = r\ell\ell_x, \ \forall x \in G_1, \forall \ell \in L.$$

Using this and the fact that T is a group we see that, if $x \in G_1$ fixes some point in rL, then $\ell_x = 1$ and consequently x fixes all points in rL. Further, x fixes all points in L, hence $x = 1$. Therefore, each element in $G_1 \setminus \{1\}$ acts fixed-point-freely on rL. Now, let $x \in G_1 \setminus \{1\}$. Since $(r\ell)^x \in \{r\ell, (r\ell)^{-1}\}$ for each $\ell \in L$ we deduce that $(r\ell)^x = (r\ell)^{-1}$ for every $\ell \in L$. Hence $G_1 \setminus \{1\} = \{x\}$. Therefore, $|G_1| = 2$ and $|G : R| = 2$ contradicting the fact that $\mathbf{N}_G(R) = R$.

We have shown that none of the three alternatives is possible. Therefore, we obtain a contradiction, and the contradiction has arisen from assuming $K \neq 1$. Hence $K = 1$, which is our original claim (4.1.2).

Now, as R is maximal in G and as R is core-free in G, we may view G as a primitive permutation group on the set $\Omega = G \backslash R$ of right cosets of R in G. Observe that in this action G_1 acts as a regular subgroup and it is an elementary abelian 2-group which itself is core-free in G.

The primitive permutation groups containing an abelian regular subgroup have been classified by Li in [85]. Applying this classification [85, Theorem 1.1] to our group G in its action on Ω and to its elementary abelian regular subgroup G_1, we deduce that one of the following holds:

1. G is an affine primitive permutation group,

2. the set Ω admits a Cartesian decomposition $\Omega = \Delta^\ell$ (for some $\ell \geq 1$) and the primitive group G preserves this cartesian decomposition; moreover, $\tilde{T}^\ell \leq G \leq \tilde{T} \mathrm{wr} \, \mathrm{Sym}(\ell)$, where the action of $\tilde{T} \wr \mathrm{Sym}(\ell)$ on Δ^ℓ is the natural primitive product action. The group $\tilde{T}$ is either $\mathrm{Alt}(\Delta)$ or $\mathrm{Sym}(\Delta)$, $G_1 = G_{1,1} \times G_{1,2} \times \cdots \times G_{1,\ell}$ with $G_{1,i} \leq \tilde{T}$ and with $G_{1,i}$ acting regularly on Δ, for each i.

Now, we shall see that neither of these two alternatives is possible.

Case (1)

Let V be socle of G. Thus $V \trianglelefteq G$ and V is an elementary abelian 2-group. Observe that

$$G = VR = G_1R,$$

where the first equality follows from the fact that V acts transitively on Ω with point stabiliser R and the second equality follows because G acts also transitively on R with point stabilizer G_1. Moreover,

$$V \cap R = 1 = G_1 \cap R,$$

where the first equality follows because V acts regularly on Ω with point stabilizer R and the second equality follows because R acts regularly on itself with point stabilizer G_1.

Since G_1 is a regular subgroup of the affine group G, from [36, Corollary 5 (1)], we deduce

$$V \cap G_1 \neq 1. \tag{4.1.7}$$

Let

$$N := \mathbf{N}_G(V \cap G_1) \quad \text{and let} \quad Q := \mathbf{N}_R(V \cap G_1).$$

Since G_1 is abelian, we have $G_1 \leq N$ and hence

$$N = N \cap G = N \cap RG_1 = (N \cap R)G_1 = QG_1.$$

Similarly, since V is abelian, we have $V \leq N$ and hence

$$N = N \cap G = N \cap RV = (N \cap R)V = QV.$$

Thus

$$N = QG_1 = QV. \tag{4.1.8}$$

Let $r \in R$ and let $v \in V \cap G_1$. We recall that $r^v \in \{r, r^{-1}\}$.

If $r^v = r$, then $1^r = r = r^v = 1^{rv}$ and hence $rvr^{-1} \in G_1$. If $r^v = r^{-1}$, then $1^{r^{-1}} = r^{-1} = r^v = 1^{rv}$ and hence $rvr = r^2(r^{-1}vr) \in G_1$. As $V \trianglelefteq G$, we have $r^{-1}vr \in V$ and hence $r^2V \in G_1V/V$. Since all the elements of G_1V/V have order at most 2, it follows that $r^4V = V$, that is $r^4 \in V \cap R = 1$. This shows that, if $o(r) \neq 4$, then $r^{-1}vr \in V \cap G_1$. Therefore, all elements of R of order different from 4 normalise $V \cap G_1$ and hence they all lie in Q.

This shows that $R \setminus Q$ is either empty, or contains only elements of order 4. In the first case (4.1.8) yields $\mathbf{N}_G(V \cap G_1) = N = QV = RV = G$, that is $V \cap G_1 \trianglelefteq G$. Since V is the unique minimal normal subgroup of G and since $V \cap G_1 \neq 1$ by (4.1.7), we deduce that $V = V \cap G_1$, that is, $V \leq G_1$. However, this contradicts the fact that G_1 is core-free in G. Thus

$$Q < R \text{ and every element in } R \setminus Q \text{ has order 4.}$$

For every $r \in R \setminus Q$, r^2 does not have order 4, so $r^2 \in Q$. This shows that Q contains the square of each element of R, hence

$$Q \trianglelefteq R \tag{4.1.9}$$

and R/Q is an elementary abelian 2-group.

Let $x \in G_1$ and let $r \in R$. If $r^x = r$, then $rxr^{-1} \in G_1 \leq G_1Q = N$. If $r^x = r^{-1}$, then $rxr \in G_1$ and hence $rxr = r^2(r^{-1}xr) \in G_1 \leq G_1Q = N$. Since $r^2 \in Q$, we deduce that $r^{-2} \cdot r^2(r^{-1}xr) = r^{-1}xr \in N$. We have shown that,

$$\text{for every } r \in R,\ r^{-1}G_1r \leq N. \tag{4.1.10}$$

From (4.1.9) and (4.1.10), we deduce that R normalises $G_1Q = N$. Since G_1 also normalizes N, we have that $RG_1 = G$ normalises N, that is,

$$QV = QG_1 = N \trianglelefteq G. \tag{4.1.11}$$

Since $Q \trianglelefteq R$ and since R is a maximal subgroup of G by (4.1.1), we deduce that either $\mathbf{N}_G(Q) = G$ or $\mathbf{N}_G(Q) = R$. If $\mathbf{N}_G(Q) = G$, then Q is a normal subgroup of G contained in the core-free subgroup R. Therefore $Q = 1$. From (4.1.8), we have $G_1 = QG_1 = N = QV = V$, contradicting the fact that G_1 is core-free in G. Thus

$$\mathbf{N}_G(Q) = R. \tag{4.1.12}$$

When G is viewed as a permutation group on R, QG_1 is the setwise stabilizer in G of $Q \subseteq R$, hence we can consider the permutation group induced by $N = QG_1$ in its action on Q. From (4.1.12), we have $\mathbf{N}_N(Q) = N \cap R = QG_1 \cap R = Q(G_1 \cap R) = Q$. Let H be the kernel of the permutational representation of N on Q. Note that $H \leq G_1$. Now, QH/H is a regular subgroup of $N/H \leq \mathrm{Sym}(Q)$ and, for every $rH \in QH/H$ and for every $gH \in G_1/H$, we have $r^gH \in \{rH, r^{-1}H\}$. If $\mathbf{N}_{N/H}(QH/H) = QH/H$, from the minimality of our counterexample, we deduce that either $N = G$ or G_1 acts trivially on Q. In the first case, $G = N = \mathbf{N}_G(V \cap G_1)$, that is $G_1 \cap V$ is a normal subgroup of G. Since V is the unique minimal subgroup of G, and since $V \cap G_1 \neq 1$ by (4.1.7), we deduce that $V = V \cap G_1$, and consequently, $V = G_1$. However, this contradicts the fact that G_1 is core-free in G. Therefore G_1 fixes Q pointwise, that is, G_1 is the kernel of the action of $N = QG_1$ on Q and hence

$$G_1 \trianglelefteq N = QG_1 = VG_1. \tag{4.1.13}$$

Let

$$U := \langle G_1^g \mid g \in G \rangle.$$

Observe that $U \trianglelefteq G$. From (4.1.11), for every $g \in G$, we have $G_1^g \leq N^g = N$, that is $U \leq N$. Moreover, for every $g \in G$, from (4.1.13), we have $G_1^g \trianglelefteq N^g = N$. Since G_1 is an elementary abelian 2-group, then each G_1^g is a normal 2-subgroup of N, for every $g \in G$. Consequently U is a normal 2-subgroup of G. In particular, $U \cap R$ is a normal 2-subgroup of R.

Since V is an irreducible $\mathbb{F}_2R$-module and $U \cap R \trianglelefteq R$, we deduce that V is completely reducible $\mathbb{F}_2(U \cap R)$-module by Clifford's theorem. Since V has characteristic 2 and since $U \cap R$ is a 2-group, this can happen only when

$$U \cap R = 1.$$

Since V is the unique minimal normal subgroup of G and since $U \trianglelefteq G$, we have $V \leq U$. Further, $U = U \cap G = U \cap G_1R = (U \cap R)G_1 = G_1$ and hence $V = G_1$. This is a contradiction because V is normal in G but G_1 is core-free in G.

Therefore we can assume that $\mathbf{N}_{N/H}(QH/H) > QH/H$. That is, there exists a non-identity element $g \in G_1$ normalizing QH/H. Hence, for every $r \in Q$, $g^{-1}rg = uh$, for some $u \in Q$ and for some $h \in H$. Since $g \in G_1$, and $r^g \in \{r, r^{-1}\}$, we get $u = u^h = 1^{uh} = 1^{g^{-1}rg} = r^g$. This means that $g^{-1}rgH \in \{rH, (rH)^{-1}\}$ for every $r \in Q$, and consequently ι_g is a non-identity automorphism of QH/H with the property that $(rH)^{\iota_g} \in \{rH, (rH)^{-1}\}$, for every $rH \in QH/H$. Thus from Theorem 4.0.12, $Q \cong QH/H$ is either an abelian group of exponent greater than 2 or a generalized dicyclic group.

Since V is an irreducibly $\mathbb{F}_2R$-module and $\mathbf{O}_2(Q) \trianglelefteq R$, we deduce that V is completely reducible $\mathbb{F}_2(Q)$-module by Clifford's theorem. Since V has characteristic 2 and since $\mathbf{O}_2(Q)$ is a 2-group, this can happen only when

$$\mathbf{O}_2(Q) = 1. \tag{4.1.14}$$

If Q is a generalised dicyclic group, that is, $Q = Dic(A, y, x)$, with A an abelian group of even order and of exponent greater than 2, and y an involution in A, then $\langle y \rangle$ is a characteristic subgroup of order 2, which contradicts (4.1.14). Thus Q is an abelian group, and Q has odd order by (4.1.14). Since $N = QV = QG_1$ by (4.1.11), and since $V \trianglelefteq N$, then V is the unique Sylow 2-subgroup of N. As $|G_1| = |V|$ and $G_1 \leq N$, we get $G_1 = V$. This contradicts the fact that G_1 is core-free in G.

Case (2)

We identify Ω with Δ^ℓ, and we recall that $\mathrm{Alt}(\Delta)^\ell \leq G \leq \mathrm{Sym}(\Delta) \mathrm{wr} \mathrm{Sym}(\ell)$. Let $\delta_1 \in \Delta$ and let $\omega = (\delta_1, \ldots, \delta_1) \in \Omega$. Since R is a maximal subgroup of G, replacing R by a suitable conjugate we may suppose that $R = G_\omega$. Now, $\mathrm{Alt}(\Delta \setminus \{\delta_1\})^\ell \leq R$. Further, recall that $G_1 = G_{1,1} \times G_{1,2} \times \cdots \times G_{1,\ell}$, where $G_{1,i} \leq \mathrm{Sym}(\Delta)$ is an elementary abelian 2-subgroup of acting regularly on Δ, for each i. Let $\delta_2 \in \Delta \setminus \{\delta_1\}$. As $G_{1,1} \leq \mathrm{Sym}(\Delta)$ is transitive on Δ, there exists $g \in G_{1,1}$ such that $\delta_1^g = \delta_2$ and, since $G_{1,1}$ is a 2-group, rearranging the points from δ_3 onwards if necessary, we can assume

$$g = (\delta_1\, \delta_2)(\delta_3\, \delta_4)(\delta_5\, \delta_6)(\delta_7\, \delta_8) \cdots .$$

(Observe that $|\Delta| \geq 8$ because $|\Delta|$ is a power of 2 larger than 5.) Let consider the 3-cycle $r = (\delta_2\, \delta_3\, \delta_4)$ and observe that it lies in R because it fixes the point δ_1 and $R = G_\omega$.

In this new setting, to look at the original action of G on R, we have to identify the set R with the set of right cosets of G_1 in G. In particular,

$$G_1 r = G_1(\delta_2\, \delta_3\, \delta_4)$$

is such a point. We have

$$G_1 rg = G_1(\delta_2\, \delta_3\, \delta_4)(\delta_1\, \delta_2)(\delta_3\, \delta_4)(\delta_5\, \delta_6)(\delta_7\, \delta_8) \cdots = G_1(\delta_1\, \delta_2\, \delta_4)(\delta_5\, \delta_6)(\delta_7\, \delta_8) \cdots .$$

Since neither $rgr^{-1} \in G_1$ nor $rgr \in G_1$, then $G_1 rg \notin \{G_1 r, G_1 r^{-1}\}$. This contradicts our hypotheses.

We have shown that neither of the alternatives is possible. Therefore, we have contradicted the existence of such G and R. □

This is sufficient to show that $\mathcal{U}_N$ is empty.

Corollary 4.1.2. *When R is neither abelian of exponent greater than 2 nor generalised dicyclic, $\mathcal{U}_N = \varnothing$.*

Proof. Recall from Notation 2 that when R is neither abelian of exponent greater than 2 nor generalised dicyclic

$$\mathcal{S}_N = \{S \subseteq R \mid S = S^{-1}, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1\},$$

while

$$\mathcal{S}_N^1 = \{S \in \mathcal{S}_N \mid R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\},$$

and

$$\mathcal{U}_N = \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \mid \forall f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ we have } x^f \in \{x, x^{-1}\} \forall x \in R\}.$$

Notice that the set of all elements of $\mathrm{Aut}(\Gamma(R, S))$ that fix the vertex 1 and fix or invert every other element of R is a subgroup of $\mathrm{Aut}(\Gamma(R, S))$. By Lemma 4.1.1 with G being generated by R and the set of all such elements, we have $\mathcal{U}_N = \varnothing$. This is because every set that could lie in $\mathcal{U}_N$ must appear in $\mathcal{S}_N^1$. □

4.2 Groups with a "large" normal subgroup

We begin this section with a lovely little general result showing that in a non-abelian group, there cannot be a group automorphism α such that the result of computing nn^α is constant for more than 3/4 of the group elements (and in fact in an abelian group, this can only happen if α is the automorphism that inverts every group element). For the special case where α is trivial and the constant is 1, our proof relies on (so does not replace) classical work by Liebeck and MacHale [88].

Lemma 4.2.1. *Let N be a group, let α be an automorphism of N and let $t \in N$. Then one of the following holds:*

1. $|\{n \in N \mid nn^\alpha = t\}| \leq 3|N|/4$,
2. *N is abelian, $t = 1$ and $n^\alpha = n^{-1}$ $\forall n \in N$.*

Proof. We let $\mathcal{S} := \{n \in N \mid nn^\alpha = t\}$. Suppose $|\mathcal{S}| > 3|N|/4$. Observe that, for every $n \in \mathcal{S}$, we have $n^\alpha = n^{-1}t$.

As $|\mathcal{S}| > 3|N|/4$, we have $\mathcal{S}^{\alpha^{-1}} \cap \mathcal{S} \neq \varnothing$. Let $n \in \mathcal{S}^{\alpha^{-1}} \cap \mathcal{S}$, so that $n, n^\alpha \in \mathcal{S}$. Then $nn^\alpha = t$ because $n \in \mathcal{S}$, and $n^\alpha (n^\alpha)^\alpha = t$ because $n^\alpha \in \mathcal{S}$. Therefore, $t = n^\alpha (n^\alpha)^\alpha = (nn^\alpha)^\alpha = t^\alpha$, that is, $t = t^\alpha$.

As $|\mathcal{S}| > 3|N|/4$, we have $|\mathcal{S}\cdot t \cap \mathcal{S}| = |\mathcal{S}\cdot t| + |\mathcal{S}| - |\mathcal{S}\cdot t \cup \mathcal{S}| > 3|N|/4 + 3|N|/4 - |N| = |N|/2$. Let $n \in \mathcal{S}\cdot t \cap \mathcal{S}$. Then $n = mt$, for some $m \in \mathcal{S}$. Therefore

$$t^{-1}m^{-1}\cdot t = n^{-1}t = n^\alpha = (mt)^\alpha = m^\alpha t^\alpha = m^{-1}t \cdot t.$$

From this we obtain $mt = t^{-1}m$, that is, $t^m = t^{-1}$. As $n = mt$, we also have $t^n = t^{-1}$. We have shown that, for every $n \in \mathcal{S}\cdot t \cap \mathcal{S}$, we have $t^n = t^{-1}$. For every two elements $n_1, n_2 \in N$ with $t^{n_1} = t^{-1} = t^{n_2}$, we have $n_1 n_2^{-1} \in \mathbf{C}_N(t)$. Therefore, we deduce that $|N|/2 < |\mathcal{S}\cdot t \cap \mathcal{S}| \leq |\mathbf{C}_N(t)|$. Thus $N = \mathbf{C}_N(t)$ and $t \in \mathbf{Z}(N)$. Moreover, for every $n \in \mathcal{S}t \cap \mathcal{S}$, we have $t^n = t^{-1}$ and, as $t \in \mathbf{Z}(N)$, we have $t^n = t$. Thus $t^2 = 1$. Summing up, t is a central element of N of order at most 2.

Suppose that $t = 1$. Then $\mathcal{S} = \{n \in N \mid n^\alpha = n^{-1}\}$. In particular, α is an automorphism inverting more than $3|N|/4$ of the elements of N. From a classical result of Liebeck and MacHale [88], we deduce that N is abelian and α is the automorphism inverting each element of N, that is, $n^\alpha = n^{-1}$ $\forall n \in N$.

Suppose that $t \neq 1$. Since $t \in \mathbf{Z}(N)$ and since $t^\alpha = t$, we may consider the group $\bar{N} := N/\langle t\rangle$ and the induced automorphism $\bar{\alpha} : \bar{N} \to \bar{N}$. In particular, in $\bar{N}$, the set $\mathcal{S}$ projects to the set $\bar{\mathcal{S}} = \{\bar{n} \in \bar{N} \mid \bar{n}^{\bar{\alpha}} = \bar{n}^{-1}\}$. Since this set has cardinality larger than $3|\bar{N}|/4$, applying again the theorem of Liebeck and MacHale, we deduce that $\bar{N}$ is abelian and $\bar{n}^{\bar{\alpha}} = \bar{n}^{-1}$ $\forall \bar{n} \in \bar{N}$. It follows that, for every $n \in N$, $n^\alpha \in \langle t\rangle n^{-1} = \{n^{-1}, tn^{-1}\}$.

Set $\mathcal{S}' := \{n \in N \mid n^\alpha = n^{-1}\}$. In particular, $\{\mathcal{S}, \mathcal{S}'\}$ is a partition of N and $|\mathcal{S}'| = |N \setminus \mathcal{S}| < |N|/4$.

Suppose that N is not abelian. As $|N \setminus \mathbf{Z}(N)| \geq |N|/2$ and $|\mathcal{S}| > 3|N|/4$, there exists $n \in (N \setminus \mathbf{Z}(N)) \cap \mathcal{S}$. Since $\bar{N}$ is abelian, we have $[N, N] = \langle t\rangle$, from which it follows that $|N : \mathbf{C}_N(n)| = 2$. For every $m \in \mathbf{C}_N(n) \cap \mathcal{S}$, we have $(nm)^\alpha = n^\alpha m^\alpha = n^{-1}t \cdot m^{-1}t = n^{-1}m^{-1}t^2 = m^{-1}n^{-1} = (nm)^{-1}$ and hence $nm \in \mathcal{S}'$. This shows that $n(\mathbf{C}_N(n) \cap \mathcal{S}) \subseteq \mathcal{S}'$. Now,

$$\begin{aligned}|\mathcal{S}'| &\geq |n(\mathbf{C}_N(n) \cap \mathcal{S})| = |\mathbf{C}_N(n) \cap \mathcal{S}| = |\mathbf{C}_N(n)| + |\mathcal{S}| - |\mathbf{C}_N(n) \cup \mathcal{S}| \\ &\geq |\mathbf{C}_N(n)| + |\mathcal{S}| - |N| = |\mathcal{S}| - \frac{|N|}{2} > \frac{|N|}{4},\end{aligned}$$

contradicting the fact that $|\mathcal{S}'| < |N|/4$. This contradiction has arisen assuming that N is not abelian and hence N is abelian.

Now, for every $n, m \in \mathcal{S}$, we have $(nm)^\alpha = n^{-1}t \cdot m^{-1}t = n^{-1}m^{-1}t^2 = (nm)^{-1}$ and hence $nm \in \mathcal{S}'$. Therefore, $\mathcal{S} \cdot \mathcal{S} \subseteq \mathcal{S}'$, but this is impossible because $|\mathcal{S}'| < |\mathcal{S}|$. This contradiction has arisen from assuming $t \neq 1$ and hence $t = 1$ and the proof is now complete. □

We will also require a similar result that considers when inversion is applied after the automorphism.

Lemma 4.2.2. *Let N be a group, let α be an automorphism of N and let $t \in N$. Then one of the following holds:*

1. $|\{n \in N \mid n(n^\alpha)^{-1} = t\}| \leq 3|N|/4$,
2. $t = 1$ *and* $n^\alpha = n \ \forall n \in N$.

Proof. The proof of this is very similar to the proof of Lemma 4.2.1, so we omit some of the repeated details.

We let $\mathcal{S} := \{n \in N \mid n(n^\alpha)^{-1} = t\}$. Suppose $|\mathcal{S}| > 3|N|/4$. Observe that, for every $n \in \mathcal{S}$, we have $n^\alpha = t^{-1}n$.

As before, by taking some $n \in \mathcal{S}^{\alpha^{-1}} \cap \mathcal{S}$, we can conclude that $t = t^\alpha$.

As $|\mathcal{S}| > 3|N|/4$, we can argue as before that $|\mathcal{S}^{-1}t \cap \mathcal{S}| > |N|/2$. Let $n \in \mathcal{S}^{-1}t \cap \mathcal{S}$. Then $n = mt$, for some $m \in \mathcal{S}^{-1}$; that is, $m^{-1} \in \mathcal{S}$. Notice that this means $(m^{-1})^\alpha = t^{-1}m^{-1}$, so $m^\alpha = mt$. Therefore

$$t^{-1}(mt) = t^{-1}n = n^\alpha = (mt)^\alpha = m^\alpha t^\alpha = (mt)t.$$

From this we obtain $mt = t^{-1}m$, that is, $t^m = t^{-1}$. As $n = mt$, we also have $t^n = t^{-1}$. We have shown that, for every $n \in \mathcal{S}^{-1}t \cap \mathcal{S}$, we have $t^n = t^{-1}$. As before, this implies that $|N|/2 < |\mathcal{S}^{-1}t \cap \mathcal{S}| \leq |\mathbf{C}_N(t)|$. Thus $N = \mathbf{C}_N(t)$ and $t \in \mathbf{Z}(N)$. As before, this implies that $t^2 = 1$. Summing up, t is a central element of N of order at most 2.

Suppose that $t = 1$. Then $\mathcal{S} = \{n \in N \mid n^\alpha = n\}$. In particular, α is an automorphism fixing more than half of the elements of N. Since the set of fixed points of an automorphism is a subgroup of N, we deduce that $\alpha = 1$; that is, $n^\alpha = n \ \forall n \in N$.

Suppose that $t \neq 1$. Since $t \in \mathbf{Z}(N)$ and since $t^\alpha = t$, we may consider the group $\bar{N} := N/\langle t \rangle$ and the induced automorphism $\bar{\alpha} : \bar{N} \to \bar{N}$. In particular, in $\bar{N}$, the set $\mathcal{S}$ projects to the set $\bar{\mathcal{S}} = \{\bar{n} \in \bar{N} \mid \bar{n}^{\bar{\alpha}} = \bar{n}\}$. Since this set has cardinality larger than $|\bar{N}|/2$, again we see that $\bar{n}^{\bar{\alpha}} = \bar{n} \ \forall \bar{n} \in \bar{N}$. It follows that, for every $n \in N$, $n^\alpha \in \langle t \rangle n = \{n, tn\}$.

Set $\mathcal{S}' := \{n \in N \mid n^\alpha = n\}$. In particular, $\{\mathcal{S}, \mathcal{S}'\}$ is a partition of N and $|\mathcal{S}'| = |N \setminus \mathcal{S}| < |N|/4$.

