UNIVERSITÀ DEGLI STUDI DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Matematica Pura ed Applicata

SCUOLA DI DOTTORATO DI RICERCA IN SCIENZE MATEMATICHE

INDIRIZZO MATEMATICA

CICLO XXII

SOME PROPERTIES OF THE MÖBIUS FUNCTION IN THE SUBGROUP LATTICE OF THE ALTERNATING AND SYMMETRIC GROUPS

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

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

Supervisore: Ch.mo Prof. Andrea Lucchini

Dottorando: Valentina Colombo

31 dicembre 2009

Abstract

In this thesis we investigate some properties of the Möbius function on the subgroup lattice of the Alternating and Symmetric groups of degree n, $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$. The study of this function is strictly related to the study of the probabilistic zeta function of a finite or profinite group. We obtain results on two different open questions. First we prove that in all the Alternating and Symmetric groups the Möbius number of each subgroup can be bounded polinomially in terms of its index and the number of subgroups with a given index n and non trivial Möbius number grows at most polynomially in n. This result is an important step in order to prove a conjecture of A.Mann on the absolute convergency of the probabilistic series associated to a positively finitely generated profinite group. Then we consider a problem introduced by A.Mann and N.Boston: they conjectured that the existence, for a fixed value of n, of a "good" correspondence between the maximal subgroups of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ reflects the equality between the probabilistic series of $\mathrm{Sym}(n)$ and the probabilistic series of the direct product of $\mathrm{Alt}(n)$ with a cyclic group of order 2. We prove that this conjecture holds whenever n is a prime; but it does not hold in general (for example when $n = 21$). Even if there exists a one-to-one correspondence between maximal subgroups of $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ the conjecture can fail; it is the case of $n = 62$.

Riassunto

In questa tesi analizziamo alcune proprietà della funzione di Möbius nel reticolo dei sottogruppi dei gruppi Alterno e Simmetrico di grado n, $\mathrm{Alt}(n)$ e $\mathrm{Sym}(n)$. Lo studio di questa funzione è strettamente correlato allo studio della funzione zeta probabilistica di un gruppo finito o profinito. Otteniamo risultati riguardanti due problemi distinti. Innanzitutto dimostriamo che in ogni gruppo Alterno o Simmetrico il numero di Möbius di ogni sottogruppo può essere limitato polinomialmente nell'indice di tale sottogruppo, ed il numero di sottogruppi con un dato indice n e con numero di Möbius non nullo cresce al più polinomialmente in n. Questo risultato è un passo importante al fine di dimostrare la validità di una congettura di A.Mann riguardante la convergenza assoluta della serie probabilistica associata ad un gruppo profinito positivamente finitamente generato. In secondo luogo consideriamo un altro problema: A.Mann e N.Boston hanno congetturato che l'esistenza, per un dato valore di n, di una "buona" corrispondenza tra i sottogruppi massimali di $\mathrm{Alt}(n)$ e $\mathrm{Sym}(n)$ rifletta l'uguaglianza tra la serie probabilistica di $\mathrm{Sym}(n)$ e la serie probabilistica del prodotto diretto fra $\mathrm{Alt}(n)$ ed un gruppo ciclico di ordine 2. Proviamo che tale congettura vale se n è primo; ma non è vera in generale (ad esempio quando $n = 21$). Persino se si assume l'esistenza di una corrispondenza biunivoca fra i massimali di $\mathrm{Alt}(n)$ e $\mathrm{Sym}(n)$, la congettura può non valere; è ciò che accade quando $n = 62$.

Contents

Introduction

In this thesis we investigate some properties of the Möbius function μ on the subgroup lattice of a finite group; in particular we will consider finite Alternating and Symmetric groups.

The most relevant results, contained in Chapter 4, are on the following problem, introduced in Chapter 2. In this chapter G denotes a finitely generated profinite group; we define the Möbius function $\mu(H, G)$ in the lattice of the open subgroups of G by the rules: $\mu(G, G) = 1$ and $\sum_{K \geq H} \mu(K, G) = 0$ if $H < G$. In [25] and [26] Mann proposed to investigate the following problems:

1. What are the groups in which $|\mu(H, G)|$ is bounded by a polynomial function in the index of H?

2. What are the groups in which the number $b_n(G)$ of subgroups H of index n satisfying $\mu(H, G) \neq 0$ grows at most polynomially in n?

The interest for these questions is related to the study of the function $P_G(t)$ expressing the probability that t randomly chosen elements of G generate G topologically (the probability being defined via the normalized Haar measure on G). As it was proved by Mann in [26], the groups G for which $\mu(H, G)$ and $b_n(G)$ are polynomially bounded in terms of $|G : H|$ and n respectively are precisely those for which the infinite sum

$$\sum_{H <_o G} \frac{\mu(H, G)}{|G : H|^s}$$

is absolutely convergent in some half complex plane. When this happens, this infinite sum represents in the domain of convergency an analytic function which assumes precisely the value $P_G(t)$ on any positive integer t large enough. Since $\mu(M, G) = -1$ for any maximal subgroup M of G, it must be

$m_n(G) \leq b_n(G)$ (where $m_n(G)$ denotes the number of maximal subgroups of G with index n). In particular, if $b_n(G)$ grows polynomially, then G has polynomial maximal subgroup growth (PMSG). A theorem by Mann and Shalev ([27]) characterizes groups with PMSG as those which are positively finitely generated (PFG), i.e. $P_G(t) > 0$ for some choice of t. Mann conjectured that, conversely, the following holds:

Conjecture 1 (Mann) *If G is a PFG group, then $|\mu(H,G)|$ is bounded by a polynomial function in the index of H and $b_n(G)$ has growth at most polynomial in n.*

Recently Lucchini has proved that this problem can be reduced to the study of the Möbius function of almost simple groups associated to the set $\Lambda(G)$ of finite monolithic groups L with $\operatorname{soc} L$ non abelian and L an epimorphic image of G. More precisely, for any $L \in \Lambda(G)$ denote by X_L the almost simple group associated to L, and by $b_n^*(X_L)$ the number of subgroups K of X_L with $|X_L : K| = n$, $K \operatorname{soc} X_L = X_L$ and $\mu(K, X_L) \neq 0$; the following holds ([20]): there exist two constants γ_1 and γ_2 such that $b_n(G) \leq n^{\gamma_1}$ and $|\mu(H,G)| \leq |G : H|^{\gamma_2}$ for each $n \in \mathbb{N}$ and for each open subgroup H of G if and only if there exist two constants c_1 and c_2 such that hold $b_n^*(X_L) \leq n^{c_1}$ and $|\mu(Y, X_L)| \leq |X_L : Y|^{c_2}$ for each $L \in \Lambda(G)$, each $n \in \mathbb{N}$ and each $Y \leq X_L$ with $Y \operatorname{soc} X_L = X_L$. This means that Mann's conjecture is true if the following holds:

Conjecture 2 (Lucchini) *There exist two constants c_1 and c_2 such that for each finite almost simple group X we have: $b_n^*(X) \leq n^{c_2}$ for each $n \in \mathbb{N}$, and $|\mu(Y,X)| \leq |X : Y|^{c_1}$ for each $Y \leq X$ with $Y \operatorname{soc} X = X$.*

In Chapter 4 we prove that this conjecture is true for all the Alternating and Symmetric groups.

Theorem 1 *There exists an absolute constant α such that for any $n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $m \in \mathbb{N}$, then $b_m(G) \leq m^{\alpha}$.*

Theorem 2 *There exists an absolute constant β such that for any $n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $H \leq G$, then $|\mu(H,G)| \leq |G : H|^{\beta}$.*

To prove these theorems we will use results contained in Chapter 1. In particular, a key ingredient in these proofs is a consequence of the closure

theorem of Crapo. It turns out (see in particular Lemma 1.3.6) that if G is a transitive permutation group on a set Γ, then in order to bound the number of subgroups H with $\mu(H,G) \neq 0$ and to estimate $|\mu(H,G)|$ it suffices to obtain:

(1) similar bounds for the particular case when H is transitive;

(2) estimations on the number of subgroups of G that are maximal with respect to the property of admitting a certain set of orbits (Γ-closed subgroups) and bounds for the number of orbits of a Γ-closed subgroup H in terms of the index $|G : H|$.

When $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$, the second task is easy, since a closed subgroup is conjugated to $(\mathrm{Sym}(n_1) \times \cdots \times \mathrm{Sym}(n_r)) \cap G$ with $n_1 + \ldots n_r = n$ (see Theorem 1.3.8 and Lemma 4.2.3). The first task can be performed considering the action of G on the set $\Delta_n = \{(a,b) \,|\, 1 \leq a, b \leq n,\ a \neq b\}$. In this way it suffices to collect informations about the Möbius number of the Δ_n-transitive subgroups of G (but these are precisely the 2-transitive subgroups of G) and to study how many transitive subgroups of G are Δ_n-closed (see Corollary 1.4.6).
We employ in our proofs the classification of the 2-transitive permutation groups (see for example [4]) and other asymptotic results on the numbers of subgroups of $\mathrm{Sym}(n)$ which have been proved with the help of the classification of the finite nonabelian simple groups; many of these results are contained in [32].

Moreover in the last section of Chapter 4 we prove that the bound on the Möbius number, in Theorem 2, can be improved if $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$, with p a "good" prime. In fact it holds:

Theorem 3 *Let p be a prime, with $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$, for any couple of natural numbers (q, d), with $q > 4$ if $d = 2$.*
If $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$ and $H \leq G$, then

$$|\mu(H,G)| \leq |G : H|.$$

In the proof of this result we will use extimations on the Möbius numbers $\mu(H, \mathrm{Alt}(p))$ and $\mu(H, \mathrm{Sym}(p))$ with H a subgroup of $\mathrm{Alt}(p)$, which are proved in Chapter 3 (see Lemma 3.2.2 and Theorem 3.2.3).

We verify that the bound of Theorem 3 does not hold in general for a degree $n \in \mathbb{N}$; but it leads us to formulate the following conjecture:

Conjecture 3 *There exists an absolute constant γ such that $\forall\, n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $H \leq G$, then*

$$|\mu(H, G)| \leq \gamma \cdot |G : H|.$$

In Chapter 3 we consider a problem on the probabilistic zeta function of a finite group; this function is introduced in the first section of Chapter 2. Let G be a finite group and denote by $P_G(t)$ the probability the t randomly chosen elements of G generate G itself; this integer function can be interpolate by a complex function $P_G(s)$, defined as:

$$P_G(s) = \sum_{|G:H|=n} \frac{\mu(H, G)}{n^s}$$

The multiplicative inverse of the function $P_G(s)$ is called the probabilistic zeta function of G.

Given $N \triangleleft G$, we define $P_{G,\,N}(s) = \sum_{\substack{|G:H|=n \\ HN=G}} \mu(H, G)/n^s$. As it is shown in [3, Section 2.2], it holds $P_G(s) = P_{G/N}(s) P_{G,\,N}(s)$. In [24] Lucchini and Massa have proved that there exist explicit criterions to recognize whether the factor group $G/\mathrm{Frat}(G)$ is isomorphic to $\mathrm{Alt}(n)$ (with $n \geq 5$) only looking at the coefficients of $P_G(s)$. Using these results they have been able to verify that if $P_G(s) = P_{\mathrm{Sym}(n)}(s)$, with $n \geq 5$, then either $G/\mathrm{Frat}(G) \cong \mathrm{Sym}(n)$ or $G/\mathrm{Frat}(G) \cong \mathrm{Alt}(n) \times C_2$. We investigate, in Chapter 3, which values of n satisfy:

$$P_{\mathrm{Sym}(n)}(s) = P_{\mathrm{Alt}(n) \times C_2}(s) = P_{\mathrm{Alt}(n)}(s) \cdot P_{C_2}(s) \tag{1}$$

This is equivalent to ask when $P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s) = P_{\mathrm{Alt}(n)}(s)$. Many authors have studied this problem (see for example [7]) and, by GAP, we already know whether n satisfies equality (1), for any $n < 12$. In [2] Boston and Mann formulated the following conjecture:

Conjecture 4 (Boston, Mann) *The validity of (1), for $n \geq 5$, reflects the non-existence of maximal subgroups of* $\mathrm{Alt}(n)$ *that coincide with their normalizer in* $\mathrm{Sym}(n)$.