Now, for every $n, m \in \mathcal{S}$, we have $(nm)^\alpha = (tn)(tm) = (nm)t^2 = nm$ since t is central of order 2, and hence $nm \in \mathcal{S}'$. Therefore, $\mathcal{S} \cdot \mathcal{S} \subseteq \mathcal{S}'$, but this is impossible because $|\mathcal{S}'| < |\mathcal{S}|$. Again this contradiction completes our proof. □

Our next few results show that except in some very special cases, if we have a group T with an index-2 subgroup N and a permutation of T that has a very specific sort of action on every element of the nontrivial coset of N in T, then the number of subsets of T that are closed under both inversion and this permutation is vanishingly small relative to the number of Cayley graphs on T.

Lemma 4.2.3. *Let T be a finite group, let N be a subgroup of T having index 2, let $\gamma \in T \setminus N$, let $t \in N$ and let $\alpha_t : T \to T$ be any permutation defined by*

$$n^{\alpha_t} \in N \quad \text{and} \quad (\gamma n)^{\alpha_t} = \gamma t n, \ \forall n \in N.$$

Then one of the following holds:

1. $|\{X \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}| \leq 2^{\mathbf{c}(T) - \frac{|N|}{16}}$,

2. *$T \cong C_4 \times C_2^\ell$ for some $\ell \in \mathbb{N}$, t is the only non-identity square in T and N is an elementary abelian 2-group,*

3. *$o(t) = 2$, $t = \gamma^2$ and $T = \mathrm{Dic}(N, \gamma^2, \gamma)$,*

4. *$t = 1$.*

In parts (2), (3) and (4), if $n^{\alpha_t} \in \{n, n^{-1}\}$ for every $n \in N$, then we have $x^{\alpha_t} \in \{x, x^{-1}\}$ $\forall x \in T$.

Proof. If $t = 1$, then we obtain part (4). Thus, for the rest of the argument, we assume $t \neq 1$.

Observe that α_t fixes N setwise and induces on $T \setminus N$ a permutation which is the product of disjoint cycles each of whose lengths is $o(t)$. For simplicity, we let $\mathcal{S} := \{X \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}$.

If $o(t) \geq 3$, then

$$|\mathcal{S}| \leq 2^{\mathbf{c}(N)+\frac{|T\setminus N|}{3}} = 2^{\mathbf{c}(N)+\frac{|N|}{3}} = 2^{\frac{|N|+|I(N)|}{2}+\frac{|N|}{3}} \leq 2^{\frac{|N|+|I(T)|}{2}+\frac{|N|}{3}} \leq 2^{\mathbf{c}(T)-\frac{|N|}{6}}$$

and hence part (1) follows.

The only remaining possibility is $o(t) = 2$. Consider $H := \langle \alpha_t, \iota \rangle$, where $\iota : T \to T$ is the mapping defined by $x^\iota = x^{-1}$ $\forall x \in T$. Clearly, $S \in \mathcal{S}$ if and only if S is H-invariant. The orbits of H on $T \setminus N$ have even cardinality because $o(\alpha_t) = o(t) = 2$ and α_t has no fixed points on $T \setminus N$. There are only two possibilities for H having an orbit of cardinality 2 on $T \setminus N$:

- this orbit is $\{\gamma n, \gamma t n\}$ where both γn and $\gamma t n$ are involutions (in this case ι fixes both γn and $\gamma t n$),
- this orbit is $\{\gamma n, \gamma t n\}$ and $(\gamma n)^{-1} = \gamma t n$ (in this case $(\gamma n)^{\alpha_t} = (\gamma n)^\iota$).

Let n_0 be an element in N with $o(\gamma n_0) = o(\gamma t n_0) = 2$. As $o(\gamma n_0) = 2$, we have $n_0\gamma = \gamma^{-1} n_0^{-1}$ and hence

$$1 = (\gamma t n_0)^2 = \gamma t n_0 \gamma t n_0 = \gamma t \gamma^{-1} n_0^{-1} t n_0.$$

Therefore $t(\gamma^{-1} n_0^{-1}) t = \gamma^{-1} n_0^{-1}$. Since $o(t) = 2$, we deduce $(n_0\gamma)^t = n_0\gamma$, that is, $n_0\gamma \in \mathbf{C}_T(t)$. As $\gamma n_0 = (n_0\gamma)^{\gamma^{-1}} \in \mathbf{C}_T(t)^{\gamma^{-1}} = \mathbf{C}_T(t^{\gamma^{-1}})$, the elements of the first type are in the set

$$\mathcal{A} := I([T \setminus N] \cap \mathbf{C}_T(t^{\gamma^{-1}})) = I(\mathbf{C}_{T\setminus N}(t^{\gamma^{-1}})).$$

Let n_1 be an element in N with $(\gamma n_1)^{-1} = \gamma t n_1$. Let $n \in N$ and suppose that $\gamma n_1 n \in T \setminus N$ also satisfies $(\gamma n_1 n)^{-1} = \gamma t n_1 n$. This means $n^{-1}\gamma t n_1 = \gamma t n_1 n$, that is, $n^{(\gamma t n_1)^{-1}} = n^{-1}$. Therefore, the elements of the second type are in the set

$$\mathcal{B} := \gamma n_1 \{n \in N \mid n^{\gamma t n_1} = n^{-1}\}.$$

Observe that $\mathcal{A}$ or $\mathcal{B}$ might be the empty set: $\mathcal{A} = \varnothing$ when there is no involution in $\mathbf{C}_{T\setminus N}(t^{\gamma^{-1}})$, $\mathcal{B} = \varnothing$ when there is no element $n_1 \in N$ with $(\gamma n_1)^{-1} = \gamma t n_1$. Observe also that $\mathcal{A} \cap \mathcal{B} = \varnothing$: indeed, if $\gamma n \in \mathcal{A} \cap \mathcal{B}$, then $(\gamma n)^2 = 1$ and $(\gamma n)^{-1} = \gamma t n$, that is $t = 1$, which is a contradiction.

Since $X \in \mathcal{S}$ if and only X is a union of orbits of H, we get

$$\begin{aligned} |\mathcal{S}| &\leq 2^{\mathbf{c}(N)+\frac{|\mathcal{A}\cup\mathcal{B}|}{2}+\frac{|T\setminus N|-|\mathcal{A}\cup\mathcal{B}|}{4}} = 2^{\mathbf{c}(N)+\frac{|\mathcal{A}\cup\mathcal{B}|}{4}+\frac{|T\setminus N|}{4}} = 2^{\frac{|N|+|I(N)|}{2}+\frac{|\mathcal{A}\cup\mathcal{B}|}{4}+\frac{|N|}{4}} \\ &= 2^{\frac{|T|+|I(N)|}{2}+\frac{|\mathcal{A}\cup\mathcal{B}|}{4}-\frac{|N|}{4}} = 2^{\frac{|T|+|I(N)|}{2}+\frac{|\mathcal{A}|}{4}+\frac{|\mathcal{B}|}{4}-\frac{|N|}{4}} = 2^{\frac{|T|+|I(N)\cup\mathcal{A}|}{2}-\frac{|\mathcal{A}|}{4}+\frac{|\mathcal{B}|}{4}-\frac{|N|}{4}} \leq 2^{\mathbf{c}(T)-\frac{|\mathcal{A}|}{4}+\frac{|\mathcal{B}|}{4}-\frac{|N|}{4}}. \end{aligned}$$

If $|\mathcal{B}| \leq 3|N|/4$, then

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T)+\frac{3|N|}{16}-\frac{|N|}{4}} = 2^{\mathbf{c}(T)-\frac{|N|}{16}}$$

and part (1) follows. Suppose now that $|\mathcal{B}| > 3|N|/4$, that is, $|\{n \in N \mid n^{\gamma t n_1} = n^{-1}\}| > 3|N|/4$. This means that the action of $\gamma t n_1$ by conjugation on N inverts more than 3/4 of the elements of N. From [88], N is abelian and the action of $\gamma t n_1$ by conjugation on N inverts each element of N. Therefore $\mathcal{B} \supset \gamma N$ and hence $\gamma \in \mathcal{B}$. Therefore $\gamma^{-1} = \gamma t$, that is, $t = \gamma^2$ (since $o(t) = 2$). When N is an elementary abelian 2-group, we deduce $T \cong C_4 \times C_2^\ell$ for some $\ell \in \mathbb{N}$ and hence part (2) holds. When N has exponent greater than 2, we deduce $T = \mathrm{Dic}(N, \gamma^2, \gamma)$ and hence part (3) holds. □

The hypotheses of the next lemma look much like the previous one, with the additional assumption that N is abelian (of exponent greater than 2), and a different action on the nontrivial coset of N. The exceptional cases and the proof are quite different, though.

Lemma 4.2.4. *Let T be a finite group, let N be an abelian subgroup of T having index 2 and exponent greater than 2, let $t \in N$, let $\gamma \in T \setminus N$, let $\alpha_t : T \to T$ be any permutation defined by*

$$n^{\alpha_t} \in N \quad \text{and} \quad (\gamma n)^{\alpha_t} = \gamma t n^{-1}, \forall n \in N.$$

Further suppose that either $o(\gamma) = 2$, or $(\gamma n)^{\alpha_t} = \gamma n$ whenever $o(\gamma n) = 2$. Then one of the following holds:

1. $|\{X \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}| \leq 2^{\mathbf{c}(T) - \frac{|N|}{24}}$;
2. *T is abelian and $t = \gamma^{-2}$;*
3. *$T \cong Q_8 \times C_2^\ell$ and $N \cong C_4 \times C_2^\ell$ for some $\ell \in \mathbb{N}$;*
4. *$t = \gamma^2$, $T \cong \langle x, y \mid x^4 = y^4 = (xy)^4, x^2 = y^2 \rangle \times C_2^\ell$ and $N \cong C_4 \times C_2^{\ell+1}$ for some $\ell \in \mathbb{N}$. (The group with presentation $\langle x, y \mid x^4 = y^4 = (xy)^4, x^2 = y^2 \rangle$ has order 16.)*

In parts (2), (3) and (4), if $n^{\alpha_t} \in \{n, n^{-1}\}$ for every $n \in N$, then we have $x^{\alpha_t} \in \{x, x^{-1}\}$ $\forall x \in T$.

Proof. We let $\iota : T \to T$ the permutation defined by $x^\iota = x^{-1}$ $\forall x \in T$. Since N is abelian, for every $n \in N$, we have

$$(\gamma n)^{\alpha_t^2} = ((\gamma n)^{\alpha_t})^{\alpha_t} = (\gamma t n^{-1})^{\alpha_t} = \gamma t (t n^{-1})^{-1} = \gamma t n t^{-1} = \gamma n.$$

Thus α_t is a permutation having order 2. Clearly, ι has also order 2. For simplicity, we let $\mathcal{S} := \{X \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}$. In particular, $X \in \mathcal{S}$ if and only if X is $\langle \alpha_t, \iota \rangle$-invariant, that is, X is a union of $\langle \alpha_t, \iota \rangle$-orbits.

Observe that $n^{-1}\gamma^{-1} = \gamma \cdot (\gamma^{-1} n^{-1} \gamma^{-1})$ and $\gamma^{-1} n^{-1} \gamma^{-1} \in N$ because $|T : N| = 2$. Therefore

$$(n^{-1}\gamma^{-1})^{\alpha_t} = (\gamma \cdot \gamma^{-1} n^{-1} \gamma^{-1})^{\alpha_t} = \gamma t \gamma n \gamma. \tag{4.2.1}$$

We divide the proof in two cases.

Case $(\gamma n)^{\alpha_t} = \gamma n$ whenever $o(\gamma n) = 2$.

Note that

$$c(T) = \frac{|T|}{2} + \frac{|I(T)|}{2} = \frac{|T|}{2} + \frac{|I(N)|}{2} + \frac{|I(T \setminus N)|}{2} = c(N) + \frac{|N|}{2} + \frac{|I(T \setminus N)|}{2}.$$

So $c(N) = c(T) - |N|/2 - |I(T \setminus N)|/2$.

Given $n \in N$, the $\langle \iota \rangle$-orbit containing γn is $\{\gamma n, n^{-1}\gamma^{-1}\}$. Now there are only two possibilities for α_t not fusing this $\langle \iota \rangle$-orbit with another $\langle \iota \rangle$-orbit. The first possibility is

when α_t fixes both γn and $n^{-1}\gamma^{-1}$; the second possibility is when $(\gamma n)^{\alpha_t} = (\gamma n)^\iota$, that is, $\gamma t n^{-1} = n^{-1}\gamma^{-1}$. Let

$$\mathcal{A} := \{n \in N \mid (\gamma n)^{\alpha_t} = \gamma n, (n^{-1}\gamma^{-1})^{\alpha_t} = n^{-1}\gamma^{-1}\},$$
$$\mathcal{B} := \{n \in N \mid \gamma t n^{-1} = n^{-1}\gamma^{-1}\}.$$

Given $n \in \mathcal{A}$, we have $\gamma t n^{-1} = (\gamma n)^{\alpha_t} = \gamma n$ and, from (4.2.1), $\gamma t \gamma n \gamma = (n^{-1}\gamma^{-1})^{\alpha_t} = n^{-1}\gamma^{-1}$. The first equality yields $n^2 = t$. The second equality yields

$$t = \gamma^{-1}n^{-1}\gamma^{-2}n^{-1}\gamma^{-1} = \gamma^{-1}n^{-2}\gamma^{-3} = \gamma^{-1}t^{-1}\gamma^{-3},$$

where in the second equality we have used that $\gamma^2 \in N$ and that N is abelian. Therefore, if $n \in \mathcal{A}$, then $n^2 = t$ and $t = \gamma^{-1}t^{-1}\gamma^{-3}$. Observe that the second condition does not depend on n any longer. This means that we have two possibilities for $\mathcal{A}$; either $\mathcal{A} = \varnothing$, or $\mathcal{A} = n_0\Omega_2(N)$ where $\Omega_2(N) := \{n \in N \mid o(n) \leq 2\}$ and where $n_0 \in N$ satisfies $n_0^2 = t$. Summing up

$$\mathcal{A} = \begin{cases} \varnothing & \text{if there is no } n \in N \text{ with } n^2 = t, \text{or if } t \neq \gamma^{-1}t^{-1}\gamma^{-3}, \\ n_0\Omega_2(N) & \text{where } n_0 \in N \text{ satisfies } n_0^2 = t \text{ and } t = \gamma^{-1}t^{-1}\gamma^{-3}. \end{cases}$$

Given $n \in \mathcal{B}$, we have $t = \gamma^{-1}n^{-1}\gamma^{-1}n = \gamma^{-1}n^{-1}\gamma n\gamma^{-2} = [\gamma, n]\gamma^{-2}$ (using $\gamma^2 \in N$ in the second equality). This means that we have two possibilities for $\mathcal{B}$; either $\mathcal{B} = \varnothing$, or $\mathcal{B} = n_1\mathbf{C}_N(\gamma)$ where $n_1 \in N$ satisfies $t = [\gamma, n_1]\gamma^{-2}$. Summing up

$$\mathcal{B} = \begin{cases} \varnothing & \text{if there is no } n \in N \text{ with } t = [\gamma, n]\gamma^{-2}, \\ n_1\mathbf{C}_N(\gamma) & \text{where } n_1 \in N \text{ satisfies } t = [\gamma, n_1]\gamma^{-2}. \end{cases}$$

We claim that $\mathcal{A} \cap \mathcal{B} = \{n \in N : o(\gamma n) = 2\}$. Certainly if $o(\gamma n) = 2$ then by the case we are in, $(\gamma n)^{\alpha_t} = \gamma n = (\gamma n)^{-1}$ and therefore $n \in \mathcal{A} \cap \mathcal{B}$. Conversely, if $n \in \mathcal{A} \cap \mathcal{B}$ then $(\gamma n)^{\alpha_t} = \gamma n$ and $(\gamma n)^{\alpha_t} = (\gamma n)^{-1}$, so $o(\gamma n) = 2$. Therefore $|\mathcal{A} \cap \mathcal{B}| = |I(T \setminus N)|$.

Using the sets $\mathcal{A}$ and $\mathcal{B}$ we are ready to estimate $|\mathcal{S}|$. Indeed, we have

$$\begin{aligned} |\mathcal{S}| &\leq 2^{\mathbf{c}(N) + \frac{|\gamma N \setminus (\gamma\mathcal{A} \cup \gamma\mathcal{B})|}{4} + \frac{|\gamma\mathcal{A} \setminus \gamma(\mathcal{A}\cap\mathcal{B})|}{2} + \frac{|\gamma\mathcal{B} \setminus \gamma(\mathcal{A}\cap\mathcal{B})|}{2} + |\gamma(\mathcal{A}\cap\mathcal{B})|} \\ &= 2^{\mathbf{c}(N) + \frac{|\gamma N|}{4} + \frac{|\mathcal{A}|}{4} + \frac{|\mathcal{B}|}{4}} = 2^{\mathbf{c}(T) - \frac{|N|}{2} + \frac{|\gamma N|}{4} + \frac{|\mathcal{A}|}{4} + \frac{|\mathcal{B}|}{4} - \frac{|I(T\setminus N)|}{2}} = 2^{\mathbf{c}(T) - \frac{|N|}{4} + \frac{|\mathcal{A}|}{4} + \frac{|\mathcal{B}|}{4} - \frac{|\mathcal{A}\cap\mathcal{B}|}{2}}. \end{aligned} \tag{4.2.2}$$

If $\mathcal{A} = \mathcal{B} = \varnothing$, then part (1) follows immediately. Suppose then $\mathcal{A}$ and $\mathcal{B}$ are not both empty. If $\mathcal{A} = \varnothing$, then part (1) follows as long as $N \neq \mathbf{C}_N(\gamma)$. If $N = \mathbf{C}_N(\gamma)$, then $[\gamma, n_1] = 1$ and hence $t = \gamma^{-2}$. Thus, we obtain part (2). If $\mathcal{B} = \varnothing$, then part (1) follows as long as $N \neq \Omega_2(N)$. However, since we are assuming that N has exponent greater than 2, we cannot have $N = \Omega_2(N)$. Thus we have finished discussing the case $\mathcal{A} = \varnothing$ or $\mathcal{B} = \varnothing$. We now assume $\mathcal{A} \neq \varnothing \neq \mathcal{B}$. In particular, $|N : \mathbf{C}_N(\gamma)| \geq 2$ and $|N : \Omega_2(N)| \geq 2$. If $|N : \mathbf{C}_N(\gamma)| \geq 3$ or if $|N : \Omega_2(N)| \geq 3$, then from (4.2.2) we have

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T) - \frac{|N|}{4} + \frac{|\mathcal{A}|}{4} + \frac{|\mathcal{B}|}{4}} \leq 2^{\mathbf{c}(T) - \frac{|N|}{4} + \frac{|N|}{12} + \frac{|N|}{8}} = 2^{\mathbf{c}(T) - \frac{|N|}{24}}$$

and part (1) follows.

It remains to deal with the case that $|N : \Omega_2(N)| = 2 = |N : \mathbf{C}_N(\gamma)|$, so $\mathcal{A}$ and $\mathcal{B}$ are both cosets of an index 2 subgroup of N. If $\mathcal{A} \cap \mathcal{B} \neq \varnothing$ then since both are cosets of index-2 subgroups of N, it is straightforward to see that their intersection has cardinality at least $|N|/4$, and part (1) follows. If $\mathcal{A} \cap \mathcal{B} = \varnothing$, we obtain that $\mathcal{A}$ and $\mathcal{B}$ are both cosets of the same index 2 subgroup of N. Therefore, $\mathbf{C}_N(\gamma) = \Omega_2(N)$ and $N \cong C_4 \times C_2^\ell$ for some $\ell \in \mathbb{N}$. Let us call this index-2 subgroup of N, M. Therefore, we have either $\mathcal{A} = M$ and $\mathcal{B} = N \setminus M$, or $\mathcal{A} = N \setminus M$ and $\mathcal{B} = M$. In the first possibility, we have $n_0^2 = 1$,

$\mathcal{A} = \Omega_2(N)$, $\gamma^4 = 1$ and $\gamma^2 = [\gamma, n_1] = \gamma^{-1}n_1^{-1}\gamma n_1$. From this it follows $\gamma^{-1} = n_1^{-1}\gamma n_1$. Since $n_1^2 = \gamma^2$ is the unique involution that is a square in N, we get part (3). In the second possibility, $\gamma^{-2} = t = n_0^2$. If we also have $(\gamma n_0)^2 = t$, then $T = \mathrm{Dic}(N, \gamma^2, \gamma)$ and we obtain again part (3). If $(\gamma n_0)^2 \neq t$, then $\langle \gamma, n_0 \rangle$ has order 16 and is isomorphic to the group with presentation $\langle x, y \mid x^4 = y^4 = (xy)^4 = 1, x^2 = y^2 \rangle$ and we obtain part (4).

Case $o(\gamma) = 2$. For every $n \in N$, from (4.2.1) (and using $o(\gamma) = 2$), we have

$$\begin{aligned}(\gamma n)^{\alpha_t\iota\alpha_t\iota} &= (\gamma t n^{-1})^{\iota\alpha_t\iota} = ((tn^{-1})^{-1}(\gamma)^{-1})^{\alpha_t\iota} = (\gamma t\gamma(tn^{-1})\gamma)^{\iota} = (\gamma t t^{\gamma}(n^{-1})^{\gamma})^{\iota} \\ &= n^{\gamma}(tt^{\gamma})^{-1}\gamma = (tt^{\gamma})^{-1}n^{\gamma}\gamma = (t^{\gamma})^{-1}t^{-1}\gamma n = \gamma(t^{\gamma}t)^{-1}n = \gamma(tt^{\gamma})^{-1}n.\end{aligned}$$

Moreover, $n^{\alpha_t\iota\alpha_t\iota} \in N\ \forall n \in N$. Define $z := (tt^{\gamma'})^{-1}$ and $\delta : T \to T$ by

$$n^{\delta} = n^{\alpha_t\iota\alpha_t\iota} \text{ and } (\gamma n)^{\delta} = \gamma z n,\ \forall n \in N.$$

In particular, $\delta = \alpha_t\iota\alpha_t\iota$.

Recall that $X \in \mathcal{S}$ if and only if X is $\langle \alpha_t, \iota \rangle$-invariant. Since $\delta \in \langle \alpha_t, \iota \rangle$, we deduce that X is also $\langle \iota, \delta \rangle$-invariant.

Subcase $o(z) \geq 3$.

Since the orbits of δ on $T \setminus N$ have all length $o(z) \geq 3$, we have

$$|\mathcal{S}| \leq 2^{\mathbf{c}(N)+\frac{|N|}{3}} = 2^{\frac{|N|+|I(N)|}{2}+\frac{|N|}{2}-\frac{|N|}{6}} = 2^{\frac{|T|+|I(N)|}{2}-\frac{|N|}{6}} \leq 2^{\mathbf{c}(T)-\frac{|N|}{6}}$$

and part (1) follows.

Subcase $o(z) = 2$.

For every $n \in N$, we have

$$(\gamma n)^{\iota\delta\iota\delta} = (n^{-1}\gamma)^{\delta\iota\delta} = (\gamma(n^{-1})^{\gamma})^{\delta\iota\delta} = (\gamma z(n^{-1})^{\gamma})^{\iota\delta} = (n^{\gamma}z\gamma)^{\delta} = (\gamma n z^{\gamma})^{\delta} = (\gamma z^{\gamma} n)^{\delta} = \gamma z z^{\gamma} n.$$

Define $\delta' : T \to T$ by

$$n^{\delta'} = n^{\delta} \text{ and } (\gamma n)^{\delta'} = \gamma z z^{\gamma} n,\ \forall n \in N.$$

If $X \in \mathcal{S}$, then X is $\langle \delta, \iota \rangle$-invariant and hence X is also $\langle \delta, \delta' \rangle$-invariant. Suppose $z^{\gamma} \neq z$. Since the orbits of $\langle \delta, \delta' \rangle$ on $T \setminus N$ have all length $|\langle z, z^{\gamma'} \rangle| \geq 4$, we have

$$|\mathcal{S}| \leq 2^{\mathbf{c}(N)+\frac{|N|}{4}} = 2^{\frac{|N|+|I(N)|}{2}+\frac{|N|}{2}-\frac{|N|}{4}} = 2^{\frac{|T|+|I(N)|}{2}-\frac{|N|}{4}} \leq 2^{\mathbf{c}(T)-\frac{|N|}{4}}$$

and part (1) follows.

Suppose $o(z) = 2$ and $z^{\gamma} = z$. For every $n \in N$, we have

$$(\gamma n)^{\iota\delta} = (n^{-1}\gamma)^{\delta} = (\gamma(n^{-1})^{\gamma})^{\delta} = \gamma z(n^{-1})^{\gamma} = z\gamma(n^{-1})^{\gamma} = zn^{-1}\gamma = (\gamma z n)^{\iota} = (\gamma n)^{\delta\iota}.$$

This shows that $\iota\delta = \delta\iota$ in its action on $T \setminus N$ and hence $\langle \iota_{|T\setminus N}, \delta_{|T\setminus N} \rangle$ is an elementary abelian 2-group of order 1, 2 or 4. (Here we are denoting by $\iota_{|T\setminus N}$ and by $\delta_{|T\setminus N}$ the restrictions of ι and of δ to $T \setminus N$.) This group cannot have order 1 because $o(z) = 2$ and hence $\delta_{|T\setminus N}$ is not the identity permutation.

If this group has order 2, then $\iota_{|T\setminus N}$ must be either $\delta_{|T\setminus N}$ or the identity permutation. Suppose that $\iota_{|T\setminus N} = \delta_{|T\setminus N}$. Then for every $n \in N$ we have $n^{-1}\gamma = \gamma z n$, so $n^{\gamma} = zn^{-1}$ and hence $nn^{\gamma} = z$. But since $z \neq 1$, Lemma 4.2.1 implies that we cannot have $z = nn^{\gamma}$ for every $n \in N$.

So we must have $\iota_{|T\setminus N}$ being the identity permutation, that is, $n^{-1}\gamma = (\gamma n)^{\iota} = \gamma n$, so $n^{\gamma} = n^{-1}\ \forall n \in N$. In particular, $\mathbf{c}(\gamma N) = |N|$ and $\mathbf{c}(T) = \mathbf{c}(N) + |N|$. Since the orbits of $\langle \delta \rangle$ on $T \setminus N$ have all length $o(z) = 2$, we have $|\mathcal{S}| \leq 2^{\mathbf{c}(N)+|N|/2} = 2^{\mathbf{c}(T)-|N|/2}$ and part (1) follows.

It remains to consider the case that $\langle \iota_{|T\setminus N}, \delta_{|T\setminus N}\rangle$ has order 4. By the orbit counting lemma, the number of orbits of $\langle\iota\rangle$ on $T\setminus N$ is

$$\frac{1}{2}(|T\setminus N| + |\mathrm{Fix}_{T\setminus N}(\iota)|) = \frac{1}{2}(|T\setminus N| + |I(T\setminus N)|) = \mathbf{c}(T\setminus N). \tag{4.2.3}$$

Also, by the orbit counting lemma, the number of orbits of $\langle \iota_{|T\setminus N}, \delta_{|T\setminus N}\rangle$ on $T\setminus N$ is

$$\begin{aligned}
&\frac{1}{4}\Big(|N| + |\mathrm{Fix}_{T\setminus N}(\iota)| + |\mathrm{Fix}_{T\setminus N}(\delta)| + |\mathrm{Fix}_{T\setminus N}(\iota\delta)|\Big)\\
=\ & \mathbf{c}(T\setminus N) - \frac{|N|}{4} - \frac{|\mathrm{Fix}_{T\setminus N}(\iota)|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\delta)|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\iota\delta)|}{4}\\
=\ & \mathbf{c}(T\setminus N) - \frac{|N|}{4} - \frac{|\mathrm{Fix}_{T\setminus N}(\iota)|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\iota\delta)|}{4}\\
\le\ & \mathbf{c}(T\setminus N) - \frac{|N|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\iota\delta)|}{4},
\end{aligned}$$

where in the first equality we have used (4.2.3) and in the second equality we have used the fact that δ has no fixed points on $T\setminus N$. Now, $\gamma n \in \mathrm{Fix}_{T\setminus N}(\iota\delta)$ if and only if $\gamma n = (\gamma n)^{\iota\delta} = \gamma z (n^{-1})^{\gamma}$, that is, $z = nn^{\gamma}$. From Lemma 4.2.1, we deduce $|\mathrm{Fix}_{T\setminus N}(\iota\delta)| \le 3|N|/4$ because $z \neq 1$. Thus

$$|\mathcal{S}| \le 2^{\mathbf{c}(N)+\mathbf{c}(T\setminus N)-\frac{|N|}{4}+\frac{3|N|}{16}} = 2^{\mathbf{c}(T)-\frac{|N|}{16}}$$

and part (1) follows.

Subcase $o(z) = 1$.

In this case, $tt^{\gamma} = z = 1$ and $t^{\gamma} = t^{-1}$. In this case, for every $n \in N$, we have

$$(\gamma n)^{\iota\alpha_t} = (\gamma(n^{-1})^{\gamma})^{\alpha_t} = \gamma t n^{\gamma} = t^{-1}\gamma n^{\gamma} = t^{-1}n\gamma = (\gamma t n^{-1})^{\iota} = (\gamma n)^{\alpha_t\iota}.$$

This shows that $\iota\alpha_t = \alpha_t\iota$ on $T\setminus N$, and hence (in particular) $\langle \iota_{|T\setminus N}, (\alpha_t)_{|T\setminus N}\rangle$ is an elementary abelian 2-group of order 1, 2 or 4. If $(\alpha_t)_{|T\setminus N}$ is the identity mapping, then $\gamma n = (\gamma n)^{\alpha_t} = \gamma t n^{-1}$, for every $n \in N$. In particular, $\gamma t = \gamma t t^{-1}$ which implies $t = 1$. This means that for every $n \in N$, $\gamma n = (\gamma n)^{\alpha_t} = \gamma n^{-1}$, so that N is an elementary abelian 2-group, contradicting our hypothesis that N has exponent greater than 2.

If $\iota_{T\setminus N}$ is the identity mapping, then $\mathbf{c}(\gamma N) = |N|$ and hence $\mathbf{c}(T) = \mathbf{c}(N) + |N|$. Observe that

$$\mathrm{Fix}_{T\setminus N}(\alpha_t) := \{\gamma n \mid t = n^2\}.$$

Let $n_0^2 = t$, an easy computation shows that

$$\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma n_0 \Omega_2(N),$$

hence $|\mathrm{Fix}_{T\setminus N}(\alpha_t)| = |\Omega_2(N)| \le |N|/2$. This shows that $\langle (\alpha_t)_{|T\setminus N}\rangle$ has at most $|N|/2 + (|N|/2)/2 = 3|N|/4$ orbits on $T\setminus N$. Therefore

$$|\mathcal{S}| \le 2^{\mathbf{c}(N)+\frac{3|N|}{4}} = 2^{\mathbf{c}(T)-|N|+\frac{3|N|}{4}} = 2^{\mathbf{c}(T)-\frac{|N|}{4}}$$

and part (1) follows. So we can assume that $\iota_{T\setminus N}$ is not the identity.

Since $\gamma^2 = 1$, when $\iota_{|T\setminus N} = (\alpha_t)_{|T\setminus N}$, then $t^{-1}\gamma = (\gamma t)^{\iota_{T\setminus N}} = (\gamma t)^{\alpha_t} = \gamma$, so $t = 1$. Further, $n^{-1}\gamma = (\gamma n)^{\iota_{T\setminus N}} = (\gamma n)^{\alpha_t} = \gamma n^{-1}$, for every $n \in N$, that is T is abelian, and part (2) holds.

It only remains to consider the case that $\langle \iota_{|T\setminus N}, (\alpha_t)_{|T\setminus N}\rangle$ has order 4.

By the orbit counting lemma, the number of orbits of $\langle \iota, \alpha_t\rangle$ on $T\setminus N$ is

$$\begin{aligned}
&\frac{1}{4}\Big(|N| + |\mathrm{Fix}_{T\setminus N}(\iota)| + |\mathrm{Fix}_{T\setminus N}(\alpha_t)| + |\mathrm{Fix}_{T\setminus N}(\iota\alpha_t)|\Big) \qquad (4.2.4)\\
&= \mathbf{c}(T\setminus N) - \frac{|N|}{4} - \frac{|\mathrm{Fix}_{T\setminus N}(\iota)|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\alpha_t)|}{4} + \frac{|\mathrm{Fix}_{T\setminus N}(\iota\alpha_t)|}{4},
\end{aligned}$$

where the equality between the two members follows by (4.2.3). If $|\mathrm{Fix}_{T\setminus N}(\alpha_t)| \leq |N|/3$ and $|\mathrm{Fix}_{T\setminus N}(\iota\alpha_t)| \leq |N|/2$, or $|\mathrm{Fix}_{T\setminus N}(\alpha_t)| \leq |N|/2$ and $|\mathrm{Fix}_{T\setminus N}(\iota\alpha_t)| \leq |N|/3$, then we immediately obtain part (1). Therefore we suppose that this does not hold. An easy computation reveals that

$$\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) := \{\gamma n \mid t^{-1} = [n, \gamma]\}.$$

As $(\alpha_t)_{|T\setminus N}$ and $(\iota\alpha_t)_{|T\setminus N}$ are not the identity mappings, we deduce

- $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma n_0 \Omega_2(N)$, $n_0^2 = t$ and $|N : \Omega_2(N)| = 2$,
- $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma n_1 \mathbf{C}_N(\gamma)$, $t^{-1} = [n_1, \gamma]$ and $|N : \mathbf{C}_N(\gamma)| = 2$,
- $|\mathrm{Fix}_{T\setminus N}(\alpha_t)| = |N|/2 = |\mathrm{Fix}_{T\setminus N}(\iota\alpha_t)|$.

If $\Omega_2(N) \neq \mathbf{C}_N(\gamma)$ or if $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \mathrm{Fix}_{T\setminus N}(\iota\alpha_t)$, we have $|\mathrm{Fix}_{T\setminus N}(\iota)| \geq |N|/4$, because $\mathrm{Fix}_{T\setminus N}(\iota)$ contains both $\gamma(\Omega_2(N) \cap \mathbf{C}_N(\gamma))$ and $\mathrm{Fix}_{T\setminus N}(\alpha_t) \cap \mathrm{Fix}_{T\setminus N}(\iota\alpha_t)$. Hence, from (4.2.4), the number of orbits of $\langle \iota, \alpha_t \rangle$ on $T \setminus N$ is at most

$$\mathbf{c}(T \setminus N) - \frac{|N|}{4} - \frac{|N|}{16} + \frac{|N|}{8} + \frac{|N|}{8} = \mathbf{c}(\gamma N) - \frac{|N|}{16}$$

and part (1) follows again. Assume, at last, $\Omega_2(N) = \mathbf{C}_N(\gamma)$ and $\mathrm{Fix}_{T\setminus N}(\alpha_t) \neq \mathrm{Fix}_{T\setminus N}(\iota\alpha_t)$. Set $M := \Omega_2(N) = \mathbf{C}_N(\gamma)$. Then $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma M$ and $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma(N \setminus M)$, or $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma(N \setminus M)$ and $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma M$. If $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma M$, then $t = 1$ and $1 = t^{-1} = [\gamma, n_1]$. Thus $n_1 \in \mathbf{C}_N(\gamma) = M$ and hence $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma M$, contradicting $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma(N \setminus M)$. Thus $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma(N \setminus M)$ and $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma M$. As $\mathrm{Fix}_{T\setminus N}(\iota\alpha_t) = \gamma M = \gamma \mathbf{C}_N(\gamma)$, we have $n_1 \in \mathbf{C}_N(\gamma)$ and hence $t^{-1} = [\gamma, n_1] = 1$. Then $n_0^2 = t = 1$ and hence $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma\Omega_2(N) = \gamma M$, contradicting $\mathrm{Fix}_{T\setminus N}(\alpha_t) = \gamma(N \setminus M)$. □

The next lemma again has a similar flavour. This time we are assuming that the index-2 subgroup N of T is generalised dicyclic, and we need to assume that our permutation fixes each of the cosets of the abelian subgroup A of N setwise.

Lemma 4.2.5. *Let T be a finite group, let $N = \mathrm{Dic}(A, y, x)$ be a generalised dicyclic subgroup of T having index 2, let $t \in N$, let $\gamma \in T \setminus N$, let $\alpha_t : T \to T$ be any permutation defined by*

$$a^{\alpha_t} \in A, (xa)^{\alpha_t} \in xA, \forall a \in A, \quad \text{and} \quad (\gamma n)^{\alpha_t} = \gamma t n^{\bar{\iota}_A}, \forall n \in N.$$

Recall that $\bar{\iota}_A$ is given in Definition 4.0.8. Then one of the following holds:

1. $|\{S \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}| \leq 2^{\mathbf{c}(\gamma N) - \frac{|N|}{24}}$,
2. $\gamma^2 = y = t$ *and* $a^\gamma = a^{-1}$ $\forall a \in A$,
3. $t = 1$, $\langle \gamma, A \rangle$ *is abelian, and* $T = \mathrm{Dic}(\langle \gamma, A \rangle, y, x)$.

In parts (2) and (3), if $n^{\alpha_t} \in \{n, n^{-1}\}$ for every $n \in N$, then we have $z^{\alpha_t} \in \{z, z^{-1}\}$ $\forall x \in T$.

Proof. We let $\iota : T \to T$ the permutation defined by $z^\iota = z^{-1}$ $\forall z \in T$. For simplicity, we let $\mathcal{S} := \{X \subseteq T \mid X = X^{-1}, X^{\alpha_t} = X\}$. Observe that, for every $a \in A$, we have $a^{\alpha_t} \in A$ and

$$(\gamma a)^{\alpha_t} = \gamma t a^{\bar{\iota}_A} = \gamma t a. \tag{4.2.5}$$

Suppose $o(t) \geq 3$. Then the orbits of $\langle \alpha_t \rangle$ on γA all have length $o(t) \geq 3$ and hence

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T\setminus(\gamma A \cup \gamma^{-1}A)) + \frac{|\gamma A|}{3}} \leq 2^{\mathbf{c}(T) - \frac{|A|}{2} + \frac{|A|}{3}} = 2^{\mathbf{c}(T) - \frac{|A|}{6}} = 2^{\mathbf{c}(T) - \frac{|N|}{12}}$$

and part (1) follows in this case. In particular, for the rest of the proof we may suppose that $o(t) \leq 2$. Since N is generalised dicyclic and $t \in N$, we obtain $t \in A$. Now, for every $a \in A$, we have $(\gamma a)^{\alpha_t} = \gamma t a \in \gamma A$ and hence γA is α_t-invariant. Therefore α_t has $|A|/o(t)$ cycles on γA. This also means that $\gamma x A$ is α_t-invariant.

Suppose that $\gamma^2 \notin A$, that is, $\gamma A \neq \gamma^{-1} A$. Then T/A is a cyclic group and $N = \langle \gamma^2, A \rangle$. If $o(t) \neq 1$, then

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T \setminus (\gamma A \cup \gamma^{-1} A)) + \frac{|A|}{2}} = 2^{\mathbf{c}(T) - |A| + \frac{|A|}{2}} = 2^{\mathbf{c}(T) - \frac{|A|}{2}} = 2^{\mathbf{c}(T) - \frac{|N|}{4}}$$

and part (1) follows in this case. Suppose then $t = 1$. In this case α_t fixes γA pointwise. For every $a \in A$, we have

$$(\gamma^{-1} a)^{\alpha_t} = (\gamma(\gamma^{-2} a))^{\alpha_t} = \gamma(\gamma^{-2} a)^{\bar{\iota}_A} = \gamma \gamma^2 a = \gamma^3 a. \tag{4.2.6}$$

As $\langle \gamma^2, A \rangle = N = \mathrm{Dic}(A, y, x)$ and as all elements in $N \setminus A$ have order 4, we deduce $o(\gamma^2) = 4$ and $o(\gamma) = 8$. In particular, $\gamma^3 \neq \gamma^{-1}$ and from (4.2.6) we deduce that α_t has no fixed points on $\gamma^{-1} A$. Hence α_t has at most $|A|/2$ cycles on $\gamma^{-1} A$. Therefore

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T \setminus (\gamma A \cup \gamma^{-1} A)) + \frac{|A|}{2}} = 2^{\mathbf{c}(T) - |A| + \frac{|A|}{2}} = 2^{\mathbf{c}(T) - \frac{|A|}{2}} = 2^{\mathbf{c}(T) - \frac{|N|}{4}}$$

and part (1) follows in this case.

Henceforth we may assume that $\gamma^2 \in A$. Then $\langle \gamma, A \rangle$ is a group having a subgroup A of index 2. Furthermore, since both $N = \langle x, A \rangle$ and $\langle \gamma, A \rangle$ are index-2 subgroups of T, we must have $(\gamma x)^2 \in N \cap \langle \gamma, A \rangle = A$. Also, since γ and x both normalise A, so does γx. So $\langle \gamma x, A \rangle$ is a group having a subgroup of index 2 and α_t restricts to a permutation of $\langle \gamma x, A \rangle$. Since $t \in A$ and $o(t) \leq 2$ we see that x and t commute, so for every $a \in A$ we have

$$(\gamma x a)^{\alpha_t} = \gamma t (x a)^{\bar{\iota}_A} = \gamma t x^{-1} a = \gamma x^{-1} t a = \gamma x (x^2 t) a. \tag{4.2.7}$$

So we can apply Lemma 4.2.3 to the group $\langle \gamma x, A \rangle$ and the permutation $(\alpha_t)_{|\langle \gamma x, A \rangle}$ with γx taking the role of the "γ" in that lemma, and $x^2 t$ taking the role of "t."

If part (1) in Lemma 4.2.3 holds, then

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T \setminus \langle \gamma x, A \rangle) + \mathbf{c}(\langle \gamma x, A \rangle) - \frac{|A|}{16}} = 2^{\mathbf{c}(T) - \frac{|N|}{32}}$$

and conclusion (1) holds.

If part (2) in Lemma 4.2.3 holds, then A is an elementary abelian 2-group, but this contradicts our definition of a generalised dicyclic group together with our hypothesis that N is such a group.

So either part (3) in Lemma 4.2.3 holds, so that $o(x^2 t) = 2$, $x^2 t = (\gamma x)^2$, and $\langle \gamma x, A \rangle = \mathrm{Dic}(A, (\gamma x)^2, \gamma x)$; or part (4) holds, so that $x^2 t = 1$, meaning $x^2 = t$. We postpone further consideration of these cases briefly.

We can also apply Lemma 4.2.3 to the group $\langle \gamma, A \rangle$ and the permutation α_t. In this case γ takes the role of "γ" in the lemma, and t takes the role of "t".

If part (1) in Lemma 4.2.3 holds, then

$$|\mathcal{S}| \leq 2^{\mathbf{c}(T \setminus \langle \gamma, A \rangle) + \mathbf{c}(\langle \gamma, A \rangle) - \frac{|A|}{16}} = 2^{\mathbf{c}(T) - \frac{|N|}{32}}$$

and conclusion (1) holds.

If part (2) in Lemma 4.2.3 holds, then A is an elementary abelian 2-group, again a contradiction.

So either part (3) in Lemma 4.2.3 holds, so that $o(t) = 2$, $t = \gamma^2$, and $\langle \gamma, A \rangle = \mathrm{Dic}(A, t, \gamma)$; or part (4) of Lemma 4.2.3 holds, so that $t = 1$.

We have now applied Lemma 4.2.3 to two different subgroups of T, and have completed the proof except in the cases where parts (3) or (4) arise from both applications. We now consider these final four possible outcomes individually.

It is not possible that part (4) holds in both applications, since this would imply that $t = 1$ and $x^2 = t$, contradicting $o(x) = 4$ from the definition of a generalised dicyclic group.

If part (3) holds in both applications, then $\langle \gamma x, A\rangle = \mathrm{Dic}(A, (\gamma x)^2, \gamma x)$ implies that $a^{\gamma x} = a^x = a^{-1}$, so $a^\gamma = a$ for every $a \in A$. But $\langle \gamma, A\rangle = \mathrm{Dic}(A, t, \gamma)$ implies that $a^\gamma = a^{-1}$ for every $a \in A$. Taken together, these imply that A is an elementary abelian 2-group, again a contradiction.

If part (3) holds in the first application and part (4) holds in the second, then we have $t = 1$, $(o(x^2t) = 2)$, $x^2t = (\gamma x)^2$, and $\langle \gamma x, A\rangle = \mathrm{Dic}(A, (\gamma x)^2, \gamma x)$. Since $\langle \gamma x, A\rangle = \mathrm{Dic}(A, (\gamma x)^2, \gamma x)$, we see that $a^{\gamma x} = a^x = a^{-1}$, so $a^\gamma = a$ for every $a \in A$, and $\langle \gamma, A\rangle$ is abelian. Since $x^2t = x^2 = (\gamma x)^2$, we have $\gamma^x = \gamma^{-1}$, so $T = \mathrm{Dic}(\langle \gamma, A\rangle, y, x)$. This is conclusion (3).

Finally, if part (4) holds in the first application and part (3) holds in the second, then we have $y = x^2 = t$, $o(t) = 2$, $t = \gamma^2$, and $\langle \gamma, A\rangle = \mathrm{Dic}(A, t, \gamma)$. This is conclusion (2).

□

With these preliminary results in hand, we are ready to prove bounds on the number of connection sets that admit various types of graph automorphisms. Recall Notation 2. We already have bounds on $|\mathcal{S}_N^1|$ and on $|\mathcal{U}_N|$. Our goal in this section is to bound $|\mathcal{T}_N|$ when $|N|$ is relatively large. In order to do this, we need to further subdivide $\mathcal{T}_N$.

Notation 3. For what follows, R is a group that is neither generalised dicyclic, nor abelian of exponent greater than 2. We let N be normal subgroup of R and we let

$$\mathcal{T}_N^1 := \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \mid \exists x \in R \text{ and } \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ and } (xN)^f \notin \{xN, x^{-1}N\}\},$$

$$\mathcal{T}_N^2 := \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \setminus \mathcal{T}_N^1 \mid \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \setminus \mathbf{C}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ and } N \text{ is neither abelian of exponent greater than 2 nor generalised dicyclic, or } N \text{ is abelian of exponent greater than 2 and } n^f \neq n^{-1} \text{ for some } n \in N, \text{ or } N = \mathrm{Dic}(A, y, x) \ncong Q_8 \times C_2^\ell \text{ and } n^f \neq n^{\bar{\iota}_A} \text{ for some } n \in N, \text{ or } N \cong Q_8 \times C_2^\ell \text{ and } n^f \notin \{n^{\bar{\iota}_i}, n^{\bar{\iota}_j}, n^{\bar{\iota}_k}\} \text{ for some } n \in N\},$$

$$\mathcal{T}_N^3 := \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \setminus \bigcup_{\ell=1}^{2} \mathcal{T}_N^\ell \mid \exists x \in R \text{ and } \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1, (xN)^f \neq xN \text{ and either } N \text{ is non-abelian or there exists } n \in N \text{ with } (xn)^f \neq (xn)^{-1}\},$$

$$\mathcal{T}_N^4 := \{S \in \mathcal{S}_N \setminus \mathcal{S}_N^1 \setminus \bigcup_{\ell=1}^{3} \mathcal{T}_N^\ell \mid \exists x \in R \text{ and } \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } 1^f = 1 \text{ and } x^f \notin \{x, x^{-1}\}\}.$$

It should be clear from this definition that

$$\mathcal{T}_N = \bigcup_{\ell=1}^{4} \mathcal{T}_N^\ell.$$

We will bound the cardinality of each of these sets. Most of the bounds we find will only be vanishingly small relative to $2^{\mathbf{c}(R)}$ if $|N|$ is relatively large compared to $|R|$. Specifically,

they will all work if $|N| \geq 9\log_2|R|$. In order to create the best possible bound, however, we will want to balance $|N|$ against $|R/N|$, so we will use these bounds only when $|N| \geq \sqrt{|R|}$.

The first bound is only useful if $|N|/2$ dominates $2\log_2|R|$. In particular, it will be useful if $|N| \geq 5\log_2|R|$.

Proposition 4.2.6. *We have* $|\mathcal{T}_N^1| \leq 2^{\mathbf{c}(R)-\frac{|N|}{2}+2\log_2|R|-\log_2|N|+(\log_2|N|)^2+2}$.

Proof. Let $S \in \mathcal{T}_N^1$ and set $G_S := \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N)$. Say, $(xN)^f = yN$, for some $xN, yN \in R/N$ with $yN \notin \{xN, x^{-1}N\}$ and for some $f \in G_S$ with $1^f = 1$. Now, $x^f = yt$, for some $t \in N$. Observe that

$$(xn)^f = x^{nf} = x^{f(f^{-1}nf)} = ytn^{\iota_f}, \tag{4.2.8}$$

where we are denoting by $\iota_f : N \to N$ the automorphism induced by the conjugation via f on N. Observe that we have at most $|\mathrm{Aut}(N)| \leq 2^{(\log_2|N|)^2}$ choices for the automorphism ι_f. Therefore, as $t \in N$, given xN and yN, we deduce from (4.2.8) that we have at most $|N|2^{(\log_2|N|)^2}$ choices for the permutation $f_{|xN} : xN \to yN$ restricted to xN.

We consider various possibilities:

(i) $o(xN) = o(yN) = 2$, or

(ii) $o(xN) > 2$ and $o(yN) > 2$, or

(iii) $o(xN) = 2$ and $o(yN) > 2$, or

(iv) $o(xN) > 2$ and $o(yN) = 2$.