We will verify that this conjecture holds whenever n is a prime. In fact if p is a "good" prime (i.e. $\mathrm{Sym}(p)$ does not contain any almost simple transitive subgroup) we prove the following:

Theorem 4 *Let $p \geq 5$ prime, $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$. Then $P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) = P_{\mathrm{Alt}(p)}(s)$.*

Otherwise, $\mathrm{Alt}(p)$ has some maximal subgroups which coincide with their normalizers in $\mathrm{Sym}(p)$; in these cases we prove:

Theorem 5 *If $p = 11$, $p = 23$ or $p = (q^d - 1)/(q - 1) > 5$, then it holds $P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) \neq P_{\mathrm{Alt}(p)}(s)$.*

In the proofs of these theorems we make a deep use of the formula expressing the difference between $P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s)$ and $P_{\mathrm{Alt}(n)}(s)$ (see Section 2.1); from this formula some conditions can be deduced that are sufficient (but not necessary) to guarantee that $P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s) = P_{\mathrm{Alt}(n)}(s)$.

The conjecture of Boston and Mann is not true in general for $n \geq 5$. In the last section of Chapter 3 we make some considerations about the difficulty to estabilish whether $\mathrm{Sym}(n)$ satisfies or not the conjecture, and we show some counterexamples. First of all the condition that any maximal subgroup of $\mathrm{Alt}(n)$ does not coincide with its normalizer in $\mathrm{Sym}(n)$ is not sufficient to guarantee the existence of a bijection between the set $\mathcal{A}$ of the maximal subgroups of $\mathrm{Alt}(n)$ and the set $\mathcal{S}$ of the maximal supplements of $\mathrm{Alt}(n)$ in $\mathrm{Sym}(n)$. We verify that this fact makes the failure of the conjecture in the case $n = 21$. Then we notice that, even if this bijection between $\mathcal{A}$ and $\mathcal{S}$ exists, it does not always imply $P_{\mathrm{Alt}(n)}(s) = P_{\mathrm{Sym}(n),\mathrm{Alt}(n)}(s)$; it is what happens when $n = 62$. The problem is that there is no hope that the bijection between $\mathcal{A}$ and $\mathcal{S}$ can be extended to a bijection between the subgroups that can be obtained as intersection of elements of $\mathcal{A}$ and those that are intersection of elements of $\mathcal{S}$. In particular it is very difficult to study the intersections of imprimitive subgroups: it is possible that the intersection of few (even two) imprimitive maximal subgroups of $\mathrm{Sym}(n)$ is already contained in $\mathrm{Alt}(n)$ (see the case $n = 21$).

We conclude Chapter 3 with an open problem. We want to consider the Symmetric groups $\mathrm{Sym}(n)$ which do not contain any primitive proper subgroup, different from $\mathrm{Alt}(n)$. By Cameron ([4]), we know that the family

$\overline{\mathcal{F}}$ of these groups has density 1 in the set of all Symmetric groups. Moreover we notice that for each $\mathrm{Sym}(n) \in \overline{\mathcal{F}}$ there exists a bijection between $\mathcal{A}$ and $\mathcal{S}$, defined as above. Then it is natural to ask if $\mathrm{Sym}(n) \in \overline{\mathcal{F}}$ satisfies or not the conjecture of Boston and Mann, and if all the Symmetric groups in $\overline{\mathcal{F}}$ have the same behaviour. We have not yet obtained an answer to this question. The possibility of expressing subgroups of the Alternating group as intersection of two (or few) imprimitive maximal subgroups of the Symmetric group, could imply the existence of a counterexample to the conjecture, even among the groups in $\overline{\mathcal{F}}$. But we are inclined to think that, if such a counterexample exists, then the degree must be quite large.

Chapter 1

Preliminaries

We start by stating some definitions and by proving some results that will be used throughout this thesis.

1.1 The Möbius function on a finite poset

Let P be a locally finite poset.

Definition 1.1.1 *The Möbius function μ on $P \times P$ is defined as follows:*

$$\mu(x,y) = \begin{cases} 0 & \text{if } x \not\leq y \\ 1 & \text{if } x = y \\ -\sum_{x<z\leq y} \mu(z,y) & \text{if } x < y \end{cases}$$

The Möbius function on P will often be written as μ_P.

Definition 1.1.2 *A closure on P is a function $^- : P \to P$ satisfying the following three conditions:*

a) $x \leq \bar{x}$ for all $x \in P$;

b) if $x, y \in P$ with $x \leq y$, then $\bar{x} \leq \bar{y}$;

c) $\bar{\bar{x}} = \bar{x}$ for all $x \in P$.

If $^-$ is a closure map on P then $\bar{P} := \{x \in P | \, \bar{x} = x\}$.

Notice that $\bar{P}$ is a poset with order induced by the order on P.

The closure theorem of Crapo ([6, Theorem 1]). Let P be a finite poset and let $^-\colon P \to P$ be a closure map. Fix $x, y \in P$ such that $y \in \bar{P}$. Then

$$\sum_{\bar{z}=y} \mu_P(x,z) = \begin{cases} \mu_{\bar{P}}(x,y) & \text{if } \bar{x} = x \\ 0 & \text{otherwise.} \end{cases}$$

Remark 1.1.3 *By definition of μ_P, we note that the closure theorem of Crapo can be formulated in the following way, using the same notations:*

$$\sum_{\substack{\bar{z}=y \\ x \leq z}} \mu_P(x,z) = \begin{cases} \mu_{\bar{P}}(x,y) & \textit{if } \bar{x} = x \\ 0 & \textit{otherwise.} \end{cases}$$

The Möbius inversion formula. Let P be a finite poset and suppose $f, g : P \to \mathbb{Z}$ two functions such that $g(x) = \sum_{y \leq x} f(y)$ for all $x \in P$. Then

$$f(y) = \sum_{x \leq y} \mu_P(x,y) g(x) \quad \text{for all } y \in P.$$

Definition 1.1.4 *A chain in P is a subset $C \subseteq P$ such that $x \leq y$ or $y \leq x$ for all $x, y \in C$. Let $C = \{x_0, \ldots, x_l\}$, with $x_i < x_{i+1}$ for $0 \leq i \leq l-1$; then the elements of C can be ordered as a sequence*

$$x_0 < x_1 < \cdots < x_l$$

The length of the chain C is l.
An antichain in P is a subset $A \subseteq P$ such that neither $x \leq y$ nor $y \leq x$ holds for any pair of distinct elements $x, y \in A$.

Theorem 1.1.5 ***([13, Theorem 2.2])*** *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let r be the length of the longest chain of P. For $-1 \leq i \leq r-2$, let $c_i = c_i(P)$ be the number of chains $\hat{0} = x_0 < x_1 < \cdots < x_{i+1} < x_{i+2} = \hat{1}$ of P. Then*

$$\mu_P(\hat{0}, \hat{1}) = \sum_{i=-1}^{r-2} (-1)^i c_i.$$

It follows

Corollary 1.1.6 *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let $y \in P$; then $\mu_P(y, \hat{1})$ is equal to the difference between the number of chains connecting y to $\hat{1}$ of even length, and the number of similar chains of odd length.*

Definition 1.1.7 *Let L be a finite lattice.*

(a) $\hat{0}$ and $\hat{1}$ denote, respectively, the unique minimum element of L and the unique maximum element of L.

(b) A complement to $x \in L$ is an element $y \in L$ such that $inf_L(x, y) = \hat{0}$ and $sup_L(x, y) = \hat{1}$. Also $x^\perp$ denote the set of complements to x in L.

The complement theorem of Crapo ([5, Theorem 3]) Let L be a finite lattice and fix $x \in L$. Then

$$\mu_L(\hat{0}, \hat{1}) = \sum_{y,z \in x^\perp} \mu_L(\hat{0}, y)\zeta_L(y, z)\mu_L(z, \hat{1}),$$

where ζ_L is the zeta function on L, with $\zeta_L(y, z) = 1$ if $y \leq z$, or $\zeta_L(y, z) = 0$ otherwise. In particular, if $x^\perp$ is an antichain, then

$$\mu_L(\hat{0}, \hat{1}) = \sum_{y \in x^\perp} \mu_L(\hat{0}, y)\mu_L(y, \hat{1}).$$

1.2 Möbius functions associated to a finite group: definitions and properties

Let G be a finite group. We consider the lattice $\mathcal{L}_G$ of subgroups of G; this is, in particular, a poset, ordered by inclusion, and we denote by $\mu_{\mathcal{L}_G}$ the Möbius function on $\mathcal{L}_G$.

Remark 1.2.1 *If $H \leq K \leq G$ then*

$$\mu_{\mathcal{L}_G}(H, K) = \mu_{\mathcal{L}_K}(H, K)$$

with $\mu_{\mathcal{L}_K}$ the Möbius function associated to $\mathcal{L}_K$. From now on, we will write $\mu(H, K)$ instead of $\mu_{\mathcal{L}_K}(H, K)$ whenever H is a subgroup of K.

Remark 1.2.2 *One of the first authors to study the Möbius function on the subgroup lattice of a group G was Hall in [13]; in this paper he noticed the following properties of $\mu_{\mathcal{L}_G}$.*

1) Let $H < G$; $\mu(H,G) \neq 0$ only if H is an intersection of maximal subgroups in $\mathcal{L}_G$.

2) Let $H \leq G$; $\mu(H,G)$ is equal to the difference between the number of chains of subgroups from H to G of even length, and the number of such chains of odd length (this is an application to the lattice $\mathcal{L}_G$ of Corollary 1.1.6).

Remark 1.2.3 *Another characterization of $\mu_{\mathcal{L}_G}$ was given by Mann in [25]: he noticed that $\mu(H,G)$, for any $H \leq G$, is the difference between the number of ways to express H as the intersection of evenly many maximal subgroups of G and the number of ways to express it as such an intersection of oddly many terms.*

Let $\mathcal{L}_G^\star$ be the set of the intersections of maximal elements in $\mathcal{L}_G$, with G adjoined; $\mathcal{L}_G^\star$ is a poset with order induced by the order on $\mathcal{L}_G$. Denote by $\mu_{\mathcal{L}_G^\star}$ the Möbius function on this poset.

Remark 1.2.4 *From the definition of $\mu_{\mathcal{L}_G}$ and Remark 1.2.2 1), it follows that*

$$\mu(H,G) = \mu_{\mathcal{L}_G^\star}(H,G)$$

for any $H \in \mathcal{L}_G^\star$.

Let $n \geq 1$ be a natural number; we may define the Möbius function $\mu(n)$, that is strictly connected to the Möbius function associated to the subgroup lattice of a cyclic group.

Definition 1.2.5 *Let $n \in \mathbb{N}$;*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2 | n \text{ for some prime } p, \\ (-1)^r & \text{if } n = p_1 p_2 \dots p_r \text{ where the } p_i \text{ are distinct primes.} \end{cases}$$

Remark 1.2.6 *By the definition of $\mu(n)$, we observe that, if $n \neq 1$, it holds*

$$\sum_{d|n} \mu(d) = 0.$$

It is now easy to prove the following proposition.