We consider these cases in turn: we let $\mathcal{B}_i, \mathcal{B}_{ii}, \mathcal{B}_{iii}, \mathcal{B}_{iv}$ be the subsets of $\mathcal{S}_N^2$ satisfying, respectively, (i), (ii), (iii) or (iv). In the first case, the number of inverse-closed subsets of $R \setminus (xN \cup yN)$ is $2^{\mathbf{c}(R)-\mathbf{c}(xN)-\mathbf{c}(yN)}$ and the number of inverse-closed f-invariant subsets T of $xN \cup yN$ is at most $2^{\mathbf{c}(xN)}$, because once $T \cap xN$ has been chosen the set $T \cap yN$ must equal $(T \cap xN)^f$. Therefore

$$\begin{aligned} |\mathcal{B}_i| &\leq |N|2^{(\log_2|N|)^2}|R/N|^2 2^{\mathbf{c}(R)-\mathbf{c}(xN)-\mathbf{c}(yN)} \cdot 2^{\mathbf{c}(xN)} \\ &= 2^{\mathbf{c}(R)-\mathbf{c}(yN)+2\log_2|R|-\log_2|N|+(\log_2|N|)^2} \leq 2^{\mathbf{c}(R)-\frac{|N|}{2}+2\log_2|R|-\log_2|N|+(\log_2|N|)^2}. \end{aligned}$$

In the second case, the number of inverse-closed subsets of $R\setminus(xN\cup yN\cup x^{-1}N\cup y^{-1}N)$ is $2^{\mathbf{c}(R)-2|N|}$ and the number of inverse-closed f-invariant subsets T of $xN\cup yN\cup x^{-1}N\cup y^{-1}N$ is at most $2^{|N|}$, because once $T\cap xN$ has been chosen we must have $T\cap x^{-1}N = (T\cap xN)^{-1}$, $T\cap yN = (T\cap xN)^f$ and $T\cap y^{-1} = ((T\cap xN)^f)^{-1}$. Therefore

$$|\mathcal{B}_{ii}| \leq |N|2^{(\log_2|N|)^2}|R/N|^2 2^{\mathbf{c}(R)-2|N|} \cdot 2^{|N|} = 2^{\mathbf{c}(R)-|N|+2\log_2|R|-\log_2|N|+(\log_2|N|)^2}.$$

In the third case, the number of inverse-closed subsets of $R \setminus (xN \cup yN \cup y^{-1}N)$ is $2^{\mathbf{c}(R)-\mathbf{c}(xN)-|N|}$ and the number of inverse-closed f-invariant subsets of $xN \cup yN \cup y^{-1}N$ is at most $2^{|N|}$, because once we choose a subset of xN all the others are uniquely determined. Therefore

$$|\mathcal{B}_{iii}| \leq |N|2^{(\log_2|N|)^2}|R/N|^2 2^{\mathbf{c}(R)-\mathbf{c}(xN)-|N|} \cdot 2^{|N|} \leq 2^{\mathbf{c}(R)-\frac{|N|}{2}+2\log_2|R|-\log_2|N|+(\log_2|N|)^2}.$$

The fourth case is similar to the third case and we have $|\mathcal{B}_{iv}| \leq 2^{\mathbf{c}(R)-\frac{|N|}{2}+2\log_2|R|-\log_2|N|+(\log_2|N|)^2}$.

The proof now follows by adding the contribution of the four sets $\mathcal{B}_i$, $\mathcal{B}_{ii}$, $\mathcal{B}_{iii}$ and $\mathcal{B}_{iv}$. □

Our second bound is useful whenever $|N|$ grows with $|R|$.

Proposition 4.2.7. *We have* $|\mathcal{T}_N^2| \leq 2^{\mathbf{c}(R)-\frac{|N|}{96}+(\log_2|N|)^2}$.

Proof. Given $S \in \mathcal{T}_N^2$, we let $G_S := \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N)$. Given $f \in (G_S)_1$, we let $\iota_f : N \to N$ denote the automorphism induced by the action of conjugation of f on N. Let $f \in (G_S)_1 \setminus \mathbf{C}_{(G_S)_1}(N)$ witnessing that $S \in \mathcal{T}_N^2$, that is,

- N is neither an abelian group of exponent greater than 2 nor a generalised dicyclic group, or
- N is an abelian group of exponent greater than 2 and $\iota_f \neq \iota$ (where $\iota : N \to N$ is defined by $x^\iota = x^{-1}$, for every $x \in N$), or
- $N = \mathrm{Dic}(A, x, y) \ncong Q_8 \times C_2^\ell$ and $\iota_f \neq \bar{\iota}_A$ (where $\bar{\iota}_A$ is given in Definition 4.0.8), or
- $N \cong Q_8 \times C_2^\ell$ and $\iota_f \notin \{\bar{\iota}_i, \bar{\iota}_j, \bar{\iota}_k\}$ (where $\bar{\iota}_i, \bar{\iota}_j, \bar{\iota}_k$ are given in Definition 4.0.8).

In each of these cases, by Theorem 4.0.12 applied to N, we deduce that the number of f-invariant inverse-closed subsets of N is at most $2^{\mathbf{c}(N)-|N|/96}$. In particular,

$$|\mathcal{T}_N^2| \leq 2^{\mathbf{c}(R\setminus N)} \cdot 2^{\mathbf{c}(N)-\frac{|N|}{96}} |\operatorname{Aut}(N)| \leq 2^{\mathbf{c}(R)-|N|/96+(\log|N|)^2},$$

where the first factor accounts for the number of inverse-closed subsets of $R \setminus N$, the second factor accounts for the number of inverse-closed f-invariant subsets of N and the third factor accounts for the number of choices of ι_f. □

For our third bound to be useful, we need $|N|/8$ to dominate $\log_2|R|$. In particular, it will be useful if $|N| \geq 9\log_2|R|$.

Proposition 4.2.8. *We have* $|\mathcal{T}_N^3| \leq 2^{\mathbf{c}(R)-\frac{|N|}{8}+\log_2|R|+(\log_2|N|)^2}$.

Proof. Given $S \in \mathcal{T}_N^3$, we let $G_S := \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N)$. Given any element $\kappa \in G_S$, we let $\iota_\kappa : N \to N$ denote the automorphism induced by the action of conjugation of κ on N. Let $x \in R$ and let $f \in (G_S)_1 \setminus \mathbf{C}_{(G_S)_1}(N)$ with $o(xN) > 2$ and assume either

- N is non-abelian, or
- N is abelian and there exists $n \in N$ with $(xn)^f \neq (xn)^{-1}$.

As $S \notin \mathcal{T}_N^1$, we have $(xN)^f \in \{xN, x^{-1}N\}$ and hence $(xN)^f = x^{-1}N$. Thus $x^f = x^{-1}t$, for some $t \in N$. Observe that

$$(xn)^f = x^{nf} = x^{f(f^{-1}nf)} = x^{-1}tn^{\iota_f}. \tag{4.2.9}$$

From (4.2.9), we deduce that we have at most $|\operatorname{Aut}(N)||N| \leq 2^{(\log_2|N|)^2+\log_2|N|}$ choices for the restriction $f_{|xN} : xN \to x^{-1}N$ of f to xN. Let $\beta : xN \to xN$ be the permutation obtained by composing first $f_{|xN}$ and then $\iota : x^{-1}N \to xN$, where ι is defined by $(x^{-1}n)^\iota = (x^{-1}n)^{-1} = n^{-1}x \ \forall n \in N$. Thus, from (4.2.9), we have

$$(xn)^\beta = ((xn)^f)^\iota = (x^{-1}tn^{\iota_f})^{-1} = (n^{-1})^{\iota_f}t^{-1}x = x(n^{-1})^{\iota_{fx}}(t^{-1})^{\iota_x}.$$

Since S is inverse-closed and f-invariant, we deduce that $S \cap xN$ is β-invariant.

Let $\beta' : N \to N$ the permutation defined by $n^{\beta'} = (n^{-1})^{\iota_{fx}}(t^{-1})^{\iota_x} \ \forall n \in N$. An easy computation reveals that $n \in \mathrm{Fix}_N(\beta')$ if and only if $n^{-1}(n^{-1})^{\iota_{fx}} = t^{\iota_x}$. In particular, we are in the position to apply Lemma 4.2.1 (with $\alpha = \iota_{fx}$ and with the element t there replaced by t^{ι_x} here). From Lemma 4.2.1, we have two possibilities:

- $|\mathrm{Fix}_N(\beta')| \leq 3|N|/4$, or
- N is abelian, $t = 1$ and $n^{\iota_{fx}} = n^{-1} \ \forall n \in N$.

If the second possibility holds, then N is abelian, $\iota_f = \iota_{x^{-1}}\iota$ and from (4.2.9) we get $(xn)^f = x^{-1}(n^{\iota_{x^{-1}}})^{-1} = x^{-1}xn^{-1}x^{-1} = (xn)^{-1}$ for every $n \in N$; however, this contradicts the fact that $S \in \mathcal{T}_N^3$. Therefore, $|\mathrm{Fix}_N(\beta')| \leq 3|N|/4$.

The definition of β' and the previous paragraph yield that β has at most

$$\frac{3|N|}{4} + \frac{|N| - \frac{3|N|}{4}}{2} = \frac{7|N|}{8}$$

orbits. Since $S \cap xN$ is β-invariant, the number of choices for $S \cap xN$ is at most $2^{7|N|/8}$. By taking in account the contributions of ι_f, xN and t, we obtain

$$|\mathcal{T}_N^3| \leq 2^{(\log_2|N|)^2}|N||R/N|2^{\mathbf{c}(R\setminus(xN\cup x^{-1}N))}2^{\frac{7|N|}{8}} = 2^{\mathbf{c}(R)-\frac{|N|}{8}+\log_2|R|+(\log_2|N|)^2}. \quad \square$$

Our fifth bound is again useful whenever $|N|$ grows with $|R|$.

Proposition 4.2.9. *We have* $|\mathcal{T}_N^4| \leq 2^{\mathbf{c}(R)-\frac{|N|}{24}+\log_2|R|+2}$.

Proof. Given $S \in \mathcal{T}_N^4$, we let $G_S := \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N)$. Given any element $\kappa \in G_S$, we let $\iota_\kappa : N \to N$ denote the automorphism induced by the action of conjugation of κ on N. Let $\gamma \in R$ and let $f \in (G_S)_1$ with $\gamma^f \notin \{\gamma, \gamma^{-1}\}$. Furthermore, if possible we will choose γ so that $o(\gamma) = 2$. Therefore we may assume that if $o(\gamma) \neq 2$, then $(\gamma')^f = \gamma'$ for every $\gamma' \in R$ with $o(\gamma') = 2$. (This will be important when we apply Lemma 4.2.4.)

We now consider various possibilities depending on the behaviour of γN, but first, we state the fact that the set S does not lie in $\mathcal{T}_N^2$ in a manner tailored to our current needs:

Case A $(G_S)_1 = \mathbf{C}_{(G_S)_1}(N)$, or
Case B N is abelian of exponent greater than 2 and, for every $f \in (G_S)_1 \setminus \mathbf{C}_{(G_S)_1}(N)$ we have $n^f = n^{-1}$ $\forall n \in N$, so $|(G_S)_1 : \mathbf{C}_{(G_S)_1}(N)| = 2$, or
Case C $N = \mathrm{Dic}(A, y, x) \ncong Q_8 \times C_2^\ell$, for every $f \in (G_S)_1 \setminus \mathbf{C}_{(G_S)_1}(N)$, $A = \mathbf{C}_N(f)$ and the automorphism ι_f induced by f on N is $\bar{\iota}_A$, or
Case D $N = Q_8 \times C_2^\ell$, $|(G_S)_1 : \mathbf{C}_{(G_S)_1}(N)| \in \{2, 4\}$, for every $f \in (G_S)_1 \setminus \mathbf{C}_{(G_S)_1}(N)$, the automorphism ι_f induced by f on N is one of $\bar{\iota}_i$, $\bar{\iota}_j$, $\bar{\iota}_k$.

In particular, in cases B, C, and D, $n^{\iota_f} \in \{n, n^{-1}\}$ $\forall n \in N$.

Suppose that $\gamma \in N$. Since $1^f = 1$ and since f normalises N, we have $\gamma^f = \gamma^{\iota_f} \in \{\gamma, \gamma^{-1}\}$. For the rest of the proof, we may suppose that $\gamma \notin N$. Since $S \notin \mathcal{T}_N^1$, we have $(\gamma N)^f \in \{\gamma N, \gamma^{-1}N\}$.

Suppose $(\gamma N)^f \neq \gamma N$. Since $S \notin \mathcal{T}_N^3$, we have $(\gamma n)^f = (\gamma n)^{-1}$ $\forall n \in N$ and hence, in particular, $\gamma^f = \gamma^{-1}$. Therefore, for the rest of the proof, we may suppose that $(\gamma N)^f = \gamma N$.

Since $\gamma^f \in \gamma N$, there exists $t \in N$ with $\gamma^f = \gamma t$. Now,

$$(\gamma n)^f = \gamma^{nf} = \gamma^{f \cdot f^{-1}nf} = (\gamma t)^{n^{\iota_f}} = \gamma t n^{\iota_f}, \quad \forall n \in N. \tag{4.2.10}$$

Suppose now that $\gamma N \neq \gamma^{-1}N$. Then $(\gamma n)^{-1} \in \gamma^{-1}N \neq \gamma N$ for every $n \in N$. Since $(\gamma N)^f = \gamma N$, we cannot have $(\gamma n)^{-1} = (\gamma n)^f$. Thus the orbits of f fuse orbits of the inverse map on $\gamma N \cup \gamma^{-1}N$ unless f has any fixed points on γN; that is, unless (using $(\gamma n)^f = \gamma n$ in (4.2.10)) there exists some $n \in N$ with

$$t = n(n^{\iota_f})^{-1}. \tag{4.2.11}$$

Note that (4.2.10) with $n = 1$ together with $\gamma^f \neq \gamma$ implies that $t \neq 1$. So applying Lemma 4.2.2 to N with $n^\alpha = n^{\iota_f}$ implies that the number of fixed points of f in γN is at most $3|N|/4$. Therefore the action of f on γN together with the action of the inverse map on $\gamma N \cup \gamma^{-1}N$ results in at least $|N|/4$ orbits of length at least 4 and all other orbits having

length at least 2. So when $f_{|\gamma N}$ is given, the number of choices for $S \cap (\gamma N \cup \gamma^{-1}N)$ is at most $2^{(3|N|/4)/2+(|N|/4)/4} = 2^{7|N|/16}$. Therefore

$$|\mathcal{T}_N^4| \leq 3|N||R/N|2^{\mathbf{c}(R)-\mathbf{c}(\gamma N\cup\gamma^{-1}N)}2^{7|N|/16} \leq 2^{2+\log_2|R|}2^{\mathbf{c}(R)-|N|+7|N|/16} = 2^{\mathbf{c}(R)-9|N|/16+\log_2|R|+2}$$

(where $3|N|$ is the number of choices for the restriction $f_{\gamma N} : \gamma N \to \gamma N$ of f to γN, and $|R/N|$ is the number of choices for $\gamma N \in R/N$).

For the remainder of the proof we may assume that $\gamma N = \gamma^{-1}N$, meaning that N is an index-2 subgroup of $\langle \gamma, N\rangle$.

Suppose that $f \in \mathbf{C}_{G_S}(N)$. Then, (4.2.10) becomes $n^f = n$ and $(\gamma n)^f = \gamma t n$, $\forall n \in N$. When $f_{|\gamma N}$ is given, from Lemma 4.2.3, we deduce that the number of choices for $S \cap \langle \gamma, N\rangle$ is at most $2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{16}}$ (recall that the other cases cannot arise since $\gamma^f \notin \{\gamma, \gamma^{-1}\}$). Therefore

$$|\mathcal{T}_N^4| \leq |N||R/N|2^{\mathbf{c}(R)-\mathbf{c}(\langle\gamma,N\rangle)}2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{16}} \leq 2^{\mathbf{c}(R)-\frac{|N|}{16}+\log_2|R|}.$$

(where $|N|$ is the number of choices for the restriction $f_{\gamma N} : \gamma N \to \gamma N$ of f to γN, and $|R/N|$ is the number of choices for $\gamma N \in R/N$). Therefore, for the rest of the proof we may suppose that $f \notin \mathbf{C}_{G_S}(N)$. In particular, only Case B, C or D may arise.

Suppose that Case B holds. Then, (4.2.10) becomes $n^f = n^{-1}$ and $(\gamma n)^f = \gamma t n^{-1}$, $\forall n \in N$, so $n^{\iota f} = n^{-1}$ for every $n \in N$. As already observed at the beginning, if γ cannot be chosen with $o(\gamma) = 2$, then for every $\gamma n \in \gamma N$ with $o(\gamma n) = 2$, we have $(\gamma n)^f = \gamma n$. So we may apply Lemma 4.2.4 with $f_{|\langle\gamma,N\rangle}$ taking the role of α_t.

When $f_{|\gamma N}$ is given, from Lemma 4.2.4, we deduce that the number of choices for $S \cap \langle \gamma, N\rangle$ is at most $2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{24}}$ (again, the other cases cannot arise since $\gamma^f \notin \{\gamma, \gamma^{-1}\}$). Therefore

$$|\mathcal{T}_N^4| \leq |N||R/N|2^{\mathbf{c}(R)-\mathbf{c}(\langle\gamma,N\rangle)}2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{24}} \leq 2^{\mathbf{c}(R)-\frac{|N|}{24}+\log_2|R|}$$

(again, $|N|$ is the number of choices for the restriction $f_{\gamma N} : \gamma N \to \gamma N$ of f to γN, and $|R/N|$ is the number of choices for $\gamma N \in R/N$).

Cases C and D can be dealt with simultaneously. Here, (4.2.10) becomes $n^f = n^{\bar{\iota}_A}$ and $(\gamma n)^f = \gamma t n^{\bar{\iota}_A}$, $\forall n \in N$. When $f_{|\gamma N}$ is given, from Lemma 4.2.5, we deduce that the number of choices for $S \cap \langle \gamma, N\rangle$ is at most $2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{24}}$ (again, the other cases cannot arise since $\gamma^f \notin \{\gamma, \gamma^{-1}\}$). Therefore

$$|\mathcal{T}_N^4| \leq 3|N||R/N|2^{\mathbf{c}(R)-\mathbf{c}(\langle\gamma,N\rangle)}2^{\mathbf{c}(\langle\gamma,N\rangle)-\frac{|N|}{24}} \leq 2^{\mathbf{c}(R)-\frac{|N|}{24}+\log_2|R|+2}$$

(where $3|N|$ is the number of choices for the restriction $f_{\gamma N} : \gamma N \to \gamma N$ of f to γN, and $|R/N|$ is the number of choices for $\gamma N \in R/N$).

□

Combining these results, we are able to bound $|\mathcal{T}_N|$.

Proof of Theorem 4.0.4. Since the initial statement excludes $\mathcal{S}_N^1$, its proof follows by adding the bounds produced in Propositions 4.2.6, 4.2.7, 4.2.8 and 4.2.9 for $|\mathcal{T}_N^i|$, for each $1 \leq i \leq 4$. If we drop the condition $R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$, then we must also add the bound produced in Proposition 4.0.13 for $\mathcal{S}_N^1$ (which has no effect on the bound we have given). Using Proposition 4.0.13 requires us to exclude groups that are either abelian of exponent greater than 2, or generalised dicyclic. □

4.3 Groups with a "small" normal subgroup

We begin this section with a counting result that we will need. The flavour of this result is quite distinct from most of the rest of the chapter and we have placed it in advance of the introduction of the notation and situational information that we will be using for the rest of this section.

Lemma 4.3.1. *Let X be a set and let f and g be permutations of X. Then either*

1. $|\{S \subseteq X \mid |S \cap S^f| = |S \cap S^g|\}| \leq \frac{3}{4} \cdot 2^{|X|}$, *or*
2. *there exists a subset $I \subseteq X$ such that*
   - *I is f- and g-invariant (that is, $I^f = I$ and $I^g = I$),*
   - *$f_{|I} = g_{|I}$,*
   - *$f_{|X\setminus I} = (g^{-1})_{|X\setminus I}$.*

Proof. We denote by F and by G the permutation matrices of f and g, respectively. Therefore, F and G are $|X| \times |X|$-matrices with $\{0,1\}$ entries, with rows and columns indexed by the set X and such that

$$F_{x,y} = \begin{cases} 1 & \text{if } x^f = y, \\ 0 & \text{otherwise,} \end{cases} \qquad G_{x,y} = \begin{cases} 1 & \text{if } x^g = y, \\ 0 & \text{otherwise.} \end{cases}$$

Let $A := F - G$. For any $S \subseteq X$, let $\delta_S \in \mathbb{Z}^X$ be the "indicator" vector of the set S, that is,

$$(\delta_S)_x := \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, let $\langle \cdot, \cdot \rangle : \mathbb{Q}^X \times \mathbb{Q}^X \to \mathbb{Q}$ be the standard scalar product and let $(e_x)_{x \in X}$ be the canonical basis of $\mathbb{Q}^X$.

With the notation above, for every subset S of X, we have

$$|S \cap S^f| = \langle \delta_S, F\delta_S \rangle \text{ and } |S \cap S^g| = \langle \delta_S, G\delta_S \rangle.$$

Therefore,

$$\{S \subseteq X \mid |S \cap S^f| = |S \cap S^g|\} = \{S \subseteq X \mid \langle \delta_S, F\delta_S \rangle = \langle \delta_S, G\delta_S \rangle\} = \{S \subseteq X \mid \langle \delta_S, A\delta_S \rangle = 0\}.$$

For simplicity, we write $\Delta : \{0,1\}^X \to \mathbb{Q}$ for the mapping defined by $\delta \mapsto \Delta(\delta) = \langle \delta, A\delta \rangle$, for every $\delta \in \{0,1\}^X$.

Suppose first that, there exist $i, j \in X$ with $i \neq j$ and $A_{i,j} + A_{j,i} \neq 0$. Fix $\delta_x \in \{0,1\}$ arbitrarily for every $x \in X \setminus \{i,j\}$, and let $\eta := \sum_{x \in X \setminus \{i,j\}} \delta_x e_x$. By restricting Δ, we define the function $\Delta' : \{0,1\} \times \{0,1\} \to \mathbb{Q}$ by setting

$$\begin{aligned} (\delta_i, \delta_j) \quad \mapsto \quad & \Delta'(\delta_i, \delta_j) := \Delta(\eta + \delta_i e_i + \delta_j e_j) = \langle \eta + \delta_i e_i + \delta_j e_j, A(\eta + \delta_i e_i + \delta_j e_j) \rangle \\ & = \langle \eta, A\eta \rangle + \delta_i \langle \eta, Ae_i \rangle + \delta_j \langle \eta, Ae_j \rangle + \delta_i \langle e_i, A\eta \rangle + \delta_j \langle e_j, A\eta \rangle \\ & + \delta_i^2 \langle e_i, Ae_i \rangle + \delta_j^2 \langle e_j, Ae_j \rangle + \delta_i \delta_j \langle e_i, Ae_j \rangle + \delta_i \delta_j \langle e_j, Ae_i \rangle. \end{aligned}$$

A computation yields

$$\Delta'(0,0) + \Delta'(1,1) - \Delta'(1,0) - \Delta'(0,1) = A_{i,j} + A_{j,i} \neq 0.$$

In particular, at least one out of the four choices $(\delta_i, \delta_j) \in \{(0,0), (0,1), (1,0), (1,1)\}$ gives rise to a non-zero value for $\Delta(\eta + \delta_i e_i + \delta_j e_j)$. Therefore, for every choice of $\delta_x \in \{0,1\}$ with

$x \in X \setminus \{i,j\}$, we have at most three more choices for $\delta_i, \delta_j \in \{0,1\}$, for constructing a vector $\delta \in \{0,1\}^X$ with $\Delta(\delta) = 0$. Therefore,

$$\{S \subseteq X \mid \langle \delta_S, A\delta_S \rangle = 0\} \leq 2^{|X|-2} \cdot 3 = \frac{3}{4} \cdot 2^{|X|}$$

and (1) holds.

Suppose that, for every $i, j \in X$ with $i \neq j$, we have $A_{i,j} + A_{j,i} = 0$. In this case,

$$\delta := \sum_{x \in X} \delta_x e_x \mapsto \Delta(\delta) = \sum_{x \in X} A_{x,x}\delta_x.$$

If $A_{i,i} \neq 0$ for some $i \in X$, then we may use the same argument as in the previous paragraph by fixing $\delta_x \in \{0,1\}$ arbitrarily for every $x \in X \setminus \{i\}$, and by considering the restriction of Δ as a function $\Delta'(\delta_i)$ of $\delta_i \in \{0,1\}$ only. In this case, we see that one of the two choices for δ_i gives rise to a vector $\delta \in \{0,1\}^X$ with $\Delta(\delta) = 0$. Therefore,

$$\{S \subseteq X \mid \langle \delta_S, A\delta_S = 0 \rangle\} \leq 2^{|X|-1} \cdot 1 \leq \frac{3}{4} 2^{|X|}$$

and (1) holds.

Suppose now that, for every $i, j \in X$ with $i \neq j$, we have $A_{i,j} + A_{j,i} = 0$ and $A_{i,i} = 0$, that is, A is antisymmetric. Let I be the set of rows of $A = F - G$ that are zero. From the fact that A is antisymmetric and from the definition of A, we see that I is f- and g-invariant, $f_{|I} = g_{|I}$ and $f_{|X\setminus J} = g^{-1}_{|X\setminus J}$. In particular, (2) holds. □

Incidentally, we observe that, if (2) holds in Lemma 4.3.1, then $|S \cap S^f| = |S \cap S^g|$, for every subset S of X. We find this quite interesting on its own. For instance, $f := (1\,2\,3\,4\,5)(6\,7\,8)(9\,10\,11\,12)$ and $g := (1\,5\,4\,3\,2)(6\,7\,8)(9\,12\,11\,10)$ have the property that $|S \cap S^f| = |S \cap S^g|$, for every subset S of $\{1, \ldots, 12\}$.

4.3.1 Specific notation

Henceforth, let R be a finite group of order r acting regularly on itself via the right regular representation: here, we identify the elements of R as permutation in $\mathrm{Sym}(R)$. Let N denote a non-identity proper normal subgroup of R. We let $b := |R : N|$ and we let $\gamma_1, \ldots, \gamma_b$ be coset representatives of N in R. Moreover, we choose $\gamma_1 := 1$ to be the identity in R. Observe that R/N defines a group structure on $\{1, \ldots, b\}$ by setting $ij = k$ for every $i, j, k \in \{1, \ldots, b\}$ with $\gamma_i N \gamma_j N = \gamma_k N$.

Write $v_0 := 1$ where v_0 has to be understood as a point in the set R. For each $i \in \{1, \ldots, b\}$, set $\mathcal{O}_i := {v_0}^{\gamma_i N} = \gamma_i N = N\gamma_i$. Observe that the $\mathcal{O}_i$s are the orbits of N on R, the group N acts regularly on $\mathcal{O}_i$ and $|\mathcal{O}_i| = |N|$.

For an inverse-closed subset S of R, we let $\Gamma(R, S)$ be the Cayley graph of R with connection set S, and we denote by F_S the largest subgroup of $\mathrm{Aut}(\Gamma(R, S))$ under which each orbit of N is invariant. In symbols we have

$$F_S := \{g \in \mathrm{Aut}(\Gamma(R, S)) \mid \mathcal{O}_i^g = \mathcal{O}_i, \text{ for each } i \in \{1, \ldots, b\}\}.$$

(The subscript S in F_S will make some of the later notation cumbersome to use, but it constantly emphasizes that the definition of "F" depends on S.) Similarly, we define

$$B_S := F_S \cap \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N).$$

As above, let S be an inverse-closed subset of R. For a vertex u of $\Gamma(R, S)$ in $\mathcal{O}_i$,

$$\text{let } \sigma(S, u, j) \text{ denote the neighbours of } v_0 \text{ and } u \text{ lying in } \mathcal{O}_j.$$

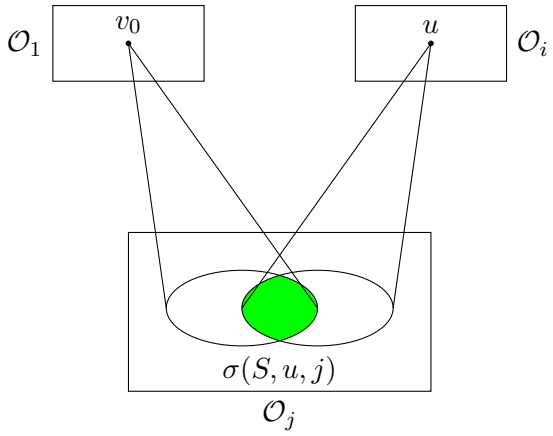

Figure 4.2: The definition of $\sigma(S,u,j)$

See Figure 4.2. It is clear that

$$\sigma(S,u,j) = S \cap S^{g_u} \cap \mathcal{O}_j = (S \cap \mathcal{O}_j) \cap S^{g_u} = S_j \cap S^{g_u},$$

where $g_u \in R$ with $v_0^{g_u} = u$. Since $u \in \mathcal{O}_i$, we have $u = v_0^{\gamma_i k_u}$, for some $k_u \in N$. In particular, $g_u = \gamma_i k_u$. Let $s \in S$ with $s^{g_u} \in S_j$. Then $s^{g_u} \in \mathcal{O}_j = v_0^{\gamma_j N} = v_0^{N\gamma_j}$ and $s^{g_u\gamma_j^{-1}} \in v_0^N = \mathcal{O}_1$. Since g_u maps the element v_0 of $\mathcal{O}_1$ to the element u of $\mathcal{O}_i$, we see that $g_u \in \gamma_i N$ and $s \in \mathcal{O}_1^{\gamma_j g_u^{-1}} = v_0^{N\gamma_j\gamma_i^{-1}} = v_0^{\gamma_j\gamma_i^{-1}N} = \mathcal{O}_{ji^{-1}}$. This shows

$$\sigma(S,u,j) = S_j \cap S_{ji^{-1}}^{g_u} = S_j \cap S_{ji^{-1}}^{\gamma_i k_u}. \tag{4.3.1}$$

For two distinct vertices $u, v \in \mathcal{O}_i$ and $j \in \{1,\dots,b\}$, let

$$\Psi(\{u,v\},j) := \{S \subseteq R \mid S = S^{-1} \text{ and } |\sigma(S,u,j)| = |\sigma(S,v,j)|\}.$$

In the results that follow, we use the notation that we have established here. Our aim with the next few results is to show that $|\Psi(\{u,v\},j)|$ is at most $\frac{3}{4}\cdot 2^{\mathbf{c}(R)}$. This will subsequently be used to bound the number of graphs admitting automorphisms that fix the vertex 1 and also fix each $\mathcal{O}_i$ setwise while mapping u to v. We generally end up with some other possibilities that we gradually eliminate by introducing additional assumptions.

Proposition 4.3.2. *Let $i \in \{2,\dots,b\}$, let u and v be two distinct vertices in $\mathcal{O}_i$ and let $j \in \{1,\dots,b\} \setminus \{1,i\}$. Then, one of the following holds:*

1. $|\Psi(\{u,v\},j)| \le \frac{3}{4}\cdot 2^{\mathbf{c}(R)}$,
2. $j^2 = i$, $\gamma_i = \gamma_j^2\bar{y}$ *for some* $\bar{y} \in N$, $k_u = \bar{y}^{-1}\gamma_j^{-1}\bar{y}k_v\gamma_j$, $k_v = \bar{y}^{-1}\gamma_j^{-1}\bar{y}k_u\gamma_j$ *and* $\gamma_i k_v, \gamma_i k_u$ *centralize* N,
3. $o(ji^{-1}) > 2$, $o(j) = 2$, $o(i)$ *is even,* $o(\gamma_j) = 4$, $\gamma_j^2 = k_v^{-1}k_u = k_u^{-1}k_v$, N *is abelian and* $y^{\gamma_j} = y^{-1}$ *for every* $y \in N$,
4. $o(ji^{-1}) = 2$, $o(j) > 2$, $o(i)$ *is even,* $o(\gamma_{ji^{-1}}) = 4$, $\gamma_{ji^{-1}}^2 = k_v^{-1}k_u = k_u^{-1}k_v$, N *is abelian and* $y^{\gamma_{ji^{-1}}} = y^{-1}$ *for every* $y \in N$,
5. $o(ji^{-1}) = o(j) = 2$

Proof. We divide the proof in various cases.

CASE $j^2 = i$.

Observe that, if $S \subseteq R$ is inverse-closed, then $S_{j^{-1}} = S_j^{-1}$. As $ji^{-1} = j^{-1}$, from (4.3.1), we obtain

$$|\sigma(S,u,j)| = |S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| = |S_{j^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}|, \tag{4.3.2}$$
$$|\sigma(S,v,j)| = |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}| = |S_{j^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}|.$$

Let $\iota : N\gamma_j^{-1} \to N\gamma_j$ be the mapping defined by $x \mapsto x^\iota = x^{-1}$ for every $x \in N\gamma_j^{-1}$ and set

$$f := k_u^{-1}\gamma_i^{-1}\iota : N\gamma_j \to N\gamma_j \text{ and } g := k_v^{-1}\gamma_i^{-1}\iota : N\gamma_j \to N\gamma_j$$

as permutations of $N\gamma_j$. Now, (4.3.2) yields

$$|\sigma(S,u,j)| = |S_j^\iota \cap S_j^{k_u^{-1}\gamma_i^{-1}}| = |S_j \cap S_j^{k_u^{-1}\gamma_i^{-1}\iota}| = |S_j \cap S_j^f|, \tag{4.3.3}$$
$$|\sigma(S,v,j)| = |S_j^\iota \cap S_j^{k_v^{-1}\gamma_i^{-1}}| = |S_j \cap S_j^{k_v^{-1}\gamma_i^{-1}\iota}| = |S_j \cap S_j^g|.$$

From (4.3.3), we see that we are in the position to apply Lemma 4.3.1 with $X := \mathcal{O}_j$. If Lemma 4.3.1 (1) holds, then the number of subsets $S_j \subseteq \mathcal{O}_j$ satisfying (4.3.3) is at most $\frac{3}{4} \cdot 2^{|N|}$. Therefore

$$|\Psi(\{u,v\},j)| \leq \frac{3}{4} 2^{|N|} \cdot 2^{\mathbf{c}(R)-|N|},$$

observe that $2^{\mathbf{c}(R)-|N|}$ counts the number of inverse-closed subsets of $R \setminus (\gamma_j N \cup \gamma_j^{-1} N)$. Thus (1) is proved in this case.

Therefore, we may suppose that Lemma 4.3.1 (2) holds. Therefore, there exists an f- and g-invariant subset I of $N\gamma_j$ such that $f_{|I} = g_{|I}$ and $f_{|N\gamma_j \setminus I} = (g^{-1})_{|N\gamma_j \setminus I}$. If $I \neq \varnothing$, then there exists $x \in I$ and hence

$$x^{k_u^{-1}\gamma_i^{-1}\iota} = x^f = x^g = x^{k_v^{-1}\gamma_i^{-1}\iota}.$$

Simplifying ι and γ_i^{-1}, we obtain $xk_u^{-1} = xk_v^{-1}$. This yields $k_u = k_v$, contradicting the fact that $u \neq v$. Therefore $I = \varnothing$ and hence $f = g^{-1}$.

This means that, for every $x \in N\gamma_j$, we have

$$x = x^{fg} = x^{k_u^{-1}\gamma_i^{-1}\iota k_v^{-1}\gamma_i^{-1}\iota} = (xk_u^{-1})^{\gamma_i^{-1}\iota k_v^{-1}\gamma_i^{-1}\iota} = (xk_u^{-1}\gamma_i^{-1})^{\iota k_v^{-1}\gamma_i^{-1}\iota} = (\gamma_i k_u x^{-1})^{k_v^{-1}\gamma_i^{-1}\iota} \tag{4.3.4}$$
$$= (\gamma_i k_u x^{-1} k_v^{-1})^{\gamma_i^{-1}\iota} = (\gamma_i k_u x^{-1} k_v^{-1}\gamma_i^{-1})^\iota = \gamma_i k_v x k_u^{-1}\gamma_i^{-1}.$$

As $j^2 = i$, there exists $\bar{y} \in N$ with

$$\gamma_i = \gamma_j^2 \bar{y}. \tag{4.3.5}$$

When $x = \gamma_j$, (4.3.4) gives

$$\gamma_i^{-1}\gamma_j\gamma_i = k_v\gamma_j k_u^{-1}.$$

Using (4.3.5), we obtain $\gamma_i^{-1}\gamma_j\gamma_i = \bar{y}^{-1}\gamma_j\bar{y}$. Therefore

$$k_u = \bar{y}^{-1}\gamma_j^{-1}\bar{y}k_v\gamma_j. \tag{4.3.6}$$

From (4.3.4), (4.3.5) and (4.3.6), we obtain

$$x = \gamma_i k_v x \gamma_j^{-1} k_v^{-1}\bar{y}^{-1}\gamma_j^{-1}, \qquad \forall x \in N\gamma_j.$$

By writing $x = y\gamma_j$ with $y \in N$, we deduce

$$y = (\gamma_i k_v) y (\gamma_i k_v)^{-1}, \qquad \forall y \in N.$$

Since y is an arbitrary element of N, we get that $\gamma_i k_v$ centralizes N. From this and from (4.3.5) and (4.3.6) we see that (2) holds. ■

For the rest of the proof, we suppose $j^2 \neq i$. From (4.3.1), we obtain

$$|\sigma(S,u,j)| = |S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| \quad \text{and} \quad |\sigma(S,v,j)| = |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}|. \tag{4.3.7}$$

From (4.3.7), we see that the condition "$|\sigma(S,u,j)| = |\sigma(S,v,j)|$" imposes no constraint on S_x, for $x \notin \{j, ji^{-1}, j^{-1}, (ji^{-1})^{-1}\}$. Observe that

$$\{j, j^{-1}\} \neq \{ji^{-1}, (ji^{-1})^{-1}\},$$

because we are assuming $j^2 \neq i$. As usual, there is one implicit condition on the set S: it is inverse-closed. This suggests a natural decomposition of S. Write $R_{j,i} := \gamma_j N \cup \gamma_j^{-1} N \cup \gamma_{ji^{-1}} N \cup \gamma_{ji^{-1}}^{-1} N$ and $R_{j,i}^c := R \setminus R_{j,i}$. We have

$$\mathbf{c}(R_{j,i}) = \begin{cases} 2|N| & \text{if } o(j) > 2 \text{ and } o(ji^{-1}) > 2, \\ |N| + \mathbf{c}(\gamma_j N) & \text{if } o(j) = 2 \text{ and } o(ji^{-1}) > 2, \\ |N| + \mathbf{c}(\gamma_{ji^{-1}} N) & \text{if } o(j) > 2 \text{ and } o(ji^{-1}) = 2, \\ \mathbf{c}(\gamma_j N) + \mathbf{c}(\gamma_{ji^{-1}} N) & \text{if } o(j) = o(ji^{-1}) = 2. \end{cases} \tag{4.3.8}$$

Observe that $R_{j,i}$ and $R_{j,i}^c$ are inverse-closed; moreover, we may write $S := S_{j,i} \cup S_{j,i}^c$, where $S_{j,i} \subseteq R_{j,i}$ and $S_{j,i}^c \subseteq R_{j,i}^c$.

Using this decomposition of the inverse-closed subsets, we get

$$|\Psi(\{u,v\}, j)| = A \cdot 2^B,$$

where 2^B is the number of inverse-closed subsets $S_{j,i}^c \subseteq R_{j,i}^c$ and A is the number of inverse-closed subsets $S_{j,i} \subseteq R_{j,i}$ such that $|S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| = |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}|$ with $S := S_{j,i} \cup S_{j,i}^c$. We deduce

$$B = \mathbf{c}(R) - \mathbf{c}(R_{j,i}). \tag{4.3.9}$$

Case $o(ji^{-1}) > 2$.

When $o(j) > 2$, let t_1 be the number of subsets S_j of $\mathcal{O}_j$ with $S_j^{k_u^{-1}} = S_j^{k_v^{-1}}$. When $o(j) = 2$, let t_1 be the number of inverse-closed subsets S_j of $\mathcal{O}_j$ with $S_j^{k_u^{-1}} = S_j^{k_v^{-1}}$. In both cases, let

$$t_2 = 2^{\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N)} - t_1.$$

Observe that for every subset $S \subseteq R$ with $S_j^{k_u^{-1}} = S_j^{k_v^{-1}}$, we have $S \in \Psi(\{u,v\}, j)$ because $S_j^{k_u^{-1}\gamma_i^{-1}} = S_j^{k_v^{-1}\gamma_i^{-1}}$ and hence $|S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| = |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}|$. (In other words, when $S_j^{k_u^{-1}} = S_j^{k_v^{-1}}$, we have no constraint on $S_{ji^{-1}}$.) If $S_j^{k_u^{-1}} = S_j^{k_v^{-1}}$, then $S_j = S_j^{k_v^{-1}k_u}$ and hence S_j is a union of $\langle k_v^{-1}k_u \rangle$-orbits. As N acts regularly on $\mathcal{O}_j$, we have

$$t_1 \leq 2^{\frac{|N|}{o(k_v^{-1}k_u)}}. \tag{4.3.10}$$

Next let $S \in \Psi(\{u,v\}, j)$ and suppose S_j is a subset of $\mathcal{O}_j$ with $S_j^{k_u^{-1}} \neq S_j^{k_v^{-1}}$. Here to estimate the number of inverse-closed subsets S of R with $|S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| = |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}|$, we estimate the number of subsets satisfying the weaker (but easier to handle) condition

$$|S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| \equiv |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}| \mod 2.$$

Now $S_j^{k_u^{-1}\gamma_i^{-1}}$ and $S_j^{k_v^{-1}\gamma_i^{-1}}$ are two distinct subsets of $\mathcal{O}_{ji^{-1}}$ of the same size a, say. Let b be the size of $S_j^{k_u^{-1}\gamma_i^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}$. Observe that $a - b > 0$ because $S_j^{k_u^{-1}} \neq S_j^{k_v^{-1}}$. A subset $S_{ji^{-1}}$ of $\mathcal{O}_{ji^{-1}}$ with $|S_{ji^{-1}} \cap S_j^{k_u^{-1}\gamma_i^{-1}}| \equiv |S_{ji^{-1}} \cap S_j^{k_v^{-1}\gamma_i^{-1}}| \mod 2$ can be written as $X \cup Y$, where X is an arbitrary subset of $\mathcal{O}_{ji^{-1}} \setminus (S_j^{k_v^{-1}\gamma_i^{-1}} \setminus S_j^{k_u^{-1}\gamma_i^{-1}})$ and Y is a subset of $S_j^{k_v^{-1}\gamma_i^{-1}} \setminus S_j^{k_u^{-1}\gamma_i^{-1}}$ of size having parity uniquely determined by the parity of $|X|$. Therefore we have $2^{|N|-(a-b)}2^{(a-b)-1} = 2^{|N|-1}$ choices for $S_{ji^{-1}}$. Altogether we have

$$A \leq t_1 \cdot 2^{|N|} + t_2 \cdot 2^{|N|-1} = t_1 2^{|N|} + (2^{\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N)} - t_1)2^{|N|-1} = 2^{|N|+\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N)-1} + t_1 2^{|N|-1}$$

As $o(ji^{-1}) > 2$, from (4.3.8), we have $|N| + \mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N) = \mathbf{c}(R_{j,i})$ and hence, from (4.3.10) (noting that if $o(j) > 2$ then $\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N) = |N|$, and otherwise $\gamma_j N \cup \gamma_j^{-1} N = \gamma_j N$), we get

$$\begin{aligned} A &\leq 2^{\mathbf{c}(R_{j,i})-1} + t_1 2^{|N|-1} \leq 2^{\mathbf{c}(R_{j,i})-1} + 2^{|N|+\frac{|N|}{o(k_v^{-1}k_u)}-1} \\ &= 2^{\mathbf{c}(R_{j,i})} \left(\frac{1}{2} + \frac{1}{2^{1+\mathbf{c}(R_{j,i})-|N|-\frac{|N|}{o(k_v^{-1}k_u)}}} \right) \\ &= 2^{\mathbf{c}(R_{j,i})} \left(\frac{1}{2} + \frac{1}{2^{1+\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N)-\frac{|N|}{o(k_v^{-1}k_u)}}} \right). \end{aligned} \tag{4.3.11}$$

When $\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N) > |N|/o(k_v^{-1}k_u)$, (4.3.11) yields

$$A \leq 2^{\mathbf{c}(R_{j,i})} \cdot \left(\frac{1}{2} + \frac{1}{2^2} \right) = \frac{3}{4} \cdot 2^{\mathbf{c}(R_{j,i})}$$

and hence (1) holds in this case. Assume $\mathbf{c}(\gamma_j N \cup \gamma_j^{-1} N) \leq |N|/o(k_v^{-1}k_u)$, that is,

$$\frac{|N|}{o(k_v^{-1}k_u)} \geq \begin{cases} \frac{|N\gamma_j| + |N\gamma_j \cap I(R)|}{2} & \text{when } o(j) = 2, \\ |N| & \text{when } o(j) > 2. \end{cases}$$

As $k_v^{-1}k_u \neq 1$, we have $o(k_v^{-1}k_u) \geq 2$ and hence $o(j) = 2$. Thus

$$\frac{|N|}{o(k_v^{-1}k_u)} \geq \frac{|N\gamma_j| + |N\gamma_j \cap I(R)|}{2}.$$

Since the left-hand side is at most $|N|/2$ and since the right-hand side is at least $|N|/2$, this implies $o(k_v^{-1}k_u) = 2$ and

$$0 \geq \frac{|N\gamma_j \cap I(R)|}{2}.$$

Therefore $N\gamma_j \cap I(R) = \varnothing$, $N\gamma_j$ contains no involutions and $\mathbf{c}(\gamma_j N) = |N|/2$. Under these strong conditions we refine the upper bound in (4.3.11) by first improving our upper bound in (4.3.10).

As $o(j) = 2$, $N\gamma_j$ is inverse-closed. Recall that t_1 is the number of inverse-closed subsets $S_j \subseteq N\gamma_j$ with $S_j^{k_v^{-1}k_u} = S_j$. Consider the permutation $\iota : \gamma_j N \to \gamma_j N$ defined by mapping

$$\gamma_j y \mapsto (\gamma_j y)^{-1} = y^{-1}\gamma_j^{-1},$$

for each $y \in N$, and consider the permutation $\delta : \gamma_j N \to \gamma_j N$ defined by mapping

$$\gamma_j y \mapsto \gamma_j y k_v^{-1} k_u,$$

for each $y \in N$. Observe that ι and δ are involutions with no fixed points: ι has no fixed points because $\gamma_j N$ contains no involutions and δ is an involution because $o(k_v^{-1}k_u) = 2$. In this new setting,

$$t_1 = 2^o,$$

where o is the number of orbits of $\langle \iota, \delta \rangle \leq \mathrm{Sym}(\gamma_j N)$. Each orbit of $\langle \iota, \delta \rangle$ has even length, because ι has order 2 and has no fixed points. Suppose $\langle \iota, \delta \rangle$ has at least one orbit of length greater then 2. Then $o \leq |N|/2 - 1$ (the upper bound is achieved when $\langle \iota, \delta \rangle$ has $|N|/2 - 2$ orbits of length 2 and one of length 4). Thus, in this case,

$$t_1 \leq 2^{\frac{|N|}{2}-1}.$$

Using this slight improvement on x and $\mathbf{c}(\gamma_j N) = |N|/2$, we obtain

$$\begin{aligned} A &\leq t_1 \cdot 2^{|N|} + t_2 \cdot 2^{|N|-1} = t_1 2^{|N|} + (2^{\frac{|N|}{2}} - t_1)2^{|N|-1} = 2^{\frac{3|N|}{2}-1} + t_1 2^{|N|-1} \\ &\leq 2^{\frac{3|N|}{2}-1} + 2^{\frac{3|N|}{2}-2} = \frac{3}{4} \cdot 2^{\frac{3|N|}{2}}. \end{aligned}$$

As $\mathbf{c}(R_{j,i}) = |N| + \mathbf{c}(\gamma_j N) = 3|N|/2$ (see (4.3.8)), we obtain

$$A \leq \frac{3}{4} \cdot 2^{\mathbf{c}(R_{j,i})}. \tag{4.3.12}$$

In particular, from (4.3.9) and (4.3.12), we see that (1) holds.

It remains to suppose that each orbit of $\langle \iota, \delta \rangle$ has length 2; this means $\iota = \delta$, that is,

$$(\gamma_j y)^\iota = (\gamma_j y)^\delta, \quad \forall y \in N.$$

In other words, $y^{-1}\gamma_j^{-1} = \gamma_j y k_v^{-1} k_u$, for every $y \in N$. Set $z := k_v^{-1}k_u$. Applying this equality with $y = 1$, we get $\gamma_j^{-1} = \gamma_j z$ and hence $\gamma_j^2 = z$ because z has order 2. Thus we have $y^{-1}\gamma_j^{-1} = \gamma_j y \gamma_j^{-2}$ and hence $\gamma_j y \gamma_j^{-1} = y^{-1}$. This shows that the element γ_j acts by conjugation on N inverting each of its elements. Therefore, N is abelian.

To complete this case, we need to show that $o(i)$ is even. Observe that since $o(j) = 2$ we have $j = (i^{-1})(ij) = ((i^{-1})(ij))^{-1} = (ij)^{-1}i$. Therefore, $i^2 j = (i)(ij) = (ij)^{-1}i^{-1} = ji^{-2}$ has order 2. Since $o(ij) = o(ji^{-1}) > 2$, we cannot have $i \in \langle i^2 \rangle$, so $o(i)$ must be even. In particular, (3) holds. ■

Case $o(ji^{-1}) = 2$ and $o(j) > 2$.

This case can be reduced to the case above. Set $u' := v_0^{g_u^{-1}}$ and observe that $g_u^{-1} = k_u^{-1}\gamma_i^{-1}$ and hence $u' \in \mathcal{O}_{i^{-1}}$. From (4.3.1), we have

$$|\sigma(S, u, j)| = |S_j \cap S_{ji^{-1}}^{g_u}| = |S_j^{g_u^{-1}} \cap S_{ji^{-1}}| = |S_{ji^{-1}} \cap S_j^{g_u^{-1}}| = |\sigma(S, u', ji^{-1})|.$$

Similarly, $|\sigma(S, v, j)| = |\sigma(S, v', ji^{-1})|$, where $v' := v_0^{g_v^{-1}}$. In particular, $|\sigma(S, u, j)| = |\sigma(S, v, j)|$ if and only if $|\sigma(S, u', ji^{-1})| = |\sigma(S, v', ji^{-1})|$. Thus $|\Psi(\{u, v\}, j)| = |\Psi(\{u', v'\}, ji^{-1})|$. As $o(j) > 2$ and $o(ji^{-1}) = 2$, this case follows by applying the previous case to $\Psi(\{u', v'\}, ji^{-1})$. We obtain that either (1) or (4) holds.

Case $o(ji^{-1}) = o(j) = 2$. This is the only remaining option.