Lemma 1.2.7 *Let G be a cyclic group of order n; then*

$$\mu(\langle 1 \rangle, G) = \mu(n).$$

1.3 Some applications on $\mathcal{L}_G$

If G is a transitive permutation group on a finite set Γ we may define a closure function on $\mathcal{L}_G$ in the following way.

Definition 1.3.1 *Let $Z \leq G$ and let $\tau = \{\Lambda_1, \dots, \Lambda_k\}$ be the set of orbits of Z in its action on Γ. For any $1 \leq i \leq k$ denote by $\mathrm{Sym}(\Lambda_i)$ the Symmetric group on the set Λ_i. We define*

$$\bar{Z} := (\mathrm{Sym}(\Lambda_1) \times \cdots \times \mathrm{Sym}(\Lambda_r)) \cap G$$

and

$$\begin{array}{rccc} {}^{\bar{}}\colon & \mathcal{L}_G & \to & \mathcal{L}_G \\ & Z & \mapsto & \bar{Z} \end{array}$$

The function ${}^{\bar{}}\colon \mathcal{L}_G \to \mathcal{L}_G$ so defined is a closure function on $\mathcal{L}_G$. We will call $\bar{Z}$ the closure of Z in $\mathcal{L}_G$, for any $Z \leq G$; in particular, if Z is transitive on Γ its closure is G. If $Z = \bar{Z}$ we will say that Z is closed in $\mathcal{L}_G$.
The set $\bar{\mathcal{L}}_G := \left\{ Z \in \mathcal{L}_G \,|\, Z = \bar{Z} \right\}$ is a poset, with order induced by $\mathcal{L}_G$, and we denote by $\mu_{\bar{\mathcal{L}}_G}$ the Möbius function on $\bar{\mathcal{L}}_G$.

Remark 1.3.2 *For $Z \in \bar{\mathcal{L}}_G$, we will write $\bar{\mu}(Z, G)$ instead of $\mu_{\bar{\mathcal{L}}_G}(Z, G)$. Notice that in general $\bar{\mathcal{L}}_K \neq \bar{\mathcal{L}}_G \cap \mathcal{L}_K$, when K is a transitive subgroup of G; then, if $Z \leq K \leq G$, it follows that in general $\bar{\mu}(Z, K) \neq \mu_{\bar{\mathcal{L}}_G}(Z, K)$.*

Definition 1.3.3 *Let $\mathcal{P}_\Gamma$ be the poset of all the partitions of Γ, ordered by refinement: so $\{A_1, \dots, A_h\} \leq \{B_1, \dots, B_l\}$ if and only if each A_i is a subset of some B_j. The maximum $\hat{1}$ of $\mathcal{P}_\Gamma$ is $\{\Gamma\}$. The orbit lattice of G is defined as*

$$\mathcal{P}_\Gamma(G) := \{\tau \in \mathcal{P}_\Gamma | \text{ the orbits of some } Z \in \mathcal{L}_G \text{ are the parts of } \tau\}.$$

This is a poset with the order induced by the order in $\mathcal{P}_\Gamma$; we can define on $\mathcal{P}_\Gamma(G)$ the Möbius function, that we denote by $\mu_{\mathcal{P}_\Gamma(G)}$.
If $\tau = \{\Lambda_1, \dots, \Lambda_k\} \in \mathcal{P}_\Gamma(G)$, then we define

$$G(\tau) := (\mathrm{Sym}(\Lambda_1) \times \cdots \times \mathrm{Sym}(\Lambda_k)) \cap G\,;$$

$G(\tau)$ is the maximal subgroup of G whose orbits are precisely the parts of τ.

Remark 1.3.4 *We notice that $Z \in \bar{\mathcal{L}}_G$ if and only if there exists $\tau \in \mathcal{P}_\Gamma(G)$ with $Z = G(\tau)$; hence there is a bijection between the sets $\bar{\mathcal{L}}_G$ and $\mathcal{P}_\Gamma(G)$. Then*

$$\bar{\mu}(Z, G) = \mu_{\mathcal{P}_\Gamma(G)}(\tau, \hat{1})$$

for any $Z \in \bar{\mathcal{L}}_G$.

Remark 1.3.5 *If $G = \mathrm{Sym}(\Gamma)$, then $\mathcal{P}_\Gamma(G) = \mathcal{P}_\Gamma$. Hence the elements of $\bar{\mathcal{L}}_G$ are the subgroups of the form $\mathrm{Sym}(\Lambda_1) \times \cdots \times \mathrm{Sym}(\Lambda_k)$, for any partition $\{\Lambda_1, \ldots, \Lambda_k\}$ in $\mathcal{P}_\Gamma$.*
If $G = \mathrm{Alt}(\Gamma)$, we have $\mathcal{P}_\Gamma(G) \neq \mathcal{P}_\Gamma$. In fact $\mathrm{Alt}(\Gamma)$ doesn't contains any subgroup with number of orbits on Γ equal to $|\Gamma| - 1$. Hence the closed subgroups of $\mathrm{Alt}(\Gamma)$ are of the form $(\mathrm{Sym}(\Lambda_1) \times \cdots \times \mathrm{Sym}(\Lambda_k)) \cap \mathrm{Alt}(\Gamma)$, for any $\{\Lambda_1, \ldots, \Lambda_k\} \in \mathcal{P}_\Gamma$ with $k \neq |\Gamma| - 1$.
Then to any closed subgroup M of $\mathrm{Sym}(\Gamma)$, with number of orbits on Γ different from $|\Gamma|-1$, corresponds a closed subgroup of $\mathrm{Alt}(\Gamma)$, that is equal to $M \cap \mathrm{Alt}(\Gamma)$. Obviously, if $M \neq \langle 1 \rangle$, $|\mathrm{Sym}(\Gamma) : M| = |\mathrm{Alt}(\Gamma) : (M \cap \mathrm{Alt}(\Gamma))|$.

Let G be transitive on Γ. For any subgroup H of G, let

$$\mathcal{S}_H := \{K \leq G \mid K \text{ transitive on } \Gamma, K \geq H\} \subseteq \mathcal{L}_G.$$

The set $\mathcal{S}_H$ is a poset with order induced by the order on $\mathcal{L}_G$. We define two functions $f, g : \mathcal{L}_G \times \mathcal{L}_G \to \mathbb{Z}$ in the following way

$$f(H, Y) = \begin{cases} \mu(H, Y) & \text{if } Y \in \mathcal{S}_H \\ 0 & \text{otherwise,} \end{cases}$$

$$g(H, X) = \begin{cases} \bar{\mu}(H, X) & \text{if } X \in \mathcal{S}_H \text{ and } H \text{ is closed in } \mathcal{L}_X \\ 0 & \text{otherwise.} \end{cases}$$

Applying the closure theorem of Crapo to $\mathcal{L}_X$, with $X \in \mathcal{S}_H$, we obtain

$$\sum_{\substack{Y \leq X \\ Y \in \mathcal{S}_H}} \mu(H, Y) = \begin{cases} \bar{\mu}(H, X) & \text{if } H \text{ is closed in } \mathcal{L}_X \\ 0 & \text{otherwise.} \end{cases}$$

This means that f and g satisfy the relation

$$g(H,X) = \sum_{\substack{Y \leq X \\ Y \in \mathcal{S}_H}} f(H,Y)$$

and, by the Möbius inversion formula, for any $Y \in \mathcal{S}_H$, we have

$$f(H,Y) = \sum_{\substack{X \leq Y \\ X \in \mathcal{S}_H}} \mu(X,Y) g(H,X).$$

Setting $Y = G$, we get:

Lemma 1.3.6 *If H is a subgroup of a transitive permutation group G, then*

$$\mu(H,G) = \sum_{K \in \mathcal{S}_H} \mu(K,G) g(H,K) \tag{1.1}$$

So in particular

$$|\mu(H,G)| \leq \sum_{K \in \mathcal{S}_H} |\mu(K,G)| \cdot |g(H,K)| \tag{1.2}$$

Remark 1.3.7 *In Chapter 4 we will apply the previous Lemma 1.3.6 to study μ when G is the Symmetric group* $\mathrm{Sym}(n)$ *or the Alternating group* $\mathrm{Alt}(n)$*. In particular we will consider G with two different actions: the natural action on the set $I_n := \{1, \ldots, n\}$, and the transitive action on the set $\Delta_n := \{(a,b) \,|\, 1 \leq a, b \leq n,\ a \neq b\}$ defined by $(a,b)g = (ag, bg)$.*

In order to apply Lemma 1.3.6, we first need to estimate $|g(H,K)|$, for $H \leq G$ and $K \in \mathcal{S}_H$. If $K = H$, $|g(H,H)| = 1$; if $K \neq H$ we prove the following proposition.

Theorem 1.3.8 *Assume that G is a transitive permutation group on a set Γ and $H \leq G$. If $K \in \mathcal{S}_H$ and $K \neq H$, then*

$$|g(H,K)| \leq \frac{(r\,!)^2}{2}$$

where r is the number of orbits of H on Γ.

Proof. Recall the definition of $g(H,K)$:

$$g(H,K) = \begin{cases} \bar{\mu}(H,K) & \text{if } H \text{ is closed in } \mathcal{L}_K \\ 0 & \text{otherwise.} \end{cases}$$

If H is not closed in $\mathcal{L}_K$, then $|g(H,K)| = 0$ and we have finished.
So we can suppose that H is closed in $\mathcal{L}_K$; in particular, since $H \neq K$, H is not transitive on Γ. We are proceeding to estimate $|\bar{\mu}(H,K)|$.
Let $\sigma = \{\Omega_1, \dots, \Omega_r\}$ be the set of orbits of H on Γ, with $r > 1$. K is transitive on Γ, then we can define the set $\mathcal{P}_\Gamma(K)$ (see Definition 1.3.3) in the following way:

$$\mathcal{P}_\Gamma(K) := \{\tau \in \mathcal{P}_\Gamma \,|\, \text{the orbits of some } Z \in \mathcal{L}_K \text{ are the parts of } \tau\}.$$

Denote by $\mu_{\mathcal{P}_\Gamma(K)}$ the Möbius function on $\mathcal{P}_\Gamma(K)$; by Remark 1.3.4 it holds

$$\bar{\mu}(H,K) = \mu_{\mathcal{P}_\Gamma(K)}(\sigma, \hat{1}).$$

By Corollary 1.1.6, $|\mu_{\mathcal{P}_\Gamma(K)}(\sigma, \hat{1})|$ is bounded by the number of the chains in $\mathcal{P}_\Gamma(K)$ connecting σ to the partition $\{\Gamma\} = \hat{1}$. This number is obviously smaller or equal than the number v of chains from σ to $\hat{1}$ in $\mathcal{P}_\Gamma$; so we are going to calculate v.
The set $\mathcal{V}$ of all chains between σ and $\hat{1}$ in $\mathcal{P}_\Gamma$ can be ordered by refinement. We start computing the number of maximal chains in the poset $\mathcal{V}$; then we will estimate how many chains are contained in each maximal chain.
Any maximal chain in $\mathcal{V}$ can be constructed in the following way. We join together two parts of σ, obtaining a partition τ_1 of $\mathcal{P}_\Gamma$, with $r-1$ parts, that contains σ; now we join two parts of τ_1 and we have a new partition τ_2, with $r-2$ parts, containing τ_1. We can repeat this process until we have obtained a partition τ_{r-2} with two parts; then, joining these two parts, we have $\{\Gamma\}$.
So a maximal chain has length $r-1$. At the step 1 we have to choose τ_1, joining two parts of σ, and then there are $\binom{r}{2}$ possibilities for τ_1; at the step 2 we have to choose two parts between $r-1$ parts, and so we have $\binom{r-1}{2}$ possibilities for τ_2. So on, until the step $r-1$: we have to join the last two parts, and so we have only one possibility; in fact we obtain the partition $\{\Omega_1 \cup \cdots \cup \Omega_r\} = \hat{1}$. Therefore there are

$$\binom{r}{2} \cdot \binom{r-1}{2} \cdots \binom{2}{2} = \frac{r\,!(r-1)!}{2^{r-1}}$$

maximal chains in $\mathcal{V}$.
Now we have to calculate how many chains are contained in each maximal chain. Let m be a maximal chain in $\mathcal{V}$; then m is of the following form

$$\sigma = \tau_0 < \tau_1 < \tau_2 < \cdots < \tau_{r-1} = \{\Gamma\}$$

To obtain a subchain of m we may delete some elements τ_j of m, with $1 \leq j < r-1$, because σ and τ_{r-1} are fixed. Then the number of subchains of m is equal to the cardinality of the set of parts of $\{\tau_1, \ldots, \tau_{r-2}\}$, with $r-2$ elements; so this cardinality is 2^{r-2}.
Each maximal chain has 2^{r-2} subchains, hence

$$v \leq \frac{r\,!(r-1)!}{2^{r-1}} \cdot 2^{r-2} = \frac{r\,!(r-1)!}{2} \leq \frac{(r\,!)^2}{2}$$