□

For three distinct vertices $u, v, w \in \mathcal{O}_i$ and $j \in \{1, \ldots, b\}$, let

$$\Psi(\{u, v, w\}, j) := \{S \subseteq R \mid S = S^{-1} \text{ and } |\sigma(S, u, j)| = |\sigma(S, v, j)| = |\sigma(S, w, j)|\}.$$

Proposition 4.3.3. *Let $i \in \{2, \ldots, b\}$, let u, v, and possibly w be distinct vertices in $\mathcal{O}_i$ and let $j \in \{1, \ldots, b\} \setminus \{1, i\}$. Then unless $o(j) = o(ji^{-1}) = 2$, we can conclude that:*

- *if $o(i)$ is odd, then $|\Psi(\{u,v\},j)| \leq \frac{3}{4}\cdot 2^{\mathbf{c}(R)}$ or $j^2 = i$; and*
- *if w exists, then $|\Psi(\{u,v,w\},j)| \leq \frac{3}{4}\cdot 2^{\mathbf{c}(R)}$.*

Proof. Assume that we do not have $o(j) = o(ji^{-1}) = 2$.

We apply Proposition 4.3.2 to $\{u,v\}$. If $o(i)$ is odd, we see immediately that Proposition 4.3.2 parts (3), (4), and (5) cannot arise. Parts (1) and (2) are the conclusions we desire.

We also apply Proposition 4.3.2 for the pairs $\{v,w\}$ and $\{w,u\}$. If Proposition 4.3.2 part (1) holds for one (or more) of the three pairs, then the result immediately follows. Therefore, we suppose that none of the pairs $\{v,w\}$, $\{v,u\}$ and $\{w,u\}$ satisfies Proposition 4.3.2 part (1).

Assume that there exists a pair satisfying Proposition 4.3.2 part (2). Then $j^2 = i$. It follows that $o(j) > 2$ and $o(ji^{-1}) > 2$. In particular, each pair satisfies Proposition 4.3.2 part (2). However, by applying Proposition 4.3.2 part (2) to the pairs $\{u,v\}$ and $\{w,v\}$, we get

$$k_u = \bar{y}^{-1}\gamma_j^{-1}\bar{y}k_v\gamma_j = k_w,$$

contradicting the fact that $u \neq w$. Therefore, none of the pairs $\{v,w\}$, $\{v,u\}$ and $\{w,u\}$ satisfies Proposition 4.3.2 part (2).

Now, it is readily seen that, if one of the pairs satisfies Proposition 4.3.2 part (3) (respectively, part (4)), then all pairs satisfy Proposition 4.3.2 part (3) (respectively, part (4)). In particular, we deduce

$$k_v^{-1}k_w = \gamma_j^2 = k_v^{-1}k_u,$$

contradicting the fact that $u \neq w$. (The argument when the pairs satisfy Proposition 4.3.2 part (4) is similar.) □

For two distinct vertices $u, v \in \mathcal{O}_i$, let

$$\Psi(\{u,v\}) := \bigcap_{j\in\{1,\ldots,b\}\setminus\{1,i\}} \Psi(\{u,v\},j).$$

Similarly, for three distinct vertices $u, v, w \in \mathcal{O}_i$ and $j \in \{1,\ldots,b\}\setminus\{1,i\}$, let

$$\Psi(\{u,v,w\}) := \bigcap_{j\in\{1,\ldots,b\}\setminus\{1,i\}} \Psi(\{u,v,w\},j).$$

Our next result further refines these possibilities.

Proposition 4.3.4. *Let $i \in \{2,\ldots,b\}$, and let u, v, and possibly w be distinct vertices in $\mathcal{O}_i$.*

- *If $o(i)$ is odd, then $|\Psi(\{u,v\})| \leq 2^{\mathbf{c}(R)-0.02\cdot\frac{|R|}{|N|}}$.*
- *If w exists and R/N is not an elementary abelian 2-group, then $|\Psi(\{u,v,w\})| \leq 2^{\mathbf{c}(R)-0.02\cdot\frac{|R|}{|N|}}$.*

Proof. If $o(i)$ is odd, then R/N is not an elementary abelian 2-group, so we may assume this throughout the proof.

We define an auxiliary graph X: the vertex-set of X is $\{\{j,j^{-1}\} \mid j \in R/N\}$ and the vertex $\{j,j^{-1}\}$ is declared to be adjacent to

$$\{ji^{-1}, ij^{-1}\},\ \{ij, j^{-1}i^{-1}\},\ \{j^{-1}i, i^{-1}j\} \text{ and } \{ji, i^{-1}j^{-1}\}.$$

In particular, X is a graph with $\mathbf{c}(R/N)$ vertices and where each vertex has valency at most 4. Observe that some vertex $\{j,j^{-1}\}$ might have valency less than four, because the

elements $\{ji^{-1}, ij^{-1}\}$, $\{ij, j^{-1}i^{-1}\}$, $\{j^{-1}i, i^{-1}j\}$ and $\{ji, i^{-1}j^{-1}\}$ are not necessarily distinct. Moreover, some vertex $\{j, j^{-1}\}$ might have a loop: indeed, it is easy to check that $\{j, j^{-1}\}$ has a loop if and only if $j^2 \in \{j, j^{-1}\}$.

Let Y be the subgraph induced by X on $R/N \setminus I(R/N)$. Since R/N is not an elementary abelian 2-group, by a result of Miller [118], we get $|R \setminus I(R/N)| \geq |R/N|/4$. Now, a classical graph theoretic result of Caro-Turán-Wei [37, 159, 162] yields that Y has an independent set, $\mathcal{I}$ say, of cardinality at least

$$\sum_{\substack{\{j,j^{-1}\} \\ o(j)>2}} \frac{1}{\deg_X(\{j, j^{-1}\}) + 1} \geq \frac{|R/N|/4}{5} = \frac{|R|}{20|N|}.$$

Thus $\mathcal{I} = \{\{j_1, j_1^{-1}\}, \ldots, \{j_\ell, j_\ell^{-1}\}\}$, for some $\ell \geq |R|/20|N|$. The independence of $\mathcal{I}$ yields that, for every two distinct vertices $\{j_u, j_u^{-1}\}$ and $\{j_v, j_v^{-1}\}$ in $\mathcal{I}$, the neighbourhood of $\{j_u, j_u^{-1}\}$ and $\{j_v, j_v^{-1}\}$ are disjoint. Therefore, (4.3.1) yields that the events $\Psi(\{u, v\}, j)$ and $\Psi(\{u, v\}, j')$ are independent, and likewise (if w exists) that the events $\Psi(\{u, v, w\}, j)$ and $\Psi(\{u, v, w\}, j')$ are independent.

Furthermore, if $o(i)$ is odd and one of these ℓ vertices corresponds to the unique j with $j^2 = i$ then the same vertex corresponds to j^{-1}, and $(j^{-1})^2 = i^{-1} \neq i$ since $o(i)$ is odd, so we may choose the event $\Psi(\{u, v\}, j^{-1})$ instead of $\Psi(\{u, v\}, j)$, avoiding the possibility that part (2) of Proposition 4.3.2 arises.

Thus, it follows from Proposition 4.3.3 for either $\Psi = \Psi(\{u, v\})$ or $\Psi = \Psi(\{u, v, w\})$ as appropriate, that

$$\Psi \leq \left(\frac{3}{4}\right)^{\ell} \cdot 2^{\mathbf{c}(R)} \leq \left(\frac{3}{4}\right)^{\frac{|R|}{20|N|}} \cdot 2^{\mathbf{c}(R)} = 2^{\mathbf{c}(R) - \log_2(4/3)(\frac{|R|}{20|N|})} < 2^{\mathbf{c}(R) - 0.02 \cdot \frac{|R|}{|N|}}. \quad \square$$

We now use the bounds we have achieved, to show that the number of graphs admitting automorphisms that fix every orbit $\mathcal{O}_k$ setwise, but act nontrivially on some $\mathcal{O}_i$ is a vanishingly small fraction of the $2^{\mathbf{c}(R)}$ Cayley graphs on R, as long as either $o(i)$ is odd, or the orbit on $\mathcal{O}_i$ has length at least 3. Actually, these formulas only produce results that are vanishingly small if $|N|$ is small enough relative to $|R|$ that $|R|/|N|$ grows with $|R|$, so this is the point at which it starts to become clear that we need to be assuming that $|N|$ is relatively small, in order to apply the results in this section. The result involving an orbit of length 3 does not work in the case that R/N is an elementary abelian 2-group; this case will need to be handled separately.

Lemma 4.3.5. *Let*

$$\mathcal{S} := \{S \subseteq R \mid S = S^{-1}, \text{ there exists } i \in \{2, \ldots, b\} \text{ with } o(i) \text{ odd such that } (F_S)_{v_0} \text{ has a nontrivial orbit on } \mathcal{O}_i\}.$$

Furthermore, if R/N is not elementary abelian 2-group, let

$$\mathcal{S}' := \{S \subseteq R \mid S = S^{-1}, \text{ there exists } i \in \{2, \ldots, b\} \text{ such that } (F_S)_{v_0} \text{ has an orbit of cardinality at least 3 on } \mathcal{O}_i\}.$$

Then $|\mathcal{S}| \leq 2^{\mathbf{c}(R) - 0.02\frac{|R|}{|N|} + \log_2(|R||N|/2)}$ *and* $|\mathcal{S}'| \leq 2^{\mathbf{c}(R) - 0.02\frac{|R|}{|N|} + \log_2(|R||N|^2/6)}$.

Proof. For each $i \in \{2, \ldots, b\}$ with $o(i)$ odd, let $\mathcal{S}_i$ be the subset of $\mathcal{S}$ defined by

$$\mathcal{S}_i := \{S \subseteq R \mid S = S^{-1}, (F_S)_{v_0} \text{ has a nontrivial orbit on } \mathcal{O}_i\}.$$

If $o(i)$ is even then define $\mathcal{S}_i = \varnothing$. Clearly, $\mathcal{S} = \bigcup_{i=2}^{b} \mathcal{S}_i$.

Similarly, for each $i \in \{2, \dots, b\}$, let $\mathcal{S}'_i$ be the subset of $\mathcal{S}'$ defined by

$$\mathcal{S}'_i := \{S \subseteq R \mid S = S^{-1}, (F_S)_{v_0} \text{ has an orbit of cardinality at least 3 on } \mathcal{O}_i\}.$$

Clearly, $\mathcal{S}' = \bigcup_{i=2}^{b} \mathcal{S}'_i$.

Let $i \in \{2, \dots, b\}$, let $S \in \mathcal{S}_i$ with $o(i)$ odd, or $S \in \mathcal{S}'_i$ (as appropriate) and let u, v, and possibly w be distinct vertices of $\mathcal{O}_i$ in the same $(F_S)_{v_0}$-orbit. In particular, there exists $f \in (F_S)_{v_0}$ with $u = v^f$, and if w exists then there exists $f' \in (F_S)_{v_0}$ with $u^{f'} = w$. Since f (and f' if it exists) is an automorphism of $\Gamma(R, S)$ fixing each N-orbit setwise, we deduce

$$\begin{aligned} \sigma(S, v, j)^f &= \sigma(S, v^f, j) = \sigma(S, u, j), \text{ and if } w \text{ exists then} \\ \sigma(S, v, j)^{f'} &= \sigma(S, v^{f'}, j) = \sigma(S, w, j), \end{aligned}$$

for every $j \in \{1, \dots, b\} \setminus \{1, i\}$. Hence, $|\sigma(S, u, j)| = |\sigma(S, v, j)| (= |\sigma(S, w, j)|)$ and $S \in \Psi(\{u, v\}, j)$ or $\Psi(\{u, v, w\}, j)$. Since this holds for each $j \in \{1, \dots, b\} \setminus \{1, i\}$, we get $S \in \Psi(\{u, v\})$ or $S \in \Psi(\{u, v, w\})$.

The argument in the previous paragraph shows that

$$\mathcal{S}_i \subseteq \bigcup_{\substack{\{u,v\} \subseteq \mathcal{O}_i \\ u \neq v}} \Psi(\{u, v\}) \text{ or } \mathcal{S}_i \subseteq \bigcup_{\substack{\{u,v,w\} \subseteq \mathcal{O}_i \\ |\{u,v,w\}| = 3}} \Psi(\{u, v, w\}).$$

From Proposition 4.3.4, we deduce that

$$|\mathcal{S}| \leq (b-1) \binom{|N|}{2} 2^{\mathbf{c}(R) - 0.02 \cdot \frac{|R|}{|N|}} \leq \frac{|R|}{|N|} \frac{|N|^2}{2} 2^{\mathbf{c}(R) - 0.02 \cdot \frac{|R|}{|N|}}$$

and

$$|\mathcal{S}'| \leq (b-1) \binom{|N|}{3} 2^{\mathbf{c}(R) - 0.02 \cdot \frac{|R|}{|N|}} \leq \frac{|R|}{|N|} \frac{|N|^3}{6} 2^{\mathbf{c}(R) - 0.02 \cdot \frac{|R|}{|N|}}. \quad \square$$

Our next result deals specifically with the case that R/N is an elementary abelian 2-group. (We refer to Section 4.3.1 for the definition of B_S.)

Lemma 4.3.6. *(Recall the notation in Section 4.3.1.) Suppose R is not an abelian group of exponent greater than 2, that R is not a generalized dicyclic group and that R/N is an elementary abelian 2-group. Then*

$$|\{S \subseteq R \mid S = S^{-1}, (B_S)_{v_0} \neq 1\}| \leq 2^{\mathbf{c}(R) - \frac{|R|}{192} + (\log_2 |R|)^2 + 2}.$$

Proof. Let $\mathcal{S} := \{S \subseteq R \mid S = S^{-1}, (B_S)_{v_0} \neq 1\}$. Observe that the definition of B_S immediately yields $B_S \trianglelefteq \mathrm{Aut}(\Gamma(R, S))$. In particular, RB_S is a group of automorphisms of $\Gamma(R, S)$ acting transitively on the vertex set R and normalizing N. Since R is also transitive on the vertex set, the Frattini argument gives $RB_S = R(B_S)_{v_0}$.

Let

$$\mathcal{S}' := \{S \in \mathcal{S} \mid R < \mathbf{N}_{RB_S}(R)\} \quad \text{and} \quad \mathcal{S}'' := \mathcal{S} \setminus \mathcal{S}'.$$

Since R is not an abelian group of exponent greater than 2 and since R is not a generalized dicyclic group, Proposition 4.0.13 yields

$$|\{S \subseteq R \mid S = S^{-1}, R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\}| \leq 2^{\mathbf{c}(R) - \frac{|R|}{96} + (\log_2 |R|)^2}.$$

In particular, $|\mathcal{S}'| \leq 2^{\mathbf{c}(R) - \frac{|R|}{96} + (\log_2 |R|)^2}$.

For each $S \in \mathcal{S}''$, choose G_S a subgroup of RB_S with $R < G_S$ and with R maximal in G_S. Observe that $\mathbf{N}_{RB_S/N}(R/N) = R/N$, because $\mathbf{N}_{RB_S}(R) = R$.

Let K be the core of R in G_S. Then

$$K = \bigcap_{g \in G_S} R^g \geq \bigcap_{g \in G_S} N^g = N.$$

Since R is maximal in G_S, G_S/K acts primitively and faithfully on the set of right cosets of R in G_S. The stabilizer of a point in this action is R/K. As $N \leq K$, we deduce that R/K is an elementary abelian 2-group. From [121, Lemma 2.1], we deduce $|G_S : R| = |(G_S)_{v_0}|$ is a prime odd number and $|R : K| = 2$.

We now partition the set $\mathcal{S}'$ further. We define

$$\mathcal{C} := \{S \in \mathcal{S}'' \mid (G_S)_{v_0} \text{ does not act trivially by conjugation on } K\},$$
$$\mathcal{C}' := \mathcal{S}'' \setminus \mathcal{C} = \{S \in \mathcal{S}'' \mid (G_S)_{v_0} \leq \mathbf{C}_{G_S}(K)\}.$$

In what follows, we obtain an upper bound on the cardinality of $\mathcal{C}$ and $\mathcal{C}'$.

For each $S \in \mathcal{C}$, let $\pi_S : (G_S)_{v_0} \to \mathrm{Aut}(K)$ the natural homomorphism given by the conjugation action of $(G_S)_{v_0}$ on K. For each $\varphi \in \mathrm{Aut}(K) \setminus \{id_K\}$, let $\mathcal{C}_\varphi := \{S \in \mathcal{C} \mid \varphi \in \pi_S((G_S)_{v_0})\}$. In other words, $\mathcal{C}_\varphi$ consists of the connection sets S such that $(G_S)_{v_0}$ contains an element acting by conjugation on K as the automorphism φ. With this new setting,

$$\mathcal{C} \subseteq \bigcup_{\varphi \in \mathrm{Aut}(K) \setminus \{id_K\}} \mathcal{C}_\varphi.$$

Since $|(G_S)_{v_0}|$ is odd, then $\varphi \in \pi_S((G_S)_{v_0})$ has odd order. Using this and applying Theorem 4.0.12 to the group K, we deduce that

$$|\{S \cap K \mid S \in \mathcal{C}_\varphi\}| \leq 2^{\mathbf{c}(K) - \frac{|K|}{96}},$$

for every $\varphi \in \mathrm{Aut}(K) \setminus \{id_K\}$. In particular, as $|K| = |R|/2$, we have

$$|\mathcal{C}_\varphi| \leq 2^{\mathbf{c}(K) - \frac{|K|}{96}} \cdot 2^{\mathbf{c}(R \setminus K)} = 2^{\frac{|K| + |I(K)|}{2} - \frac{|R|}{192} + \frac{|R \setminus K| + |I(R \setminus K)|}{2}} \leq 2^{\frac{|R| + |I(R)|}{2} - \frac{|R|}{192}} = 2^{\mathbf{c}(R) - \frac{|R|}{192}}.$$

Since $|\mathrm{Aut}(K)| \leq 2^{(\log_2 |K|)^2}$, we deduce

$$|\mathcal{C}| \leq 2^{\mathbf{c}(R) - \frac{|R|}{192} + (\log_2 |R|)^2}.$$

Let $S \in \mathcal{C}'$ and let η_S be a generator of $(G_S)_{v_0}$: recall that $(G_S)_{v_0}$ is a cyclic group of order p_S, where p_S is an odd prime number. Suppose that η_S fixes some vertex $x \in R \setminus K$. Then $x^{\eta_S} = x$, that is, $v_0^{x\eta_S} = v_0^x$. This yields $x\eta_S x^{-1} \in (G_S)_{v_0}$ and $x \in \mathbf{N}_{G_S}((G_S)_{v_0})$. Since $(G_S)_{v_0}$ centralizes K, we get $\langle K, x, (G_S)_{v_0} \rangle \leq \mathbf{N}_{G_S}((G_S)_{v_0})$. As $G_S = \langle K, x, (G_S)_{v_0} \rangle$, we deduce $(G_S)_{v_0} \trianglelefteq G_S$, which is a contradiction because $(G_S)_{v_0}$ is core-free in G_S. Therefore, η_S fixes no vertex in $R \setminus K$. Fix $x \in R \setminus K$. Then $x^{\eta_S} = xk$, for some $k \in K \setminus \{1\}$. Observe that, for each $k' \in K$, the image of xk' under η_S is uniquely determined because

$$(xk')^{\eta_S} = x^{k'\eta_S} = x^{\eta_S k'} = (x^{\eta_S})^{k'} = (xk)^k = xkk'.$$

Applying this equality with $k' = k$, we deduce $o(k) = p_S$ and hence $k \in N$, because R/N is an elementary abelian 2-group. This shows that the mapping η_S is uniquely determined by the image of one fixed element $x \in R \setminus K$, which has to be of the form xk for some $k \in N$. Thus we have at most $|N|$ choices for η_S. Once that η_S is fixed, we have at most $2^{|R|/2p_S} \leq 2^{|R|/6}$ choices for an η_S-invariant subset of $R \setminus K$. We deduce

$$|\mathcal{C}'| \leq 2^{\mathbf{c}(K)} \cdot |N| \cdot 2^{\frac{|R|}{6}} \leq 2^{\mathbf{c}(R) - \frac{|R|}{12} + \log_2 |N|} \leq 2^{\mathbf{c}(R) - \frac{|R|}{192} + (\log_2 |R|)^2 + 1}. \quad \square$$

We end this section by pulling together the above results. We are able to show that for all but a small number of connection sets, every connection set S for every group R containing a nontrivial proper normal subgroup N is covered in one of the previous two results. However, we may have to substitute a larger normal subgroup $K > N$ of R for N, which may mean that the bound we achieve is not useful. These situations can be covered by the results from Section 4.2.

Proof of Theorem 4.0.5. We use the notation established in Section 4.3.1. Let

$$\mathcal{S} := \{S \subseteq R \mid S = S^{-1}, \exists f \in \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(N) \text{ with } f \neq 1 \text{ and } 1^f = 1, f \text{ fixes each } N\text{-orbit setwise}\}.$$

Observe that, for every $S \in \mathcal{S}$, we have $(B_S)_{v_0} \neq 1$. We divide the set $\mathcal{S}$ futher:

$$\begin{aligned}
\mathcal{S}_1 :=&\{S \in \mathcal{S} \mid && R < \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)\},\\
\mathcal{S}_2 :=&\{S \in \mathcal{S} \setminus \mathcal{S}_1 \mid && \exists i \in \{2,\dots,b\} \text{ with } o(i) \text{ odd such that}\\
& && (F_S)_{v_0} \text{ has a nontrivial orbit on } \mathcal{O}_i\},\\
\mathcal{S}_3 :=&\{S \in \mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2) \mid && R/N \text{ not an elementary abelian 2-group},\\
& && \exists i \in \{2,\dots,b\} \text{ such that } (F_S)_{v_0} \text{ has}\\
& && \text{an orbit of cardinality at least 3 on } \mathcal{O}_i\},\\
\mathcal{S}_4 :=&\{S \in \mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3) \mid && R/N \text{ is an elementary abelian 2-group}, (B_S)_{v_0} \neq 1\},\\
\mathcal{S}_5 :=&\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2 \cup \mathcal{S}_3 \cup \mathcal{S}_4).
\end{aligned}$$

From Proposition 4.0.13, Lemma 4.3.5 and Lemma 4.3.6, we have explicit bounds for $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$ and $\mathcal{S}_4$, and hence we may consider only the set $\mathcal{S}_5$.

Let $S \in \mathcal{S}_5$. Since $S \notin \mathcal{S}_4$, R/N is not an elementary abelian 2-group. Since $S \notin \mathcal{S}_3$, $(F_S)_{v_0}$ has orbits of cardinality at most 2, and so does $(B_S)_{v_0}$. Therefore, $(F_S)_{v_0}$ and $(B_S)_{v_0}$ are elementary abelian 2-groups.

Now let $L_S = \{\gamma_j : (F_S)_{v_0} \text{ is trivial on } \mathcal{O}_j\}$. Notice that L_S is in fact a group. Since $(F_S)_{v_0}$ is nontrivial, then L_S is a proper subgroup of R. Since $S \notin \mathcal{S}_2$, $\gamma_i \in L_S$ for every i with $o(i)$ odd. Therefore NL_S contains all elements of R of odd order. Let

$$K := \bigcap_{g \in RB_S} (NL_S)^g$$

be the core of NL_S in RB_S. Since all conjugates of NL_S in R also contain all elements of R of odd order, we deduce that K also contains all elements of R of odd order and hence R/K is a 2-group. As $(B_S)_{v_0}$ is also a 2-group, we obtain that RB_S/K is a 2-group. Therefore $\mathbf{N}_{RB_S/K}(R/K) > R/K$. However, this implies that $\mathbf{N}_{RB_S}(R) > R$, but this contradicts the fact that $S \notin \mathcal{S}_1$. This shows that $\mathcal{S}_5 = \varnothing$. Now, adding the bounds produced for $\mathcal{S}_i$ for each $1 \leq i \leq 4$, we get the result. Indeed, using the first bound in Lemma 4.3.5 and the fact that $|R| \geq 2|N| \geq 4$, we get

$$|\mathcal{S}_2| \leq 2^{\mathbf{c}(R) - \frac{|R|}{192|N|} + \log_2|R| + \log_2|N| - 1} \leq 2^{\mathbf{c}(R) - \frac{|R|}{192|N|} + (\log_2|R|)^2 - 2}.$$

Further, if $|R| < 8$, then $|R| \neq 7$ (because N is a nontrivial proper subgroup), that is $|R| \leq 6$. Consequently,

$$\log_2(|R||N|^2/6) \leq 2\log_2|R| - 2 \leq (\log_2|R|)^2 - 2.$$

If $|R| \geq 8$, then

$$\log_2(|R||N|^2/6) \leq \log_2|R| + 2\log_2|N| \leq 3\log_2|R| - 2 \leq (\log_2|R|)^2 - 2.$$

Using these, and the second bound in Lemma 4.3.5 we get

$$|\mathcal{S}_3| \leq 2^{\mathbf{c}(R) - \frac{|R|}{192|N|} + \log_2(|R||N|^2/6)} \leq 2^{\mathbf{c}(R) - \frac{|R|}{192|N|} + (\log_2|R|)^2 - 2}.$$

This together with Proposition 4.0.13, and Lemma 4.3.6, yields

$$|\mathcal{S}| \leq 2^{\mathbf{c}(R)-\frac{|R|}{192|N|}+(\log_2|R|)^2}(1+2^{-2}+2^{-2}+2^2) \leq 2^{\mathbf{c}(R)-\frac{|R|}{192|N|}+(\log_2|R|)^2+3},$$

as required.

As in the proof of Theorem 4.0.4, we do not need to include the bound from Proposition 4.0.13 if we include the condition $R = \mathbf{N}_{\mathrm{Aut}(\Gamma(R,S))}(R)$. If we omit this condition, then we include this extra piece (which does not affect the overall bound as we have stated it) but must not allow groups that are either abelian of exponent greater than 2, or generalised dicyclic. □

Chapter A

Appendix

A.1 Quantitative version of Borel-Cantelli Lemma

Let P be a set with a positive, countable-additive measure μ such that $\mu(P) = 1$. Denoting with $(X_n)_{n\in\mathbb{N}}$ a sequence of events, we say that the events are pairwise independent if $\mu(X_i \cap X_j) = \mu(X_i)\mu(X_j)$ for every $i \neq j$. Fix the notations

$$p_k := \mu(X_k), \quad X_k^c := P \setminus X_k.$$

Theorem A.1.1 (Borel-Cantelli Lemma)**.** *Let $(X_k)_{k\in\mathbb{N}}$ be a sequence of events.*

1. *If $\sum_{1\leq k\leq\infty} p_k$ is convergent, then*
$$\mu\left(\bigcap_{k\in\mathbb{N}}\left(\bigcup_{k\leq n\leq\infty} X_n\right)\right) = 0.$$
2. *Assume that the events X_k are pairwise independent. If the series $\sum_{1\leq k\leq\infty} p_k$ is divergent, then*
$$\mu\left(\bigcap_{k\in\mathbb{N}}\left(\bigcup_{k\leq n\leq\infty} X_n\right)\right) = 1.$$

See [97, Propositions 16.4.1, 16.4.2] for a proof of Lemma A.1.1. A slightly stronger form is proved in [142, Chapter VII §5]. We want to show that, for any $n \in \mathbb{N}$, the following holds.

Lemma A.1.2 (Quantitative version of Borel-Cantelli Lemma)**.** *Let $(X_k)_{k\in\mathbb{N}}$ be a sequence of pairwise independent events. Then*

$$\mu\left(\bigcap_{1\leq k\leq n} X_k^c\right) \leq \frac{1}{\sum_{1\leq k\leq n} p_k} \tag{A.1.1}$$

The proof need some preliminaries. For any $n \in \mathbb{N}$, let $\alpha_n : P \to \{0, 1\}$ be the characteristic function of X_n, that is,

$$\alpha_n(x) := \begin{cases} 1, & \text{if } x \in X_n \\ 0, & \text{otherwise.} \end{cases}$$

Note that, α_n is a measurable function on P, and $p_n = \mu(X_n) = \int_P \alpha_n$. Define

$$F_n(x) := \sum_{1\leq k\leq n} (\alpha_k(x) - p_k).$$

The expectation of this random variable is $E(F_n) = 0$.

Lemma A.1.3. [97, Lemma 16.4.3] *For each n, the variance of F_n can be computed as follows:*

$$var(F_n) = \sum_{1\leq k\leq n} p_k(1-p_k) \leq \sum_{1\leq k\leq n} p_k.$$

Observe that, the proof of Lemma A.1.3 required the pairwise independency of the sequence of events $\{X_k\}_{k\in\mathbb{N}}$.

Lemma A.1.4 (Chebyshef's inequality, [97, Lemma 16.4.4])**.** *Let f be a measurable function on P. For $\lambda > 1$ put*

$$B_\lambda = \left\{x \in P \ : (f(x) - E(f))^2 > \lambda \cdot var(f)\right\}.$$

Then

$$\mu(B_\lambda) \leq 1/\lambda.$$

Proof of Theorem A.1.2. We may suppose $\sum_{1\leq k\leq n} p_k > 1$ (otherwise the inequality is trivial). For each n, define

$$Y_n := \{x \in P \mid F_n(x) < -\varepsilon \cdot \sum_{1\leq k\leq n} p_k\}, \quad \text{with} \quad 0 < \varepsilon < 1.$$

For every $x \in Y_n$, we get that

$$(F_n(x) - E(F_n))^2 > \varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right)^2 = \lambda \cdot var(F_n),$$

where

$$\lambda = \frac{\varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right)^2}{var(F_n)} \geq \varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right).$$

(Note that the inequality above follows form Lemma A.1.3.)

We know that $\sum_{1\leq k\leq n} p_k > 1$, thus $\sum_{1\leq k\leq n} p_k > 1+\delta$, for some $\delta > 0$. Taking $\varepsilon^* = \frac{1}{\sqrt{(1+\delta)}}$, for every $\varepsilon \in (\varepsilon^*, 1)$, we get that

$$\varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right) > 1.$$

Hence, form Lemma A.1.4, with $f = F_n$, we deduce that

$$\mu(Y_n) \leq \frac{1}{\varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right)}.$$

However, for every $x \in \bigcap_{1\leq k\leq n} X_k^c$, we have that

$$F_n(x) = -\sum_{1\leq k\leq n} p_k < -\varepsilon \cdot \sum_{1\leq k\leq n} p_k.$$

Therefore,

$$\mu(\bigcap_{1\leq k\leq n} X_k^c) \leq \mu(Y_n) \leq \frac{1}{\varepsilon^2 \cdot \left(\sum_{1\leq k\leq n} p_k\right)}.$$

Taking the limit as ε go to 1 we get (A.1.2). □

Glossary

In this section, we list some definitions and notations used throughout the thesis. First, we list some symbols or acronyms and juxtapose the description. Then the other lists are organized as follow: we have what should be defined on the left, a definition on the middle and the symbol or the acronym (if necessary) on the right. If we do not say differently, in what follows G will be an abstract group.

Symbol or Acronym	Description
CFSG	Classification of finite simple group.
PFG	Positively finitely generated.
$\mathbf{c}(G)$	The number of inverse-closed subsets of G
$\mathbf{C}_G(\varphi)$	$\{x \in G \mid x^\varphi = x\}$, where φ is an automorphism of G.
$d(G)$	The minimal size of a generating set of a finitely generated group G.
$d_p(G)$	The minimal number of generators of a Sylow p-subgroup of a finite group G.
$e(G)$	The expected number of elements of a (pro)finite group G which have to be drawn at random, with replacement, before a set of generators is found.
$e_{\mathcal{T}}(G)$	The expected number of elements of a permutation group $G \leq \mathrm{Sym}(n)$ which have to be drawn at random, with replacement, before a set of generators of a transitive subgroup of G is found.
$\mathbf{F}^*(G)$	Generalized Fitting subgroup of G
$\log x$	Logarithm in base 2 of x.
$\log_a x$	Logarithm in base a of x.
$m(G)$	the largest size of a minimal generating set of G.
$m(G, N)$	$m(G) - m(G/N)$ where N is a normal subgroup of a finite group G.

Symbol or Acronym	Description
$m_n(G)$	number of maximal subgroups of index n in G.
$\max(H, G)$	$\lvert\{M \mid M \text{ maximal subgroup of } G \text{ with } H \leq M\}\rvert$, where H is a subgroup of a finite group G.
$\mathcal{M}(G)$	$\sup_{n\geq 2} \log_n m_n(G)$.
$\mathcal{M}_G(H)$	The set of maximal members of $\mathcal{O}_G(H)''$.
$\mathcal{O}_G(H)'$	$\mathcal{O}_G(H)\setminus\{H, G\}$, where H is a subgroup of a finite group G.
$\mathcal{O}_G(H)''$	$\{M \in \mathcal{O}_G(H) \mid \mathbf{F}^*(G) \not\leq M\}$, where H is a subgroup of a finite group G.
$o(x)$ or $\lvert x\rvert$	The order of the element x in G
$\mathcal{P}(X)$	$\{Y \mid Y \subseteq X\}$, for some set X.
$P_G(k)$	Probability that k randomly chosen elements of a (pro)finite group G generate G.
$\mathrm{P}_{\mathcal{T}}(G, k)$	Probability that k randomly chosen elements of a permutation group $G \leq \mathrm{Sym}(n)$ generate a transitive subgroup of G.
$\delta(G)$	$\sum_{p\in\pi(G)} d_p(G)$.
$\delta_G(A)$	The number of non-Frattini chief factors G-equivalent to A in any chief series of G.
$\chi(G)$	$\chi(1, G)$.
$\nu(G)$	$\min\{k \in \mathbb{N} \mid P_G(k) \geq 1/e\}$, where e is the Nepero number
$\pi(G)$	The set of prime divisors of the order of a finite group G.
$\tilde{\pi}(r)$	The number of distinct prime divisors of r.
$\pi(x)$	The number of prime numbers less than or equal to x.
$\hat{0}$	The minimum of a (finite) lattice L.
$\hat{1}$	The maximum of a (finite) lattice L.

	Definition	Notation
(a,b)- **regular partition**	A partition Σ ofa set Ω is an (a,b)-regular partition when it consists of b parts each having cardinality a.	
Atom of a lattice	An atom of a finite lattice L is an element $t \in L$ covering $\hat{0}$, that is $\hat{0} \leq t$ and $[\hat{0}, t] = \{\hat{0}, t\}$.	
Base	A subset $\mathcal{B}$ of Ω is a base for a permutation group $G \leq \mathrm{Sym}(\Omega)$ if the pointwise stabilizer $G_{(\mathcal{B})}$ is trivial.	
Base size	The base size a permutation group $G \leq \mathrm{Sym}(\Omega)$ is the minimal cardinality of a base for G	$b(G,\Omega)$ or $b(G)$ when Ω is clear
Block of imprimitivity	A block of imprimitivity of a transitive group $G \leq \mathrm{Sym}(\Omega)$ is a non-empty subset B of Ω such that, for every $g \in G$, either $B \cap B^g = \varnothing$ or $B = B^g$.	
Block system or **System of imprimitivity**	Let B be a block of of a transitive group $G \leq \mathrm{Sym}(\Omega)$, the set $\{B^g \mid g \in G\}$ is a block system	
Boolean lattice	A lattice $\mathcal{L}$ is said to be Boolean if $\mathcal{L}$ is isomorphic to the lattice of subsets of a set X, that is, $\mathcal{L} \cong \mathcal{P}(X)$.	
BN-pair	A BN-pair in G is a pair (B,N) of subgroups of G such that 1. B and N generates G and $H := N \cap B$ is normal in N, 2. The group $W = N/H = \langle S \rangle$ where all the elements of S have order 2, 3. For every $s \in S$ and $w \in W$, then sBw is contained in the union of $BswB$ and BwB, 4. No generator s normalizes B.	
Centralizer	If A is a G-group the centralizer of A in G is $\{g \in G \mid a^g = a\,, \forall a \in A\}$.	$C_G(A)$
Coatom of a lattice	A coatom of a finite lattice L is an element $s \in L$ that $\hat{1}$ covers, that is $s \leq \hat{1}$ and $[s, \hat{1}] = \{s, \hat{1}\}$.	
Complemented lattice	A lattice L with $\hat{0}$ and $\hat{1}$ is complemented if for all $s \in L$ there is a $t \in L$ such that $s \wedge t = \hat{0}$ and $s \vee t = \hat{1}$.	

	Definition	Notation
Cayley digraph and Cayley graph	Let R be a group and let S be a subset of R. The Cayley digraph with connection set S, is the digraph (V, E) with with $V = R$ and $\{r, t\} \in E$ if and only if $tr^{-1} \in S$. When $S = S^{-1}$ is an inverse-closed subset of R, then (V, E) is the Cayley graph with connection set S.	$\Gamma(R, S)$
Chief factor	A chief factor of a finite group G is a quotient H/K where K is a normal subgroup of G and H/K is a minimal normal subgroup of G/K.	
Complemented chief factor	A chief factor X/Y of G is complemented if there exists a subgroup U, called complement, such that $G = UX$ and $Y = U \cap X$.	
Core	The core of a subgroup M of G is the group $\cap_{g \in G} g^{-1} M g$. This is the largest subgroup of M that is normal in G.	$\mathrm{core}_G(M)$ or M_G
Crown	Let A be a non-Frattini chief factor of G, $\mathcal{N}_A := \{N \lhd G \mid G/N \cong L_A \text{ and } \mathrm{soc}(G/N) \sim_G A\}$ and let $R_G(A) := \bigcap_{N \in \mathcal{N}_A} N$. Then $G/R_G(A)$ is isomorphic to the crown-based power $(L_A)_{\delta_G(A)}$. The *A-crown* of G is the socle of $G/R_G(A)$.	$I_G(A)/R_G(A)$
Crown-based power	The crown-based power of G of size k is the subgroup of the group G^k defined by $\{(l_1, \ldots, l_k) \in G^k \mid l_1 \equiv \cdots \equiv l_k (mod\, \mathrm{soc}(G))\}$.	G_k
d-generated group	A d-generated group is a finitely generated group G such that $d(G) \leq d$	
Distributive lattice	A lattice L is distributive lattices when the distributive laws are satified. That is, for all $s, t, u \in L$, the following are verified $s \vee (t \wedge u) = (s \vee t) \wedge (s \vee u)$ $s \wedge (t \vee u) = (s \wedge t) \vee (s \wedge u)$. (Either of these laws implies the other.)	
Dicyclic or generalised quaternion group	A group is called dicyclic or generalised quaternion group if it is isomorphic to some $\mathrm{Dic}(A, y, x)$ with A a cyclic group	

	Definition	Notation
Dual Euler totient of H in G	For a subgroup H of G, the dual Euler totient of H in G is defined as follows: $$\sum_{K \in \mathcal{O}_G(H)} \mu(H,K)\lvert G:K\rvert.$$	$\hat{\varphi}(H,G)$
Euler totient of G	Let G be a finite group, the Euler totient of G is the number of elements g such that $\langle g \rangle = G$.	$\varphi(G)$
Euler totient of H in G	For a subgroup H of G, the Euler totient of H in G is the number of cosets Hg such that $\langle Hg \rangle = G$.	$\varphi(H,G)$
Fixed-points-free permutation	A permutation $g \in G \leq \mathrm{Sym}(\Omega)$ with no fixed points.	
Fixed points set of a permutation	The set of points in Ω fixed by $g \in G \leq \mathrm{Sym}(\Omega)$.	$\mathrm{fix}_\Omega(g)$
Frattini chief factor	A Frattini chief factor of G if is a chief factor X/Y contained in the Frattini subgroup of G/Y	
Frattini subgroup	The Frattini subgroup of G is the intersection of all the maximal subgroups of G	$\mathrm{Frat}(G)$
G-group	A *G-group* is a group A together with a group homomorphism $\theta : G \to \mathrm{Aut}(A)$.	
G-isomorphic groups	Two G-groups A and B are said to be G-somorphic if there exists an isomorphism $\varphi : A \to B$ such that $(a^g)^\varphi = (a^\varphi)^g$, for every $a \in A$ and for every $g \in G$.	$A \cong_G B$
G-isomorphic groups	Two G-groups A and B are G-equivalent if there exist two isomorphisms $\varphi : A \to B$ and $\Phi : A \rtimes G \to B \rtimes G$ such that the following diagram commutes. $$\begin{array}{ccccccccc} 1 & \hookrightarrow & A & \hookrightarrow & A \rtimes G & \twoheadrightarrow & G & \twoheadrightarrow & 1 \\ & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \Phi} & & \| & & \\ 1 & \hookrightarrow & B & \hookrightarrow & B \rtimes G & \twoheadrightarrow & G & \twoheadrightarrow & 1 \end{array}$$	$A \sim_G B$,
Generalised dicyclic group	Let A be an abelian group of even order and of exponent greater than 2, and let y be an involution of A. The generalised dicyclic group is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A \rangle$. A group is called generalised dicyclic if it is isomorphic to some $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A \rangle$.	$\mathrm{Dic}(A,y,x)$
Generating set and generators	We say that a subset X of G is a generating set for G if every element of G can be express as a product of elements of $X \cup X^{-1}$. The elements of X are called generators	$G = \langle X \rangle$

	Definition	Notation
Graph (Digraph)	A graph (digraph) Γ is an ordered pair (V, E) with V a finite non-empty set of vertices, and E a set of unordered (ordered) pairs from V, representing the edges.	
Graph (Digraph) automorphism	An automorphism of a graph (digraph) (V, E) is a permutation on V that preserves the set E.	
Graphical (Digraphical) regular representation	A graphical (digraphical) regular representation for a group R is a graph (digraphical) whose full automorphism group is the group R acting regularly on the vertices of the graph.	GRR (DRR)
Group-complemented boolean lattice	A lattice L is called group-complemented if $ss^{\complement} = s^{\complement}s$ for every $s \in L$.	
Imprimitive group	A transitive permutation group $G \leq \mathrm{Sym}(\Omega)$ is imprimitive if it admit a non-trivial block.	
Intervals of a poset	An interval with extremes $s, t \in P$ of a poset $(P, \leq)$ is the set $\{u \in P \mid s \leq u \leq t\}$	$[s, t]$
Irreducible G-group	A G-group A is said to be irreducible if G leaves invariant no non-identity proper normal subgroup of A.	
Large base permutation group	The permutation group G is large base if there exist integers m and $r \geq 1$ such that $\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \mathrm{wr} \mathrm{Sym}(r)$, where the action of $\mathrm{Sym}(m)$ is on k-element subsets of $\{1, \ldots, m\}$	
Lattice-complement	A lattice-complement of a element s in complemented lattice L is an element $t \in L$ such that $s \vee t = \hat{1}$ and $s \wedge t = \hat{0}$	$s^{\complement}$
Maximal system of imprimitivity	A system of imprimitivity Σ of a transitive group $G \leq \mathrm{Sym}(\Omega)$ is maximal if the induced permutation group $G^{\Sigma} \leq \mathrm{Sym}(\Sigma)$ is primitive.	
Minimal or Independent generating set	A generating set X of a group G is said to be minimal if no proper subset of X generates G.	
Möbius function on a poset	Let $\Lambda = (X, \leq)$ be a finite poset. The Möbius function on the poset Λ is the unique function $\mu_\Lambda : X \times X \to \mathbb{Z}$, satisfying $\mu(x, y) = 0$ unless $x \leq y$ and the recursion formula $$\sum_{x \leq y \leq z} \mu_\Lambda(y, z) = \begin{cases} 1 & \text{if } x = z, \\ 0 & \text{otherwise.} \end{cases}$$	μ_Λ
Orbit	Let $G \leq \mathrm{Sym}(\Omega)$. The orbit of $\omega \in \Omega$ is the set $\{\omega^g \mid g \in G\}$	ω^G
Overgroup lattice	The overgroup lattice of a subgroup H of G is the set of subgroups of G containing H	$\mathcal{O}_G(H)$

	Definition	Notation
Open intervals of a poset	An open interval with extremes $s,t \in P$ of a poset $(P,\leq)$ is the set $\{u \in P \mid s < u < t\}$	(s,t)
Normalizer	The normalizer of a subgroup H of G is the set $\{g \in G \mid g^{-1}Hg = H\}$	$\mathbf{N}_G(H)$
Partial order in the set of all regular product structures	Let $\mathcal{F} := \{\Omega_i \mid i \in I\}$ and $\tilde{\mathcal{F}} := \{\tilde{\Omega}_j \mid j \in \tilde{I}\}$ be regular (m,k)- and $(\tilde{m},\tilde{k})$-product structures on Ω, respectively. Set $I := \{1,\ldots,k\}$ and $\tilde{I} := \{1,\ldots,\tilde{k}\}$, and define $\mathcal{F} \leq \tilde{\mathcal{F}}$ if there exists a positive integer s with $\tilde{k} = ks$, and a regular (s,k)-partition $\Sigma = \{\sigma_i \mid i \in I\}$ of $\tilde{I}$, such that for each $i \in I$ and each $j \in \sigma_i$, $\tilde{\Omega}_j \leq \Omega_i$, that is, the partition Ω_i is a refinement of the partition $\tilde{\Omega}_j$.	
Primitive group	An abstract group G is said to be primitive if it has a maximal subgroup with trivial core. A transitive permutation group $G \leq \mathrm{Sym}(\Omega)$ is primitive if it admits only the trivial blocks. Note that the two definition are equivalent.	
Primitive monolithic group	A primitive group G is said to be monolithic if $\mathrm{soc}(L)$ is a minimal normal subgroup of G. G is of type I when $\mathrm{soc}(L)$ is abelian G is of type II when $\mathrm{soc}(L)$ is nonabelian	
Primitive monolithic group associated to a chief factor	The monolithic primitive group associated to the chief factor A of G is defined $A \rtimes (G/C_G(A))$ when A is abelian or $G/C_G(A)$ otherwise.	L_A
Pointwise stabilizer	The pointwise stabilizer in $G \leq \mathrm{Sym}(\Omega)$ of $\Gamma \subseteq \Omega$ is the subgroup of G consisting of the elements $g \in G$ for which $\gamma^g = \gamma$ for any $\gamma \in \Gamma$.	$G_{(\Gamma)}$
Rank of a Boolean lattice	The rank of a Boolean lattice $\mathcal{L} \cong \mathcal{P}(X)$ is the size of X	
Reduced Euler characteristic H in G	For a subgroup H of G, the reduced Euler characteristic H in G is defined as follows: $$-\sum_{K \in \mathcal{O}_G(H)} \mu(K,G)\lvert G:K\rvert.$$	$\chi(H,G)$

	Definition	Notation
Regular (m,k)-product structure	A regular (m,k)-product structure on Ω is a bijection $f : \Omega \to \Gamma^I$, where $I := \{1,\ldots,k\}$ and Γ is an m-set. The function f consists of a family of functions $(f_i : \Omega \to \Gamma \mid i \in I)$ where $f(\omega) = (f_1(\omega),\ldots,f_k(\omega))$, for each $\omega \in \Omega$. The following is an equivalent definition. Let $\mathcal{F} := \{\Omega_i \mid i \in I\}$ be a set of partitions Ω_i of Ω into m blocks of size m^{k-1}, let $[\omega]_i$ be the block of Ω_i containing the point ω, and let $\mathcal{F}(\omega) := \{[\omega]_i \mid i \in I\}$. The set $\mathcal{F}$ is a product structure if, for each pair of distinct points $\omega,\omega' \in \Omega$, we have $\mathcal{F}(\omega) \neq \mathcal{F}(\omega')$.	
Regular orbit	A regular orbit of $G \leq \mathrm{Sym}(\Omega)$ is a orbit having a point ω such that $G_\omega = 1$	
Refinement of a partition	A refinement of a partition Σ_1 of a set Ω is a partition Σ_2 of Ω such that every element in Σ_1 is a union of elements in Σ_2.	$\Sigma_1 \leq \Sigma_2$
Regular or uniform partition	A partition Σ of a set Ω is said to be regular or uniform if all parts in Σ have the same cardinality.	
Semi-direct product	Given a G-group A, we have the corresponding semi-direct product where the multiplication is given by $g_1a_1 \cdot g_2a_2 = g_1g_2a_1^{g_2}a_2$, for every $a_1,a_2 \in A$ and for every $g_1,g_2 \in G$.	$A \rtimes_\theta G$ $A \rtimes G$ when θ is clear
Setwise stabilizer	The setwise stabilizer in $G \leq \mathrm{Sym}(\Omega)$ of $\Gamma \subseteq \Omega$ is the subgroup of G consisting of the elements $g \in G$ for which $\gamma^g \in \Gamma$ for every $\gamma \in \Gamma$.	G_Γ or $\mathbf{N}_G(\Gamma)$
Socle	The socle of a group G is the subgroup generated by the minimal normal subgroups.	$\mathrm{soc}(G)$
Stabilizer or point stabilizer	Let $G \leq \mathrm{Sym}(\Omega)$. The stabiliser of $\omega \in \Omega$ the subgroup of G consisting of those elements that fix ω.	G_ω
Stabilizer of a partition	Let Σ be a partition of a set Ω. The stabilizer of the partition Σ consisting of the elements $g \in G$ for which $\Gamma^g \in \Sigma$ for every part Γ of Σ.	$\mathbf{N}_G(\Sigma)$
Stabilizer of a regular (m,k)-product structure	Let $\mathcal{F} = \{\Omega_1,\ldots,\Omega_k\}$ be a (m,k)-product structure on Ω. The stabilizer of $\mathcal{F}$ consisting of the elements $g \in G$ for which $\Omega_i^g \in \mathcal{F}$, for every $i \in \{1,\ldots,k\}$.	$\mathbf{N}_G(\mathcal{F})$
(strongly) extendible generating set	An extendible generating set of a finite group G is a minimal generating set having a (strong) immediate descendant	

	Definition	Notation
(strong) immediate descendant of a generating set	An extendible generating set of a finite group G is a minimal generating set $\omega := \{g_1, \ldots, g_k\}$ for which there exist $1 \leq i \leq k$ and x_1, x_2 in G such that $\tilde{\omega} = \{g_1, \ldots, g_{i-1}, x_1, x_2, g_{i+1}, \ldots, g_k\}$ is a minimal generating set of G. If $g_i = x_1 x_2$, then we say that $\tilde{\omega}$ is a strong immediate descendant of ω.	
(strong) descendant of a generating set	A minimal generating set ω^* of cardinality t (with $t > k$) is a (strong) descendant of ω if there exists a sequence $\omega_0, \omega_1, \ldots, \omega_{t-k}$ where $\omega_0 = \omega$, $\omega^* = \omega_{t-k}$ and ω_j is a (strong) immediate descendant of ω_{j-1} for every $1 \leq j \leq t-k$.	
(strongly) totally extendible generating set	A (strongly) totally extendible extendible generating set of a finite group G is a minimal generating set having a (strong) descendant $m(G)$.	
Transitive group	An abstract group G is said to be transitive if it admits a subgroup with trivial core. A permutation group $G \leq \mathrm{Sym}(\Omega)$ is transitive if $\omega^G = \Omega$, for any $\omega \in \Omega$. Note that the two definition are equivalent.	
Trivial blocks	The singleton $\{\omega\} \subseteq \Omega$ and the whole Ω are the trivial blocks of every transitive group $G \leq \mathrm{Sym}(\Omega)$.	
Trivial partitions	A partition Σ of Ω is said to be trivial if $\Sigma = \{\Omega\}$ or if $\Sigma = \{\{\omega\} \mid \omega \in \Omega\}$.	
Wreath product	Let $H \leq \mathrm{Sym}(\Gamma)$ and $K \leq \mathrm{Sym}(n)$ be permutation groups with $\lvert\Gamma\rvert, n \geq 2$. Let H^n be the direct product of n copies of H. The group K acts on H^n by permuting the coordinates. Specifically $\pi \in K$ acts on H^n by setting: $$(x_1, \ldots, x_n)^\pi = (x_{1^{\pi^{-1}}}, \ldots, x_{n^{\pi^{-1}}}).$$ The wreath product of H and K is the corresponding semidirect product $H^n K$, so the group operation is defined as follows: $$(a_1, \ldots, a_n)\sigma \cdot (b_1, \ldots, b_n)\tau = (a_1 b_{1^\sigma}, \ldots, a_n b_{n^\sigma})\sigma\tau$$ The direct product H^n is the base group and K is the top group of the wreath product	$H \mathrm{wr} K$ or $H \wr K$

Bibliography

[1] P. Apisa and B. Klopsch, A generalization of the Burnside basis theorem, *J. Algebra* **400** (2014), 8–16.