It follows

$$|\bar{\mu}(H, G)| \leq \frac{(r\,!)^2}{2}\,.$$

□

Remark 1.3.9 *We know that the upper bound on $|g(H,K)|$ stated in the previous Theorem 1.3.8 is not the best possible for any $K \in \mathcal{S}_H$. In fact Stanley proved in [35] that if $K \in \{\mathrm{Sym}(\Gamma), \mathrm{Alt}(\Gamma)\}$ then, for any $H \leq K$ closed in $\mathcal{L}_K$ ($H \neq \langle 1 \rangle$ when $K = \mathrm{Alt}(\Gamma)$),*

$$|\bar{\mu}(H, K)| = (r-1)!$$

where r is the number of orbits of H on Γ. Hence, for any $H \leq K$ ($H \neq \langle 1 \rangle$ when $K = \mathrm{Alt}(\Gamma)$), it holds

$$|g(H, K)| \leq (r-1)!\,.$$

1.4 Bounds on permutation groups

In this section we will collect a series of results on permutation groups, that will be very useful in the proofs of our main theorems. We consider $n \in \mathbb{N}$ and $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$, with its natural action on $I_n = \{1, \ldots, n\}$. We can give a bound on the Möbius number of a 2-transitive subgroup of G in the following way.

Theorem 1.4.1 *Suppose $G \in \{\mathrm{Sym}(n), \mathrm{Alt}(n)\}$ and let H be a 2-transitive subgroup of G. Then*

$$|\mu(H, G)| \leq 1.$$

Proof. Clearly $\mu(\mathrm{Alt}(n), \mathrm{Sym}(n)) = -1$, so we may assume $\mathrm{Alt}(n) \not\leq H$. We use the classification of the 2-transitive permutation groups. If H is 2-transitive on I_n, then it is an affine or an almost simple subgroup of G. All affine and almost simple 2-transitive groups are well known; they are listed, for example, in [4], respectively in Table 6.3 and Table 6.4.

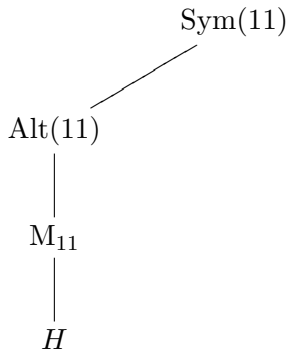
To prove the thesis, it suffices to verify that there are at most two maximal subgroups of G containing H. In fact, if this happens, $\mu(H, G) \neq 0$ only if H is maximal in G or H corresponds to the intersection of these two maximal subgroups (see Remark 1.2.2 *1)*); in both cases, by Remark 1.2.3, we obtain $|\mu(H, G)| = 1$.

Let H be an affine 2-transitive subgroup of G; so $n = p^m$ for some prime p, $m \in \mathbb{N}$, and $H \leq \mathrm{AGL}(m, p) \cap G$ such that $\mathrm{soc}\, H = \mathrm{soc}(\mathrm{AGL}(m, p))$ (we are assuming $p^m \neq 2$). Using [30, Proposition 6.2.] and comparing Table 2 in [30] with Table 6.3, we verify that H is not contained in any proper almost simple subgroup of G different from $\mathrm{Alt}(n)$. Then H may be contained only in some affine subgroups of G and in $H\,\mathrm{Alt}(n)$; moreover $\mathrm{AGL}(m, p) \cap G$ is the unique maximal affine subgroup of G containing H. Hence there are at most two maximal subgroups of G containing H.

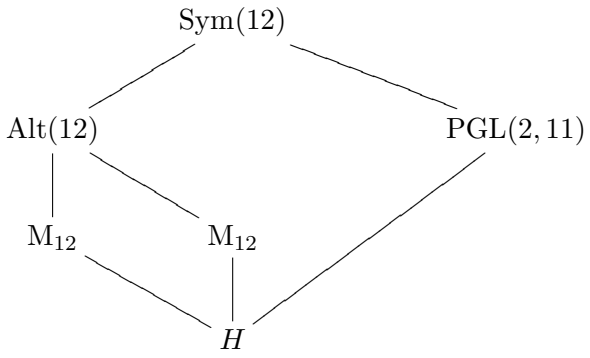
Finally let H be an almost simple 2-transitive subgroup of G. We use [30, Proposition 6.1.] and [4, Table 6.4] to determine the possible proper subgroups of G containing H: we deduce that H is not contained in any affine subgroup of G, but it may be contained in some almost simple 2-transitive subgroups. Denote by S the socle of H. The maximal almost simple subgroup of G containing H and with socle S is $N_G(S)$, that is isomorphic to a subgroup of $\mathrm{Aut}(S)$; we are supposing $\mathrm{Alt}(n) \not\leq H$, and hence $N_G(S) \neq G$. Tables III,IV,V,VI in [17] list all the possible inclusions between almost simple primitive groups with different socles; we compare these tables with Table 6.4 in [4] to determine the inclusions between almost simple 2-transitive proper subgroups of G, with different socles. If $n \notin \{11, 12, 24\}$, then no almost simple K exists with $H \leq K \leq G$ and $\mathrm{soc}\, K \notin \{S, \mathrm{Alt}(n)\}$; hence the maximal subgroups of

G containing H are elements of the set $\{N_G(S), \mathrm{Alt}(n)\}$, and we obtain the thesis. The following exceptional inclusions require more attention: $(n, S, \operatorname{soc} K) \in \{(11, \mathrm{PSL}(2,11), \mathrm{M}_{11}), (12, \mathrm{PSL}(2,11), \mathrm{M}_{12}), (12, \mathrm{M}_{11}, \mathrm{M}_{12}), (24, \mathrm{PSL}(2,23), \mathrm{M}_{24})\}$. We are going to consider these cases.

- $(n, S, \operatorname{soc} K) = (11, \mathrm{PSL}(2,11), \mathrm{M}_{11})$: we observe that $N_{\mathrm{Sym}(11)}(S) = S$ and $N_{\mathrm{Sym}(11)}(\mathrm{M}_{11}) = \mathrm{M}_{11} \Rightarrow H = \mathrm{PSL}(2,11)$ and $K = \mathrm{M}_{11}$. Moreover $H \leq_{\max} K \leq_{\max} \mathrm{Alt}(11)$.
  We obtain the following diagram:

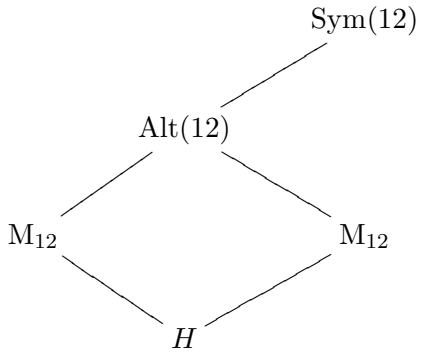


- $(n, S, \operatorname{soc} K) = (12, \mathrm{PSL}(2,11), \mathrm{M}_{12})$: $N_{\mathrm{Sym}(12)}(S) = \mathrm{PGL}(2,11)$ and $N_{\mathrm{Sym}(12)}(\mathrm{M}_{12}) = \mathrm{M}_{12} \Rightarrow H = \mathrm{PSL}(2,11)$ and $K = \mathrm{M}_{12}$. Notice that $H \leq_{\max} \mathrm{PGL}(2,11) \leq_{\max} \mathrm{Sym}(12)$ and $H \leq_{\max} K \leq_{\max} \mathrm{Alt}(12)$. We have this situation:

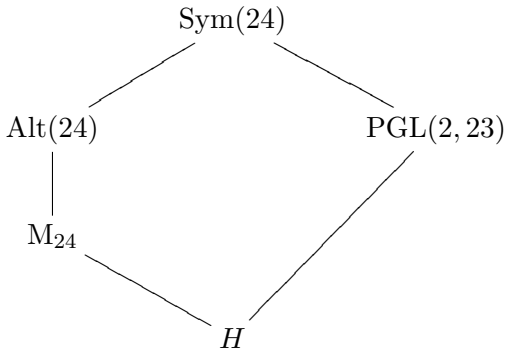


- $(n, S, \operatorname{soc} K) = (12, \mathrm{M}_{11}, \mathrm{M}_{12})$: $N_{\mathrm{Sym}(12)}(S) = S \Rightarrow H = \mathrm{M}_{11}$ and

$K = \mathrm{M}_{12}$. Moreover $H \leq_{\max} K \leq_{\max} \mathrm{Alt}(12)$. We obtain:



- $(n, S, \operatorname{soc} K) = (24, \mathrm{PSL}(2,23), \mathrm{M}_{24})$: $N_{\mathrm{Sym}(24)}(S) = \mathrm{PGL}(2,23)$ and $N_{\mathrm{Sym}(24)}(\mathrm{M}_{24}) = \mathrm{M}_{24} \Rightarrow H = \mathrm{PSL}(2,23)$ and $K = \mathrm{M}_{24}$. Notice that $H \leq_{\max} \mathrm{PGL}(2,23) \leq_{\max} \mathrm{Sym}(24)$ and $H \leq_{\max} K \leq_{\max} \mathrm{Alt}(24)$. We obtain the following diagram:



Hence it turns out that, even in these cases, there are at most two maximal subgroups of G containing H. □

Definition 1.4.2 *A subgroup H of $\mathrm{Sym}(n)$ is called orbit-minimal if every proper subgroup of H has strictly more orbits than H has.*

The following proposition gives an upper bound on the number of minimally transitive groups of degree n; a similar result is in [32].