[2] J. Araújo and P. J. Cameron, Primitive groups, road closures, and idempotent generation, arXiv:1611.08233

[3] J. Araújo, P. J. Cameron, B. Steinberg, Between primitive and 2-transitive: Synchronization and its frineds, *EMS Surv. Math. Sci.* **4** (2017), 101–184.

[4] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984) 469–514.

[5] M. Aschbacher, Overgroups of primitive groups, *J. Aust. Math. Soc.* **87** (2009), 37–82.

[6] M. Aschbacher, Overgroups of primitive groups II, *J. Algebra* **322** (2009), 1586–1626.

[7] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, *J. Algebra* **90** (1984), 446–460.

[8] M. Aschbacher, J. Shareshian, Restrictions on the structure of subgroup lattices of finite alternating and symmetric groups, *J. Algebra* **322** (2009), 2449–2463.

[9] L. Babai, Finite digraphs with given regular automorphism groups, *Periodica Mathematica Hungarica* **11** (1980), 257–270.

[10] L. Babai, C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15.

[11] A. Ballester-Bolinches and L. M. Ezquerro, *Classes of finite groups*, Mathematics and its Applications 584, *Springer*, Dordrecht, 2006.

[12] A. Ballester-Bolinches, R. Esteban-Romero, P. Jiménez-Seral and Hangyang Meng, Bounds on the number of maximal subgroups with applications to random generation of finite groups, preprint.

[13] M. Balodi, S. Palcoux, On Boolean intervals of finite groups, *J. Comb. Theory, Ser. A*, **157** (2018), 49–69.

[14] A. Basile, *Second maximal subgroups of the finite alternating and symmetric groups*, PhD thesis, Australian National Univ., 2001.

[15] C. Benbenishty, On actions of primitive groups, PhD thesis, Hebrew University, Jerusalem, 2005.

[16] C. Benbenishty, J. A. Cohen, A. C. Niemeyer, The minimum length of a base for the symmetric group acting on partitions, *European Journal of Combinatorics* **28** (2007), 1575—1581.

[17] A. Bochert, Uber die Zahl verschiedener Werte, die eine Funktion gegebener Buchstaben durch Vertauschung derselben erlangen kann, *Math. Ann.* **33** (1889), 584–590.

[18] A.V. Borovik, L. Pyber and A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. AMS* **348** (1996), 3745–3761.

[19] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[20] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal, The Maximal Subgroups of the Low-Dimensional Finite Classical Groups, London Mathematical Society Lecture Note Series, 407 (Cambridge University Press, Cambridge, 2013).

[21] K. S. Brown, The coset poset and probabilistic zeta function of a finite group, *J. Algebra* **225** (2) (2000), 989–1012.

[22] T. C. Burness, On base sizes for actions of finite classical groups, *J. Lond. Math. Soc.* (2) **75** (2007), no. 3, 545–562.

[23] T. C. Burness, Simple groups, generation and probabilistic methods, 2017, arXiv:1710.10434

[24] T. C. Burness and M. Giudici, Classical Groups, Derangements and Primes, Australian Mathematical Society Lecture Series, 25. Cambridge University Press, Cambridge (2016).

[25] T. C. Burness, R. M. Guralnick, and J. Saxl, On base sizes for symmetric groups, *Bull. Lond. Math. Soc.* **43** (2011), no. 2, 386–391.

[26] T.C. Burness, M. Liebeck, A. Shalev, Base sizes for simple groups and a conjecture of Cameron, *Proceedings of the London Mathematical Society* (3) **98** (2009), no. 1, 116–162.

[27] T.C. Burness, E. A. O'Brien, R. A. Wilson, Base sizes for sporadic simple groups, *Israel Journal of Mathematics* , **177**, (2010), 307–333.

[28] T. C. Burness, A, Seress, On Pyber's base size conjecture, *Transactions of the American Mathematical Society* **367**, no. 8, (2015), 5633–5651.

[29] S. Burris and H. P. Sankappanavar, A course in universal algebra. Graduate Texts in Mathematics, 78. *Springer-Verlag*, New York-Berlin, 1981.

[30] P. J. Cameron, https://cameroncounts.wordpress.com.

[31] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1) (1981) 1–22.

[32] P. J. Cameron, Permutation groups, *Cambridge University Press*, Cambridge,1999.

[33] P. J. Cameron, 'Some open problems on permutation groups', *Groups, combinatorics and geometry* (eds M. W. Liebeck and J. Saxl), LMS Lecture Note Series **165** (Cambridge University Press, Cambridge,1992), 340–350.

[34] P. Cameron and P. Cara, Independent generating sets and geometries for symmetric groups, *J. Algebra* **258** (2002), 641–650.

[35] P. J. Cameron and W. M. Kantor, 'Random permutations: some group-theoretic aspects', *Combin. Probab. Comput.* **2** (1993) 257–262.

[36] A. Caranti, F. Dalla Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings, *Publ. Math. Debrecen* **69** (2006), 297–308.

[37] Y. Caro, New results on the independence number, *Tech. Report, Tel-Aviv University*, 1979.

[38] H. Cohen, High precision computation of Hardy-Littlewood constants, preprint available on the author's web page.

[39] E. Crestani and A. Lucchini, d-Wise generation of prosolvable groups, J. Algebra 369 (2012), 59–69.

[40] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, An $\mathbb{ATLAS}$ of Finite Groups, *Clarendon Press, Oxford*, 1985; reprinted with corrections 2003.

[41] F. Dalla Volta and A. Lucchini, Generation of almost simple groups, *J. Algebra* **178** (1995), 194–223.

[42] I. De Las Heras, A. Lucchini, Intersections of maximal subgroups in prosolvable groups, *Comm. Algebra* **47** (2019), 3432–3441.

[43] E. Detomi and A. Lucchini, Crowns and factorization of the probabilistic zeta function of a finite group, J. Algebra, 265 (2003), no. 2, 651–668.

[44] E. Detomi, A. Lucchini and F. Morini, How many elements are needed to generate a finite group with good probability?, *Isr. J. Math.* **132** (2002), 29–44

[45] E. Detomi, A. Lucchini, M. Moscatiello, P. Spiga and G. Traustason, Groups satisfying a strong complement property, *Journal of Algebra* **535** (2019), 35–52.

[46] E. Detomi and A. Lucchini, Some generalizations of the probabilistic zeta function, *Ischia Group Theory* 2006, Ischia Group Theory 2006 World Scientific Publishing Company, Singapore, 2007, 56–72

[47] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[48] J.D. Dixon and B. Mortimer, Permutation Groups, *Springer-Verlag*, New York, 1996.

[49] E. Dobson, P. Spiga, G. Verret, Cayley graphs on abelian groups, *Combinatorica* **36** (2016), 371–393.

[50] H. Duyan, Z. Halasi and A. Maróti, A proof of Pyber's base size conjecture, *Advances in Mathematics* **331** (2018), 720–747

[51] D. Easdown and C. Praeger, On minimal faithful permutation representations of finite groups, *Bull. Austral. Math. Soc.* **38** (1988), no. 2, 207–220.

[52] J. B. Fawcett, 'The base size of a primitive diagonal group', *J. Algebra* **375** (2013), 302—321

[53] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.7 (2015). http://www.gap-system.org.

[54] D. Gluck and K. Magaard, Base sizes and regular orbits for coprime affine permutation groups, *J. London Math. Soc.* **58** (1998), 603–618.

[55] W. Gaschütz, Die Eulersche Funktion endlicher auflösbarer Gruppen, *Illinois J. Math.* **3** (1959), 469–476.

[56] W. Gaschütz, Praefrattinigruppen, *Arch. Mat.* **13** (1962), 418–426

[57] C. D. Godsil, GRRs for nonsolvable groups, *Algebraic Methods in Graph Theory,* (Szeged, 1978), 221–239, *Colloq. Math. Soc. János Bolyai* **25**, North-Holland, Amsterdam-New York, 1981.

[58] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256.

[59] S. Guest and P. Spiga, 'Finite primitive groups and regular orbits of group elements', *Trans. Amer. Math. Soc.* **369** 2 (2017), 997-–1024

[60] R. Guralnick, On the number of generators of a finite group, *Arch. Math.* **53** (1989), no. 6, 521-523.

[61] R. M. Guralnick, Subgroups of prime power index in a simple group, *J. Algebra* **81** (1983), 304–311.

[62] R. Guralnick, The dimension of the first cohomology group, in *Lecture Notes in Math.* **1178**, Springer, Berlin, 1986.

[63] R. Guralnick, T. Hodge, B. Parshall, L. Scott, Wall conjecture.

[64] P. Hall, The Eulerian functions of a group, *Q. J. Math., Oxf. Ser.*, **7** (1936), 134–151.

[65] Z. Halasi, M. W. Liebeck, A. Maróti, Base sizes of primitive groups: bounds with explicit constants, *J. of Algebra* **521** (2019) 16–43

[66] Z. Halasi, A. Maróti, The minimal base size for a p-solvable linear group, *Proc. Amer. Math. Soc.* **144** (2016), 3231–3242.

[67] M. Herzog, On finite simple groups of order divisible by three primes only, *J. Algebra* **10** (1968), 383–388.

[68] D. Hetzel, Über reguläre graphische Darstellung von auflösbaren Gruppen. Technische Universität, Berlin,1976.

[69] D. Holt, Representing quotients of permutation groups, *Quart. J. Math. Oxford Ser. (2)* **48** (1997), no. 191, 347–350.

[70] B. Huppert, Endliche Gruppen I, *Springer-Verlag*, Berlin, Heidelberg, New-York, 1967.

[71] W. Imrich, Graphen mit transitiver Automorphismengruppen, *Monatsh. Math.* **73** (1969), 341–347.

[72] W. Imrich, Graphs with transitive abelian automorphism group, *Combinat. Theory (Proc. Colloq. Balatonfüred, 1969*, Budapest, 1970, 651–656.

[73] W. Imrich, On graphs with regular groups, *J. Combinatorial Theory Ser. B.* **19** (1975), 174–180.

[74] P. Jiménez-Seral and J. Lafuente, On complemented nonabelian chief factors of a finite group, *Israel J. Math.* **106** (1998), 177–188.

[75] A. Jaikin-Zapirain and L. Pyber, Random generation of finite and profinite groups and group enumeration, *Ann. of Math.* (2) **173** (2011), no. 2, 769–814.

[76] G. A. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory* **5** (2002), 403–407.

[77] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom.Dedic.* **36** (1990), 67–87.

[78] P. J. Keen, *Independent Sets in Some Classical Groups of Dimension Three*, University of Birmingham. Ph.D. Thesis (2012).

[79] P. B. Kleidman, 'The maximal subgroups of the finite 8-dimensional orthogonal groups $\mathrm{P}\Omega_8^+(q)$ and of their automorphism groups', *J. Algebra* **110** (1987) 173–242.

[80] P. B. Kleidman and M. W. Liebeck, The subgroup structure of the finite classical groups, *LMS Lecture Note Series* **129** (Cambridge University Press, Cambridge, 1990).

[81] W. Kimmerle, R. Lyons, R. Sandling and D N. Teague, Composition Factors from the Group Ring and Artin's Theorem on Orders of Simple Groups, *Proc. London Math. Soc* **60** (1990), 89–122.

[82] L. G. Kovács and Hyo-Seob Sim, Generating finite soluble groups, *Indag. Math.* (N.S.) **2** (1991), 229–232.

[83] L. G. Kovács and C. E. Praeger, Finite permutation groups with large abelian quotients, *Pacific J. Math.* **123** (1989), 283–292.

[84] J. Lafuente, Crowns and centralizers of chief factors of finite groups, *Commun. Algebra* **13** (1985) 657–668.

[85] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc. (3)* **87** (2003), 725–747.

[86] M.W. Liebeck, On minimal degrees and base sizes of primitive permutation groups, *Arch. Math. (Basel)* **43** (1) (1984), 11–15.

[87] M.W. Liebeck, Probabilistic and asymptotic aspects of finite simple groups, in Probabilistic group theory, combinatorics, and computing, 1–34, *Lecture Notes in Math.*, 2070, Springer, London, 2013

[88] H. Liebeck and D. MacHale, Groups with Automorphisms Inverting most Elements, *Math. Z.* **124** (1972), 51–63.

[89] M.W. Liebeck and A. Shalev, Bases of primitive linear groups, *J. Algebra* **252** (2002), 95–113.

[90] M.W. Liebeck and A. Shalev, Simple groups, permutation groups, and probability, *J. Amer. Math. Soc.* **12** (1999), 497–520.

[91] M. W. Liebeck and A. Shalev, The probability of generating a finite simple group, *Geom. Dedicata* **56** (1995), 103–113.

[92] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Australian Math. Soc. (A)* **44** (1988), 389–396.

[93] 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), 365–383.

[94] M. W. Liebeck, C. E. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Mem. Am. Math. Soc.* **432** (1990)

[95] M. W. Liebeck, L. Pyber, A. Shalev, On a conjecture of G. E. Wall, *J. Algebra* **317** (2007), 184–197.

[96] A. Lubotzky, The expected number of random elements to generate a finite group, *J. Algebra* **257** (2002), 452–495.

[97] A. Lubotzky and D. Segal, Subgroup growth, Progress in Mathematics, 212. Birkhäuser Verlag, Basel (2003)

[98] A. Lucchini, A bound on the number of generators of a finite group, *Arch. Math.*, Vol.53 (1989), 313–317.

[99] A. Lucchini, A bound on the expected number of random elements to generate a finite group all of whose Sylow subgroups are d-generated, *Arch. Math.* **107** (2016), no. 1, 1–8.

[100] A. Lucchini, Generators and minimal normal subgroups, *Arch. Math.*, Vol. 64 (1995), 273–276.

[101] A. Lucchini, On groups with d-generator subgroups of coprime index, *Comm. Algebra* **28** (2000), no. 4, 1875–1880.

[102] A. Lucchini, Subgroups of solvable groups with non-zero Möbius function. *J. Group Theory* **10** (2007), no. 5, 633–639.

[103] A. Lucchini, The expected number of random elements to generate a finite group, *Monatsh. Math.* **181** (2016), no. 1, 123–142

[104] A. Lucchini, The largest size of a minimal generating set of a finite group, *Arch. Math.* **101** (2013), 1–8.

[105] A. Lucchini, Minimal generating sets of maximal size in finite monolithic groups, *Arch. Math.* **101** (2013), 401–410.

[106] A. Lucchini and M. Moscatiello, A probabilistic version of a theorem of László Kovács and Hyo-Seob Sim, *International Journal of Group Theory* Vol. 9 No. 1 (2020),1–6.

[107] A. Lucchini and M. Moscatiello, Comparing the expected number of random elements from the symmetric and the alternating groups needed to generate a transitive subgroup, *Ars Mathematica Contemporanea* **16** (2019), no. 1, 237–244

[108] A. Lucchini and M. Moscatiello, Generation of finite groups and maximal subgroup growth, *Adv. Group Theory Appl.*, Vol. 9 (2020), 39–49

[109] A. Lucchini and M. Moscatiello, The expected number of elements to generate a finite group with d-generated Sylow subgroups, *Rocky Mountain Journal of Mathematics* **48** (2018), no. 6, 1963–1982

[110] A. Lucchini and M. Moscatiello, The Tarski irredundant basis theorem and the finite soluble groups, *Mathematische Nachrichten* **292** (2019), no. 5, 1022–1031

[111] A. Lucchini, M. Moscatiello, S. Palcoux and P. Spiga, Boolean lattices in finite alternating and symmetric groups, *Forum of Mathematics, Sigma*, to appear

[112] A. Lucchini, M. Moscatiello and P. Spiga, A polynomial bound for the number of maximal systems of imprimitivity of a finite transitive permutation group, *Forum Mathematicum* **32** (3), (2019), 713–721.

[113] A. Lucchini, M. Moscatiello and P. Spiga, Bounding the maximal size of independent generating sets of finite group, *Proc. A Royal Soc. Edinburgh*, (2020), 1–18

[114] A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996) 429-459.

[115] A. Mann and A. Shalev, Simple groups, maximal subgroups and probabilistic aspects of profinite groups, *Israel J. Math.* **96** (1996) 449–468.

[116] N. E. Menezes, Random generation and chief length of finite groups, PhD Thesis, http://hdl.handle.net/10023/3578.

[117] G. Miller, On the groups generated by two operators, *Bull. Amer. Math. Soc.* **7** (1901), 424–426.

[118] G. A. Miller, Groups containing the largest possible number of operators of order two, *Amer. Math. Monthly* **12** (1905), 149–151.

[119] J. Morris, M. Moscatiello and P. Spiga, On the asymptotic enumeration of Cayley graphs, arXiv:2005.07687.

[120] J. Morris and P. Spiga, Asymptotic enumeration of Cayley digraphs, *Israel J. Math.*, to appear.

[121] J. Morris, P. Spiga and G. Verret, Automorphisms of Cayley graphs on generalised dicyclic groups, *European J. Combin.* **43** (2015), 68–81.

[122] M. Moscatiello and C. M. Roney-Dougal, Base size of primitive permutation groups, in preparation.

[123] E. Netto, The theory of substitutions and its applications to algebra, Second edition, *Chelsea Publishing Co.*, New York 1964 (first published in 1892).

[124] L. A. Nowitz and M. Watkins, Graphical regular representations of direct product of groups, *Monatsh. Math.* **76** (1972), 168–171.

[125] L. A. Nowitz and M. Watkins, Graphical regular represntations of non-abelian groups, II, *Canad. J. Math.* **24** (1972), 1009–1018.

[126] L. A. Nowitz and M. Watkins, Graphical regular representations of non-abelian groups, I, *Canad. J. Math.* **24** (1972), 993–1008.

[127] O. Ore, Structures and group theory. II, *Duke Math. J.* **4** (2) (1938), 247–269.

[128] S. Palcoux, Ore's theorem for cyclic subfactor planar algebras and beyond, *Pacific J. Math.* **292** (1) (2018), 203–221.

[129] S. Palcoux, Ore's theorem on subfactor planar algebras, *To appear in Quantum Topology* (2019), arXiv:1704.00745.

[130] S. Palcoux, Dual Ore's theorem on distributive intervals of finite groups, *J. Algebra* **505** (2018), 279–287.

[131] S. Palcoux, Euler totient of subfactor planar algebras, *Proc. Am. Math. Soc.* **146** (11) (2018), 4775–4786.

[132] P. Pálfy, P. Pudlák, Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups, *Algebra Universalis* **11** (1980), 22–27.

[133] The PARI Group, PARI/GP version `2.9.0`, Univ. Bordeaux, 2016, http://pari.math.u-bordeaux.fr/.

[134] M. Patassini, The probabilistic zeta function of $\mathrm{PSL}(2,q)$, of the Suzuki groups ${}^2B_2(q)$ and of the Ree groups ${}^2G_2(q)$, *Pacific J. Math.* **240** (2009), no. 1, 185–200.

[135] M. Patassini, On the (non-)contractibility of the order complex of the coset poset of a classical group, *J. Algebra* **343** (2011), 37—77.

[136] M. Patassini, On the (non-)contractibility of the order complex of the coset poset of an alternating group, *Rend. Semin. Mat. Univ. Padova* **129** (2013), 35–46.

[137] C. Pomerance, The expected number of random elements to generate a finite abelian group, *Period. Math. Hungar.* **43** (2001), 191–198.

[138] L. Pyber , Asymptotic results for permutation groups. In *Groups and Computation* (eds. L. Finkelstein and W. Kantor), DIMACS Series, Vol. 11, pp. 197–219, 1993.

[139] C. E. Praeger, Finite quasiprimitive graphs, in *Surveys in combinatorics*, London Mathematical Society Lecture Note Series, vol. 24 (1997), 65–85.

[140] C. E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. London Math. Soc. (3)* **60** (1990), 68–88.

[141] C. E. Praeger, C. Schneider, *Permutation groups and cartesian decompositions*, London Mathematical Society Lecture Notes Series 449, Cambridge University Press, Cambridge, 2018.

[142] A. Renyi, Probability Theory, North-Holland, Amsterdam, 1970.

[143] P. Ribenboin, *The Book of Prime Number Records*, Second Edition, Springer-Verlag, New York, 1989.

[144] D. Robinson, A course in the theory of groups, Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1993.

[145] C. M. Roney-Dougal and S. Siccha, Normalisers of primitive permutation groups in quasipolynomial time, *Bull. London Math. Soc.* **52** (2020) 358–366.

[146] B. Rosser, Explicit bounds for some functions of prime numbers, *Amer. J. Math.* **63**, (1941), 211–232.

[147] J. K. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[148] J. Saxl and J. Whiston, On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$, *J. Algebra* **258** (2002), 651–657.

[149] Á. Seress, Permutation group algorithms, *Cambridge Tracts in Mathematics* **152**, Cambridge University Press 2003.

[150] Á. Seress, The minimal base size of primitive solvable permutation groups, *J. London Math. Soc.* **53** (1996), 243–255.

[151] L.L. Scott, Representations in characteristic p, *In The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)* (1980), vol. 37, 319– 331.

[152] J. Shareshian, R. Woodroofe, Order complexes of coset posets of finite groups are not contractible, *Adv. Math.* **291** (2016), 758–773.

[153] P. Spiga, Finite primitive groups and edge-transitive hypergraphs, *J. Algebr. Comb.* **43** (3) (2016), 715–734.

[154] P. Spiga, On the equivalence between a conjecture of Babai-Godsil and a conjecture of Xu concerning the enumeration of Cayley graphs, submitted.

[155] R. P. Stanley, Enumerative combinatorics, Vol. 1, *Cambridge studies in Advanced Mathematics*, vol. 49, Cambridge University Press, Cambridge, 1997.

[156] R. Steinberg, Generators for simple groups, *Canad. J. Math.* **14** (1962), 277–283.

[157] D. E. Taylor, The geometry of the classical groups, Heldermann Verlag, 1992.

[158] J. Tits, *The Geometric Vein. The Coxeter Festschrift*, Springer-Verlag, New York, 1982.

[159] P. Turán, An extremal problem in graph theory (hungarian), *Mat. Fiz. Lapok* **48** (1941), 436–452.

[160] G. E. Wall, Some applications of the Eulerian functions of a finite group, *J. Aust. Math. Soc.* **2** (1961), 35–59.

[161] M. E. Watkins, On the action of non-abelian groups on graphs, *J. Combin. Theory* **11** (1971), 95–104.

[162] V. K. Wei, A lower bound on the stability number of a simple graph, *Bell Laboratories Technical Memorandum*, 81–11217–9, Murray Hill, NJ, 1981.

[163] J. Whiston, Maximal independent generating sets of the symmetric group, *J. Algebra* **232** (2000), 255–268.

[164] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsch. Math. Phys.* **3** (1892), 265–284.

Acknowledgements

I am greatly indebted to my supervisor Andrea Lucchini for his neverending patience and guidance, and for sharing his enthusiasm and love for mathematics with me. This thesis without him it would not exist.

Thank you to my "cosupervisor ad honorem" Pablo Spiga for never stopped motivating me with new questions and problems. He always advised me on every aspect of my professional growth. I am very glad to have the opportunity to work with him.

I would like to thank Colva Roney-Dougal for introducing me to the intriguing topic of the bases and for giving me the possibility to work with her in the exciting environment of St. Andrews and Cambridge.

I would like to thank my colleagues for their moral support, for listening to my complaints, and for making this experience so much fun.

Thank you to my parents for always believe in me and for their support during these years.

Finally, this dissertation would not have been possible without the love, encouragement, patience and tolerance of Umberto.