Theorem 1.4.3 *There exists an absolute constant ρ such that the number of minimally transitive subgroups of $\mathrm{Sym}(n)$ is at most $(n\,!)^{\rho}$, for any $n \in \mathbb{N}$.*

Proof. We are going to prove the statement asymptotically on n; then the result holds for all $n \in \mathbb{N}$.
Let X be a minimally transitive subgroup of $\mathrm{Sym}(n)$. By a result in [1], X can be written as $X = \langle Y, g \rangle$ for some solvable subgroup Y of $\mathrm{Sym}(n)$ and some $g \in \mathrm{Sym}(n)$.
We observe that Y can be chosen orbit-minimal in $\mathrm{Sym}(n)$: in fact, if Y is not orbit-minimal, then $\exists\, Z < Y$, orbit-minimal, with the same orbits of Y; $\langle Z, g \rangle$ is transitive and then, by the minimality of X, we obtain $X = \langle Z, g \rangle$.
Our aim is to give an upper bound on the number of the minimally transitive subgroups of $\mathrm{Sym}(n)$; it is equivalent to count all the possible pairs (Y, g), with Y solvable and orbit-minimal and $g \in \mathrm{Sym}(n)$.
Let $d(Y)$ be the minimum number of generators of Y; by [32, Theorem 1.5.], it holds $d(Y) \leq \log n$, for n large enough. Y solvable is contained in some maximal solvable subgroup of $\mathrm{Sym}(n)$; using [32, Lemma 4.1.] we obtain that the number m of maximal solvable subgroups of $\mathrm{Sym}(n)$ is at most $n\,!\,2^{17n}$. By Stirling formula, there exists $\epsilon \in \mathbb{R}$ such that

$$m \leq (n\,!)^{\epsilon}$$

for any n large enough.
Fix M maximal solvable subgroup of $\mathrm{Sym}(n)$; we are calculating the number of the orbit-minimal subgroups of M. Applying [32, Theorem 2.2.] we have $|M| \leq a^n$, $a \in \mathbb{R}$ ($a = \sqrt[3]{24}$); then the orbit-minimal subgroups of M are at most $a^{n \log n} = 2^{n \log n \log a}$. By Stirling formula, for n sufficiently large, it holds $2^{n \log n \log a} \leq (n\,!)^{\delta}$, with $\delta \in \mathbb{R}$.
The number of possible choices for Y in $\mathrm{Sym}(n)$ is at most $(n\,!)^{\epsilon} \cdot (n\,!)^{\delta}$. For the element g we have $n\,!$ choices; then we may conclude that the possible pairs (Y, g) are at most $(n\,!)^{\epsilon+\delta+1}$, for n large enough. □

Remark 1.4.4 *We observe that $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ acts on the set $\Delta_n := \{(a, b) \,|\, 1 \leq a, b \leq n,\ a \neq b\}$ in the following way: $(a, b)g := (ag, bg)$, $\forall g \in G$ and $\forall\, (a, b) \in \Delta_n$. This is a faithful and transitive action of degree $|\Delta_n| = n(n-1)$. Then any subgroup of G is a permutation group of degree $n(n-1)$. Let $T \leq G$ be transitive on I_n and with t orbits in its action on Δ_n; each orbit on Δ_n contains at least n elements, and then we may conclude $t \leq n - 1$.*

Lemma 1.4.5 *Let T be a transitive subgroup of $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$, and denote by t the number of orbits of T on the set Δ_n. Then*

$$|G : T| \geq \frac{t\,!}{2}.$$

Proof. Denote by $C_1, \ldots, C_t$ the orbits of T on Δ_n. Fix $a \in I_n$ and let $K = \mathrm{Stab}_T(a)$. There exists a bijection φ between the set of T-orbits on Δ_n and the set of K-orbits on $I_n - \{a\}$: by transitivity of T on I_n, there is at least one element $(a, c_j) \in C_j$, for each $j \in \{1, \ldots, t\}$; we define $\varphi(C_j)$ the K-orbit on $I_n - \{a\}$ containing the element c_j, and we can easily verify that the map φ so defined is a bijection. We denote by $\Lambda_1, \ldots, \Lambda_t$ the K-orbits and we choose $b_j \in \Lambda_j$, for each $1 \leq j \leq t$. Define the set $\phi := \{b_1, \ldots, b_t\}$; it follows $\mathrm{Alt}(\phi) \cap T = \mathrm{Alt}(\phi) \cap K = \langle 1 \rangle$, and then $|G : T| \geq |\,\mathrm{Alt}(\phi)| = (t\,!)/2$. □

Using Theorem 1.4.3, we obtain a bound concerning the action of G on Δ_n.

Corollary 1.4.6 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and let $\mathcal{P}$ be the set of the partitions of Δ_n whose parts are the orbits of some transitive subgroup of G in its action on Δ_n. Then there exists δ, independent from n, such that*

$$|\mathcal{P}| \leq (n\,!)^{\delta}$$

for any $n \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$. We notice that any transitive subgroup of G contains at least one minimally transitive subgroup; by Theorem 1.4.3, we know that the number of minimally transitive subgroups of G is at most $(n\,!)^{\rho}$, with ρ an absolute constant.
Fix a minimally transitive subgroup X of G. Let $\{\Omega_1, \ldots, \Omega_x\}$ be the set of orbits of X on Δ_n; by Remark 1.4.4, it holds $x \leq n - 1$.
Now the set of orbits on Δ_n of any transitive subgroup of G containing X is obtained as a partition of $\{\Omega_1, \ldots, \Omega_x\}$; so we have to estimate the cardinality of the set S of all partitions of $\{\Omega_1, \ldots, \Omega_x\}$. We can easily prove that there exists an injective function between S and $\mathrm{Sym}(x)$; hence

$$|S| \leq x\,! \leq (n-1)!.$$

Then $|\mathcal{P}| \leq n\,! \cdot (n\,!)^{\rho}$, and we can take $\delta = \rho + 1$ for any $n \in \mathbb{N}$.

□

Now we give a series of bounds for the indices of some subgroups of $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. It turns out that the order of a transitive subgroup of G is in general "small" with respect to $|G|$. First of all we give a result on the primitive subgroups of G.

Lemma 1.4.7 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. If n is large enough and P is a primitive subgroup of G with $\mathrm{Alt}(n) \not\leq P$, then*

$$|G : P|^2 \geq n!.$$

Proof. By a result of Praeger and Saxl (see [31]), any primitive subgroup of $\mathrm{Sym}(n)$, not containing $\mathrm{Alt}(n)$, has order smaller or equal than 4^n; it follows $|P| \leq 4^n$. Then

$$|G : P|^2 \geq |G|^2/(4^n)^2 \geq (n\,!)^2/4(4^n)^2.$$

Then it suffices to prove $n\,! \leq (n\,!)^2/4(4^n)^2$, that is equivalent to verify

$$4^{2n+1} \leq n!.$$

By Stirling formula: $n\,! \sim n^{(n+1)/2}e^{-n}\sqrt{2\pi} \sim 2^{(n+1)/2\,\log n} \sim 2^{n\,\log n/2}$; $4^{2n+1} = 2^{\,4n+2} \Rightarrow 4^{2n+1} \leq n\,!$ asymptotically. □

For the index of the imprimitive subgroups of G we have the following lower bound.

Lemma 1.4.8 *There exists a constant $\sigma \in \mathbb{R}$ such that*

$$|G : H| \geq 2^{\,\sigma n}$$

for each $n \in \mathbb{N}$ and each imprimitive subgroup H of $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$.

Proof. If $H \leq G$ has an imprimitive system of b blocks of cardinality a, then $H \leq \mathrm{Sym}(a) \wr \mathrm{Sym}(b)$ and $|G : H| \geq n!/(a!)^b b! \geq 2^{[(n+1)/2]}$ when $n \geq 8$, as it is noticed in the proof of [28, Lemma 2.1]. □

A stronger lower bound holds under additional hypotheses.

Lemma 1.4.9 *There exists a constant $c \in \mathbb{R}$ such that*

$$|G : H|^c \geq n\,!$$

for each $n \in \mathbb{N}$ and each imprimitive subgroup H of $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ which satisfies one of the following conditions:

1) *$a^2 \leq n$, where a is the cardinality of a block of H;*

2) *the kernel of the action of H on the set of the blocks has order at most $(2a!)^{\frac{n}{2a}}$, where a is the cardinality of a block of H;*

3) *the permutation group induced on a block B by its setwise stabilizer in H is primitive and does not contain $\mathrm{Alt}(B)$.*

Proof. Let $\mathcal{B} = \{B_1, \ldots, B_b\}$ be a set of blocks of imprimitivity for H, with $|B_1| = a$. Since $H \leq \mathrm{Sym}(a) \wr \mathrm{Sym}(b)$, we have $|G : H| \geq n!/(a!)^b b!$. Moreover, as it is noticed in the proof of [28, Lemma 21], for a fixed value of n, $n!/(a!)^b b!$ increases when a decreases; so, in order to prove that the statement holds if 1) is satisfied, it suffices to check that there exists γ_1 such that $(n!)^{(1-1/\gamma_1)} \geq (a!)^b b!$ when n is large enough and $a \sim b \sim \sqrt{n}$. Let x be a natural number; by Stirling formula: $x\,! \sim \sqrt{2\pi x}\,(\frac{x}{e})^x$. Then, for a number x large enough, it holds $(\frac{x}{e})^x \leq x\,! \leq x\,(\frac{x}{e})^x$. We apply this formula to $n\,!$; then we take γ_1 large enough such that

$$\left(\frac{n}{e}\right)^{n-n/\gamma_1} \geq \left(\frac{a^{a+1}}{e^a}\right)^b \frac{b^{b+1}}{e^b}.$$

Denote by $\psi : H \to \mathrm{Sym}(b)$ the permutation representation induced by the action of H on the set of blocks. If 2) holds, then $|H| \leq (2a!)^{\frac{n}{2a}} \cdot b\,!$, and it follows $|G : H| \geq n!/(2 \cdot (2a!)^{b/2} \cdot b!)$. We may suppose $a^2 > n$; to verify that the thesis holds when 2) is satisfied, we have to prove the existence of a constant γ_2 such that $(n!)^{(1-1/\gamma_2)} \geq 2(2a!)^{b/2} b!$, for any n large enough. We know that $\mathrm{Sym}(n)$ contains imprimitive subgroups with order $(a!)^b b!$; therefore $(a!)^{b/2} \leq (n\,!)^{1/2}$. Moreover we observe that, for n sufficiently large, $2^{(1+b/2)} b! \leq (a!)^{b/4}$; then we may take $\gamma_2 = 4$.

We suppose that 3) holds; we want to prove that there exists a constant γ_3 such that $|G : H|^{\gamma_3} \geq n!$. As it is shown in [4, Theorem 1.8], we have $H \leq P \wr \mathrm{Sym}(b)$ with P a primitive subgroup of $\mathrm{Sym}(a)$ which does not

contain $\mathrm{Alt}(a)$. By [31], $|P| \leq 4^a$ so $|G : H| \geq n!/(2 \cdot 4^n \cdot b!)$. We may assume $a^2 > n$; using the Stirling formula, for a large enough, we can prove $2 \cdot 4^n \cdot b! \leq 2 \cdot (2a!)^{b/2} \cdot b!$, and then we can take $\gamma_3 = 4$.
To conclude we take $c = \max(\gamma_1, \gamma_2, \gamma_3) = \max(4, \gamma_1)$, for any n large enough. □

Lemma 1.4.10 *There exists a constant c such that for any imprimitive subgroup H of $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$, n large enough, the following holds. Let $\mathcal{B} = \{B_1, \ldots, B_b\}$ be a set of blocks for H with minimal size, say a. If $|G : H|^c < n!$ then $a^2 \geq n$ and the kernel of the action of H on the blocks of $\mathcal{B}$ contains $(\mathrm{Alt}(a)^b)$.*

Proof. We take c as in Lemma 1.4.9; we want to prove that it satisfies the thesis. Suppose that $|G : H|^c < n!$. We know from the previous lemma that $a^2 > n$. Denote by P be the primitive subgroup of $\mathrm{Sym}(a)$ induced on B_1 by its setwise stabilizer in H and by $\psi : H \to \mathrm{Sym}(b)$ the permutation representation induced by the action of H on the set of blocks; let $J = \psi(H)$. Up to permutation isomorphisms, we may identify H with a subgroup of the wreath product $P \wr J$, with respect to its imprimitive action. In this identification, $\ker \psi = H \cap P^b$, being P^b the base of this wreath product. By Lemma 1.4.9, $\mathrm{Alt}(a) \leq P$. If $\ker \psi \cap (\mathrm{Alt}(a))^b \neq \langle 1 \rangle$ we proceed as described in [22] (p.531). Denote $\ker \psi \cap (\mathrm{Alt}(a))^b = N$. Notice that $H \leq (\mathrm{Sym}(a))^b \wr J$; let $M = (\mathrm{Sym}(a))^b$. For any $j \in \{1, \ldots, b\}$ we define the projection map

$$\pi_j : M \to \mathrm{Sym}(a);$$

$S_j := \left\{ m \in M \mid \pi_j(m) \in \mathrm{Alt}(a),\ \pi_i(m) = 1_{\mathrm{Sym}(a)} \text{ if } i \neq j \right\}$ is isomorphic to $\mathrm{Alt}(a)$, for any j. Since $(S_1 \times \cdots \times S_b) \lhd (\mathrm{Sym}(a))^b \wr J$ and $J = \psi(H)$ is transitive on $\{1, \ldots, b\}$, it follows that for any $i \geq 2$ there exists $h_i \in H$ such that $S_i = S_1^{h_i}$. But $N \leq S_1 \times \cdots \times S_b$ and $N \lhd H$; then, for any i, $\pi_i(N) = (\pi_1(N))^{h_i}$, and so it follows $\pi_i(N) \cong \pi_j(N)$, for any $1 \leq i, j \leq b$. Consider one of this projection, for example $\pi_1(N)$; it is normalized by the permutation group induced by $\mathrm{Stab}_J(B_1)$ on B_1, that is isomorphic to P. For $n \geq 5$ we can conclude $\pi_j(N) \cong \mathrm{Alt}(a)$, with $1 \leq j \leq b$; hence N is a subgroup of $(\mathrm{Alt}(a))^b$ with all the b projections isomorphic to $\mathrm{Alt}(a)$, and N is normalized by H.

If we suppose $N \neq ((\mathrm{Alt}(a))^b$, then N has to be of the following form. Let $I_1, \ldots, I_t$ be a system of imprimitivity for the action of H on the set $\mathcal{B}$; hence $t \leq \frac{b}{2}$. Then $N = D_1 \times \cdots \times D_t$, where D_i, for any $1 \leq i \leq t$, is a full diagonal subgroup of $\prod_{j \in I_i} \pi_j(N)$ (i.e. the resctriction to the subgroup D_i of the projection $\prod_{j \in I_i} \pi_j(N) \to \pi_k(N)$ is an isomorphism for any $k \in I_i$). Hence $D_i \cong \mathrm{Alt}(a)$, for any $1 \leq i \leq t$, and $N \cong (\mathrm{Alt}(a))^t$, with $t \leq \frac{b}{2}$.
Therefore, if $(\mathrm{Alt}(a))^b \not\leq \ker \psi$, then $|\ker \psi| \leq (a!/2)^{b/2} 2^b$; but this, by Lemma 1.4.9, would imply $|G : H|^c \geq n!$, a contradiction. □

Chapter 2

The probabilistic zeta function

Let G be a group. Denote by $P_G(t)$ the probability that t randomly chosen elements of G generate G itself. The study of $P_G(t)$ has been developed by many authors when G is a finite group (see for examples [13], [3], [8]), and later extended to profinite groups (see [25] and [2]).

2.1 The finite case

Let G be a finite group. To estabilish the probability that a random t-ple of elements of G generates G itself, we simply calculate the number of systems of generators of G.

Definition 2.1.1 *Define the function $\phi_G : \mathbb{N} \to \mathbb{N} \cup \{0\}$ in the following way: for any $t \in \mathbb{N}$, $\phi_G(t)$ is the number of t-bases of G, that is, ordered t-tuples $(g_1, \ldots, g_t)$ of elements of G that generate G. This function is called the Eulerian function associate to G.*

Remark 2.1.2 *The Eulerian function ϕ_G was introduced by Hall in [13]; in this paper he proved that*

$$\phi_G(t) = \sum_{H \leq G} \mu(H, G)|H|^t$$

where μ is the Möbius function on the subgroup lattice $\mathcal{L}_G$ (see Section 1.2).

For any $t \in \mathbb{N}$, the probability $P_G(t)$ that a random t-tuple of elements of G generates G is given by

$$P_G(t) = \frac{\phi_G(t)}{|G|^t}.$$

Then, by the previous remark, we may write

$$P_G(t) = \sum_{H \leq G} \frac{\mu(H,G)}{|G:H|^t} \tag{2.1}$$

We may interpolate the integer function P_G and define $P_G(s)$ for any complex variable s. By rearranging the addends in (2.1) we obtain a Dirichlet polynomial as follows (see also [13], [25], [34]):

$$P_G(s) := \sum_{n \in \mathbb{N}} \frac{a_n}{n^s}$$

where

$$a_n := \sum_{|G:H|=n} \mu(H,G).$$

Definition 2.1.3 *The multiplicative inverse of the complex function P_G, so defined, is called the probabilistic zeta function of G.*

Given a normal subgroup N of G we define a Dirichlet poynomial $P_{G,N}(s)$ as follows:

$$P_{G,N}(s) := \sum_{n \in \mathbb{N}} \frac{b_n}{n^s} \qquad \text{with} \qquad b_n := \sum_{\substack{|G:H|=n \\ HN=G}} \mu(H,G).$$

As it is shown in [3, Section 2.2], it holds

$$P_G(s) = P_{G/N}(s) P_{G,N}(s) \tag{2.2}$$

If G is an almost simple group, i.e. $S \leq G \leq \mathrm{Aut}(S)$ with S a non abelian simple group, and G/S has prime order, then, as it is proved in [7] p.288,

$$P_S(s) - P_{G,S}(s) = \sum_{H \leq S} \frac{\mu(H,S) + \mu(H,G)}{|G:H|^s}.$$

In particular we have

Corollary 2.1.4 ([7]) *Suppose G an almost simple group, with $\operatorname{soc} G = S$, and that G/S has prime order; $P_S(s) = P_{G,S}(s)$ if $\mu(H,S) + \mu(H,G) = 0$ for any $H \leq S$.*

Remark 2.1.5 *We will use this corollary when G and S are respectively the Symmetric group and the Alternating group of degree n (see Chapter 3).*

2.2 The profinite case

To discuss this part we often use definitions and remarks contained in [25] and [26]. Let G be an infinite group. We ask what is the probability that t randomly chosen elements of G generate G itself. In order for our question to make sense, we have to define a measure on G; this leads us naturally to the class of profinite groups, i.e. inverse limits of finite groups. Such groups are compact topological groups, with the topology induced by the discrete topology on the finite groups in the given inverse system; therefore they also have a *Haar measure* (see [11, Chapter 16]). For some properties of profinite groups, see for example [9]. The finite Haar measure ν on G is normalized so that G has measure 1, and then we may consider G as a probability space: this means that the measure of a subset X of G express the probability that a random element of G lies in X. Denote by $X_G(t)$ the set of t-ples generating G; we note that $X_G(t)$ is a closed set in $G^{(t)}$, and then it is measurable. Then the probability that a random t-ple of elements generates G is formally defined as

$$P_G(t) = \nu\left\{(x_1, \ldots, x_t) \in G^{(t)} \mid \langle x_1, \ldots, x_t \rangle = G\right\} = \nu(X_G(t)),$$

where ν denotes also the product measure on $G^{(t)}$ and $\langle x_1, \ldots, x_t \rangle$ means the closed subgroup topologically generated by the set $(x_1, \ldots, x_t)$. Thus $0 \leq P_G(t) \leq 1$, and if $P_G(t) > 0$ then the minimal number $d(G)$ of generators of G is smaller or equal than t.

Remark 2.2.1 *We observe that if G is finite we have $\nu(X) = |X|/|G|$ for each subset X; so the concept of probability in profinite groups reduces to the usual one in finite groups, studied in Section 2.1.*

Remark 2.2.2 *Of course, a profinite group (unless it is finite) can be finitely generated only in the topological sense, i.e. be the closure of the discrete subgroup generated by some finite subsets. In other words, a subset X of G generates it in this sense, if and only if the image of X in any finite factor group of G generates this factor group. From now on we interpret finite generation of profinite groups in this sense.*

Let G be a finitely generated profinite group; denote by $\mathcal{N}$ the set of all open normal subgroups of G. As it is showed in [18], if X is a closed subset

of G, then $X = \bigcap_{i=1}^{\infty} XN_i$, where $N_1 > N_2 > \cdots$ is a descending chain in $\mathcal{N}$. By the properties of the Haar measure ν we have

$$\nu(X) = \lim_{i\to\infty} \nu(XN_i) = \inf_{N\in\mathcal{N}} \nu(XN).$$

For each $N \in \mathcal{N}$ the set XN is the union of $|XN/N|$ cosets of N; so $\nu(XN) = |XN/N|\nu(N) = |XN/N|/|G : N|$, and then

$$\nu(X) = \inf_{N\in\mathcal{N}} \frac{|XN/N|}{|G/N|} \tag{2.3}$$

Definition 2.2.3 *A set of open subgroups of G such that each open subgroup contains one of them is called subgroup basis of G.*

Recall that open subgroups of profinite groups are of finite index, and $X_G(t)$ is closed; hence using (2.3) the following statement can be proved.

Theorem 2.2.4 ([25]) *Let G be a finitely generated profinite group. Then*

$$P_G(t) = \inf\left\{P_{G/N}(t) \mid N \in \mathcal{N}\right\}.$$

Moreover, if $\{N_i\}_{i\in\mathbb{N}}$ is a subgroup basis of G consisting of normal subgroups, then

$$P_G(t) = \inf_{i\in\mathbb{N}} P_{G/N_i}(t).$$

Definition 2.2.5 *A profinite group G is positively finitely generated (*PFG*), if for some t, the probability $P_G(t)$ is positive.*

Notice that a PFG group is obviously finitely generated. In [25] Mann formulated the following conjecture:

Conjecture 2.2.6 (Mann, 1996) *If G is a* PFG *group, then the integer function P_G can be interpolated in a natural way to an analytic function $P_G(s)$, defined for all s in some right half-plane of the complex plane.*

We call *probabilistic zeta function* of G the multiplicative inverse of a complex function $P_G(s)$ with these properties.

Remark 2.2.7 *If G is finite, then we already know (see Section 2.1) that $P_G(t) = \sum_{H\leq G} \mu(H,G)/|G : H|^t$ for any positive integer t, and this function is interpolated by the complex function $P_G(s) = \sum_{H\leq G} \mu(H,G)/|G : H|^s$.*

Mann proposed the following approach to find a candidate for the conjectured function. Let G be a finitely generated profinite group. Firts of all we define by recursion the Möbius number for any finite index subgroup H of G:

$$\mu(H,G) = \begin{cases} 1 & \text{if } H = G \\ -\sum_{H < K \leq G} \mu(K,G) & \text{otherwise.} \end{cases}$$

Remark 2.2.8 *As we have already observed when G is finite (see Remarks 1.2.2 and 1.2.3), also for the Möbius function associated to a profinite group the following properties hold:*

1) *if $H < G$ has finite index, then $\mu(H,G) \neq 0$ only if H is an intersection of maximal subgroups of G;*

2) *$|\mu(H,G)|$ is bounded by the number of ways to express H as an intersection of maximal subgroups.*

Now define a series associated to G in the following way:

$$\sum_{H \leq_o G} \frac{\mu(H,G)}{|G:H|^s} \qquad (S)$$

where s is a complex variable, and H ranges over all open subgroups of G, arranged in some order. Now let $\{N_i\}_{i \in \mathbb{N}}$ be a normal subgroup basis, with $\bigcap_{i=1}^{\infty} N_i = \langle 1 \rangle$. Using Remark 2.2.7 and Theorem 2.2.4, we obtain

$$P_G(t) = \lim_{i \to \infty} P_{G/N_i}(t) = \lim_{i \to \infty} \left(\sum_{N_i \leq H \leq G} \frac{\mu(H,G)}{|G:H|^t} \right).$$

Then the series (S), with the above insertion of parentheses, converges, for a positive integer t, to $P_G(t)$. It follows that (S), with this insertion of parentheses, is a candidate for the function $P_G(s)$ of the Conjecture 2.2.6. So, in order to prove the conjecture of Mann, we have to estabilish if this series (with this insertion of parentheses) converges in some half plane.

Remark 2.2.9 *Note that different choices of the subgroup basis $\{N_i\}_{i \in \mathbb{N}}$ lead to different groupings of the terms in (S); so we have also to know if two different bases lead to the same function. But we also notice that if (S) is absolutely convergent, then its sum is independent from the ordering of the summands; in this case the function $P_G(s)$ would be independent*

from the choice of the basis $\{N_i\}_{i\in\mathbb{N}}$*, and therefore it would follow that* $P_G(s) = \sum_{H\leq_o G} \mu(H,G)/|G:H|^s$*, for any* s *in the convergency domain.*

In 2005 Mann has formulated a conjecture on the convergence of (S) for PFG groups.

Conjecture 2.2.10 (Mann, 2005) *Let* G *a* PFG *group. Then the infinite series* (S) *converges absolutely in some right half plane.*

Definition 2.2.11 *Let* G *be a finitely generated profinite group. For any* $n \in \mathbb{N}$*, denote by* $b_n(G)$ *the number of subgroups* H *of* G *with* $|G:H| = n$ *and* $\mu(H,G) \neq 0$*. We say:*

- $b_n(G)$ *grows polynomially if there exists* α *such that* $b_n(G) \leq n^\alpha$*, for any* $n \in \mathbb{N}$*;*
- $|\mu(H,G)|$ *grows polynomially if there exists* β *such that, for any finite index subgroup* H *of* G*,* $|\mu(H,G)| \leq |G:H|^\beta$*.*

In [26] Mann proved the following statement.

Theorem 2.2.12 *Let* G *be a finitely generated profinite group. The series* (S) *converges absolutely in some half plane if and only if both* $|\mu(H,G)|$ *and* $b_n(G)$ *grow polynomially.*

Then Conjecture 2.2.10 can be reformulated as: if G is a PFG group, then we have polynomial bounds for $b_n(G)$ and $|\mu(H,G)|$. To discuss this conjecture we need to recall an important result of Mann and Shalev on the behaviour of maximal subgroups of PFG groups.

Definition 2.2.13 *For any* $n \in \mathbb{N}$*, denote by* $m_n(G)$ *the number of maximal subgroups of* G *of index* n*. We say that* G *has polynomial maximal subgroup growth (*PMSG*) if there exists a constant* c *such that* $m_n(G) \leq n^c$*, for any* $n \in \mathbb{N}$*.*

We observe thay if $b_n(G)$ grows polynomially, then G has PMSG. Moreover it holds:

Theorem 2.2.14 (Mann-Shalev, [27]) G *is* PFG *if and only if* G *has* PMSG.

Remark 2.2.15 *Using Remark 2.2.8, we notice that $b_n(G)$ is bounded in terms of the number of maximal subgroups of G of index dividing n, and $|\mu(H,G)|$ can be bounded in terms of the number of maximal subgroups of G containing H.*

Some interesting bounds can be obtained with these arguments (see for example [25, Theorem 21]), but even if one assumes that G has PMSG, it is not known whether this implies that there is a polynomial bound for the number of maximal intersections of G of index at most n.

Remark 2.2.16 *The Conjecture 2.2.10 has been proved in [26], [23] and [21] for profinite completions of arithmetic groups satisfying the congruence subgroup property, finitely generated prosolvable groups, adelic groups and groups with polynomial subgroup growth (*PSG *groups). These results depend on the fact that we have a better description of the subgroups with non trivial Möbius function: in all these cases it can be proved that if $\mu(H,G) \neq 0$, then not only H is an intersection of maximal subgroups, but also these maximal subgroups can be choosen with additional "good" properties.*

In [19] Lucchini has proved that in order to decide whether a PFG group G satisfies Conjecture 2.2.10, it suffices to investigate the behaviour of the Möbius function on the subgroup lattice of the finite monolithic groups that appear as epimorphic images of G. Recently Lucchini has obtained a stronger result, which allows us to deal only with almost simple groups; a paper with this result is in preparation. We now explain more precisely these argumentations; we start giving some definitions.

Definition 2.2.17 *Let L be a finite monolithic group (i.e. a group with a unique minimal normal subgroup) with non abelian socle; then it holds $\operatorname{soc} L = S_1 \times \cdots \times S_r$, where the S_i's are all isomorphic simple groups. Denote by X_L the subgroup of $\operatorname{Aut} S_1$ induced by the conjugation action of $N_G(S_1)$ on S_1; this X_L is a finite almost simple group, uniquely determined by L.*

Theorem 2.2.18 (Reduction theorem) *Let G be a* PFG *group and we denote by $\Lambda(G)$ the set of finite monolithic groups L with $\operatorname{soc} L$ non abelian and L an epimorphic image of G. Moreover if $L \in \Lambda(G)$, let $b_n^*(X_L)$ be the*

number of subgroups K of X_L such that $|X_L : K| = n$, $\mu(K, X_L) \neq 0$ and $K \operatorname{soc} X_L = X_L$. Then the followings are equivalent.

(1) There exist two constants γ_1 and γ_2 such that

$$b_n(G) \leq n^{\gamma_1} \quad \text{and} \quad |\mu(H, G)| \leq |G : H|^{\gamma_2}$$

for each $n \in \mathbb{N}$ and each open subgroup H of G.

(2) There exist two constants c_1 and c_2 such that

$$b_n^*(X_L) \leq n^{c_1} \quad \text{and} \quad |\mu(Y, X_L)| \leq |X_L : Y|^{c_2}$$

for each $L \in \Lambda(G)$, each $n \in \mathbb{N}$ and each $Y \leq X_L$ with $Y \operatorname{soc} X_L = X_L$.

This theorem and Theorem 2.2.14 allow us to reformulate Conjecture 2.2.10 of Mann as follows.

Conjecture 2.2.19 *There exists a constant c such that if X is a finite almost simple group, then $b_n^*(X) \leq n^c$ and $|\mu(Y, X)| \leq |X : Y|^c$ for each $n \in \mathbb{N}$ and each $Y \leq X$ with $Y \operatorname{soc} X = X$.*

In Chapter 4 we will verify that this conjecture is satisfied by the Alternating and Symmetric groups; in fact we will prove the followings:

Theorem 1 *There exists an absolute constant α such that for any $n \in \mathbb{N}$, if $X \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $m \in \mathbb{N}$, then $b_m(X) \leq m^\alpha$.*

Theorem 2 *There exists an absolute constant β such that for any $n \in \mathbb{N}$, if $X \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $Y \leq X$, then $|\mu(Y, X)| \leq |X : Y|^\beta$.*

These theorems imply:

Corollary 2.2.20 *If G is a PFG group and for each open normal subgroup N of G, all the composition factors of G are either abelian or Alternating groups, then*

- *there exists γ_1 such that $|\mu(H, G)| \leq |G : H|^{\gamma_1}$ for each open subgroup H of G;*
- *there exists γ_2 such that $b_n(G) \leq n^{\gamma_2}$ for each $n \in \mathbb{N}$.*

By this corollary, we notice that, for example, $G = \prod_n (\mathrm{Alt}(n))^n$ satisfies the Conjecture 2.2.10, because G is PFG, as it is proved in [16].
From [19, Theorem 9] it can be deduced the following statement:

Theorem 2.2.21 *Let $G = \prod_i S_i$, where the S_i's are finite nonabelian simple groups; suppose that G is d-generated and that there exists a constant c with the following property: for any i and for any $Y \leq S_i$, $|\mu(Y, S_i)| \leq |S_i : Y|^c$. Then*

$$|\mu(H, G)| \leq |G : H|^{\epsilon}$$

for each open subgroup H of G, where $\epsilon = \max(d, c) + 1$.

Combined Theorem 2 and Theorem 2.2.21, it follows:

Corollary 2.2.22 *Let $G = \prod_i A_i$, where the A_i's are Alternating groups; suppose that G is d-generated. Then*

$$|\mu(H, G)| \leq |G : H|^{\max(d, \beta)+1}$$

with β as in Theorem 2.

We have already noted that if $b_n(G)$ grows polynomially, then G must be a PFG group. Using Corollary 2.2.22, we observe that a group G in which $|\mu(H, G|$ is bounded by a polynomial function in the index of H is not necessarily PFG. An example is $G = \prod_{n \geq 5} (\mathrm{Alt}(n))^{n!/8}$: G is 2-generated but not PFG (see [16]), and by Corollary 2.2.22 we have

$$|\mu(H, G)| \leq |G : H|^{\max(2, \beta)+1}$$

for each open subgroup H of G.

Chapter 3

Maximal subgroups of the Alternating and Symmetric groups

3.1 A conjecture of Boston and Mann

Let n be a natural number. Denote by $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ respectively the finite Symmetric group and the finite Alternating group of degree n. For $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ we can define the complex functions $P_{\mathrm{Sym}(n)}$ and $P_{\mathrm{Alt}(n)}$, as described in Section 2.1. Then, using formula (2.2), we obtain

$$\begin{aligned} P_{\mathrm{Sym}(n)}(s) &= P_{\mathrm{Sym}(n)/\,\mathrm{Alt}(n)}(s) \cdot P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s) = \\ &= P_{C_2}(s) \cdot P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s). \end{aligned}$$

Let G be a finite group. In a recent work Lucchini and Massa have proved that there exist explicit criterions to recognize whether the factor group $G/\mathrm{Frat}(G)$ is isomorphic to $\mathrm{Alt}(n)$ (with $n \geq 5$) only looking at the coefficients of $P_G(s)$. Using these results they have been able to verify that if $P_G(s) = P_{\mathrm{Sym}(n)}(s)$, with $n \geq 5$, then either $G/\mathrm{Frat}(G) \cong \mathrm{Sym}(n)$ or $G/\mathrm{Frat}(G) \cong \mathrm{Alt}(n) \times C_2$ ([24, Theorem 1.4.]).

Question We want to investigate for which values of n it holds

$$P_{\mathrm{Sym}(n)}(s) = P_{\mathrm{Alt}(n)\times C_2}(s) = P_{\mathrm{Alt}(n)}(s) \cdot P_{C_2}(s) \tag{3.1}$$

This is equivalent to ask when

$$P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s) = P_{\mathrm{Alt}(n)}(s).$$

The probabilistic zeta functions of $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)\times C_2$ can be computed with GAP ([12]) when n is small ($n < 12$): it turns out that (3.1) holds for $n = 2, 5, 6, 10$ but not for $n = 3, 4, 7, 8, 9, 11$, as it has been already noticed by Boston in [2]. In this paper, Boston has presented an interesting conjecture, formulated with Mann, to estabilish when (3.1) holds.

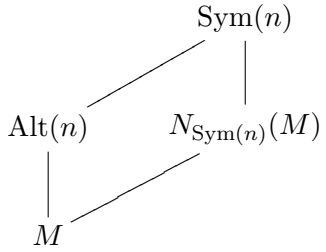
Conjecture 3.1.1 (Boston, Mann) *The validity of the equality* (3.1)*, for* $n \geq 5$*, reflects the non existence of maximal subgroups of* $\mathrm{Alt}(n)$ *which coincide with their normalizers in* $\mathrm{Sym}(n)$*.*

We will study the conjecture of Boston and Mann; we will prove that it is true when $n = p$, for any prime $p \geq 5$. But it doesn't hold in general; in fact we will show counterexamples to the conjecture. First of all we observe some facts, that will be useful in the next; from now on we consider $n \geq 5$.

Remark 3.1.2 *Each maximal subgroup* M *of* $\mathrm{Alt}(n)$ *is contained in the normalizer* $N_{\mathrm{Sym}(n)}(M)$*, which is a proper subgroup of* $\mathrm{Sym}(n)$*, different from* $\mathrm{Alt}(n)$*. If* $N_{\mathrm{Sym}(n)}(M) \neq M$*, we can verify that* $N_{\mathrm{Sym}(n)}(M)$ *is the unique maximal subgroup of* $\mathrm{Sym}(n)$*, different from* $\mathrm{Alt}(n)$*, that contains* M*. In fact, we suppose that* N *is a maximal subgroup of* $Sym(n)$*, different from* $\mathrm{Alt}(n)$*, and that* $N \geq M$*; then* $\mathrm{Alt}(n)N = \mathrm{Sym}(n)$ *and*

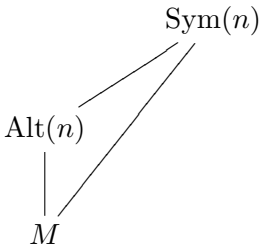
$$\frac{N}{N \cap \mathrm{Alt}(n)} = \frac{N}{M} \cong \frac{\mathrm{Sym}(n)}{\mathrm{Alt}(n)}.$$

Therefore $|N : M| = 2 \Rightarrow M \lhd N \leq N_{\mathrm{Sym}(n)}(M)$*. But* N *is maximal in* $\mathrm{Sym}(n)$*, and then we may conclude* $N = N_{\mathrm{Sym}(n)}(M)$*. So we have the following diagram:*



In this situation, we observe: $\mu(M, \mathrm{Alt}(n)) = -1$ *and* $\mu(M, \mathrm{Sym}(n)) = 1$*.*

If $N_{\mathrm{Sym}(n)}(M) = M$*, then we have:*



with $\mu(M, \mathrm{Alt}(n)) = -1$ *and* $\mu(M, \mathrm{Sym}(n)) = 0$.
The conjecture of Boston and Mann state that there exists M *such that* $N_{\mathrm{Sym}(n)}(M) = M$ *if and only if* $P_{\mathrm{Sym}(n)}(s) \neq P_{\mathrm{Alt}(n)}(s) \cdot P_{C_2}(s)$.

Remark 3.1.3 *If* M *is an intransitive or imprimitive maximal subgroup of* $\mathrm{Alt}(n)$*, then* $M \neq N_{\mathrm{Sym}(n)}(M)$*. We are going to justify this assertion.*
Any intransitive maximal subgroup of $\mathrm{Alt}(n)$ *is of the form*

$$(\mathrm{Sym}(a) \times \mathrm{Sym}(b)) \cap \mathrm{Alt}(n)$$

with $\mathrm{Sym}(a) \times \mathrm{Sym}(b)$ *an intransitive maximal subgroup of* $\mathrm{Sym}(n)$*. In fact we observe that any subgroup isomorphic to* $\mathrm{Sym}(a) \times \mathrm{Sym}(b)$ *in* $\mathrm{Sym}(n)$*, with* $a + b = n$*, is not contained in* $\mathrm{Alt}(n)$*: we assume that* a *is equal or bigger than* 2*, and then* $\mathrm{Sym}(a) \not\leq \mathrm{Alt}(n)$*. Hence the map* $M \mapsto N_{\mathrm{Sym}(n)}(M)$ *induces a bijection between intransitive maximal subgroups of* $\mathrm{Alt}(n)$ *and* $\mathrm{Sym}(n)$*. Any imprimitive maximal subgroup of* $\mathrm{Alt}(n)$ *is of the form*

$$(\mathrm{Sym}(a) \wr \mathrm{Sym}(b)) \cap \mathrm{Alt}(n)$$

where $\mathrm{Sym}(a) \wr \mathrm{Sym}(b)$ *is an imprimitive maximal subgroup of* $\mathrm{Sym}(n)$*. As above, it is easy to prove that any subgroup of* $\mathrm{Sym}(n)$ *isomorphic to* $\mathrm{Sym}(a) \wr \mathrm{Sym}(b)$*, with* $ab = n$*, is not contained in* $\mathrm{Alt}(n)$ *(in fact* $a \geq 2$*). Then there exists a bijection between maximal imprimitive subgroups of* $\mathrm{Alt}(n)$ *and* $\mathrm{Sym}(n)$*: to each maximal imprimitive subgroup of* $\mathrm{Alt}(n)$ *corresponds its normalizer in* $\mathrm{Sym}(n)$*.*

3.2 The case $n = p$

We are supposing p a prime, with $p \geq 5$.

Remark 3.2.1 *Each affine maximal subgroup of* $\mathrm{Sym}(p)$ *is isomorphic to* $C_p \rtimes C_{p-1}$*; then its intersection with* $\mathrm{Alt}(p)$ *is isomorphic to* $C_p \rtimes C_{(p-1)/2}$*. Hence any affine maximal subgroup* M *of* $\mathrm{Alt}(p)$ *is a subgroup of the form* $C_p \rtimes C_{(p-1)/2}$*, and it does not coincide with its normalizer in* $\mathrm{Sym}(p)$*. Moreover we note that any affine subgroup of* $\mathrm{Alt}(p)$ *is of the form* $C_p \rtimes C_t$*, with* C_t *a subgroup of* $C_{(p-1)/2}$*.*

By [29, Theorem 2] we know that any transitive subgroup T of $\mathrm{Sym}(p)$ has a simple normal subgroup S and T/S is cyclic; all the possibilities for S are listed in [29, Table I]. By using this list, we can deduce that if $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$, for any couple of natural numbers (q, d), with $q > 4$ if $d = 2$, then $\mathrm{Sym}(p)$ contains only transitive subgroups of affine type. On the other hand, if $p = 11$, $p = 23$ or $p = (q^d - 1)/(q - 1) > 5$, then $\mathrm{Sym}(p)$ contains some almost simple transitive subgroups but, as it is proved in [29, Corollary 3], these subgroups are all contained in $\mathrm{Alt}(p)$. Then, also for these values of the degree p, it results that $\mathrm{Sym}(p)$ contains only transitive subgroups of affine type. Denote by $\mathcal{M}_{\mathrm{Sym}(p)}$ the set of all the intransitive and affine maximal subgroups of $\mathrm{Sym}(p)$, and by $\mathcal{M}_{\mathrm{Alt}(p)}$ the set of the intransitive and affine maximal subgroups of $\mathrm{Alt}(p)$. We notice that, for the previous considerations, the set $\mathcal{M}_{\mathrm{Sym}(p)}$ coincides with the set of all maximal subgroups of $\mathrm{Sym}(p)$, different from $\mathrm{Alt}(p)$, for any p prime. Moreover, if M is an affine or an intransitive maximal subgroup of $\mathrm{Alt}(p)$, then, by Remark 3.1.3 and Remark 3.2.1, $M \neq N_{\mathrm{Sym}(p)}(M)$; the normalizer $N_{\mathrm{Sym}(p)}(M)$ is a maximal subgroup of $\mathrm{Sym}(p)$, of the same type of M. Hence there exists a bijection between $\mathcal{M}_{\mathrm{Sym}(p)}$ and $\mathcal{M}_{\mathrm{Alt}(p)}$: to each $M \in \mathcal{M}_{\mathrm{Alt}(p)}$ corresponds $N_{\mathrm{Sym}(p)}(M) \in \mathcal{M}_{\mathrm{Sym}(p)}$.

Lemma 3.2.2 *Let* $H < \mathrm{Alt}(p)$*,* $H \neq \langle 1 \rangle$*, such that if* N *is a maximal subgroup of* $\mathrm{Alt}(p)$ *with* $H \leq N$*, then* $N \in \mathcal{M}_{\mathrm{Alt}(p)}$*. It holds*

$$\mu(H, \mathrm{Sym}(p)) = -\mu(H, \mathrm{Alt}(p)).$$

Proof. If H is not intersection of elements of $\mathcal{M}_{\mathrm{Alt}(p)}$ then, by the bijection between $\mathcal{M}_{\mathrm{Sym}(p)}$ and $\mathcal{M}_{\mathrm{Alt}(p)}$, it results that H is not also intersection of elements of $\mathcal{M}_{\mathrm{Sym}(p)}$; hence it follows $\mu(H, \mathrm{Alt}(p)) = \mu(H, \mathrm{Sym}(p)) = 0$ (see Remark 1.2.2). Then we have to calculate $\mu(H, \mathrm{Alt}(p))$ and $\mu(H, \mathrm{Sym}(p))$ when H is an intersection of elements of $\mathcal{M}_{\mathrm{Alt}(p)}$.

We consider $H \in \mathcal{M}_{\mathrm{Alt}(p)}$ a maximal subgroup of $\mathrm{Alt}(p)$; H is obtained as the intersection between $N_{\mathrm{Sym}(p)}(H)$ and $\mathrm{Alt}(p)$. As we have already observed in Remark 3.1.2, we obtain $\mu(H, \mathrm{Sym}(p)) = -\mu(H, \mathrm{Alt}(p))$.
We suppose now H an intersection of maximal subgroups in $\mathcal{M}_{\mathrm{Alt}(p)}$, but H not maximal in $\mathrm{Alt}(p)$. In other words H is an intersection of some maximal affine or intransitive subgroups of $\mathrm{Sym}(p)$ with $\mathrm{Alt}(p)$. We observe that the intersection of two maximal affine subgroups of $\mathrm{Sym}(p)$ is intransitive, and then it follows that H is intransitive. Applying the closure theorem of Crapo to $\mathcal{L}_{\mathrm{Sym}(p)}$, we obtain

$$\sum_{\substack{T \leq \mathrm{Sym}(p) \\ \bar{T} = \mathrm{Sym}(p)}} \mu(H, T) = \begin{cases} \bar{\mu}(H, \mathrm{Sym}(p)) & \text{if } H \text{ is closed in } \mathcal{L}_{\mathrm{Sym}(p)} \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

If doesn't esixts any transitive subgroup $T \notin \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$ such that $H \leq T$, then H has the form

$$(\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_k)) \cap \mathrm{Alt}(p)$$

for some partition $\{\Omega_1, \cdots, \Omega_k\}$ of $\{1, \ldots, p\}$, with $2 < k < p-1$ (in fact $H \neq \langle 1 \rangle$).
We observe that $H \neq \mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_k)$, and hence H is not closed in $\mathcal{L}_{\mathrm{Sym}(p)}$. From (3.2)

$$\mu(H, \mathrm{Sym}(p)) + \mu(H, \mathrm{Alt}(p)) = 0.$$

Then we may suppose that there exists at least one transitive subgroup $T \notin \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$ such that $H \leq T$.
We have $T \leq A$, with A a maximal affine subgroup of $\mathrm{Sym}(p)$; so H is an intransitive subgroup of A. It holds $A = P \rtimes K = N_{\mathrm{Sym}(p)}(P)$, for some $P \cong C_p$ and $K \cong C_{p-1}$; then H is a cyclic subgroup of order dividing $p-1$. By hypothesis, $H \neq \langle 1 \rangle$, and then H is not closed in $\mathcal{L}_{\mathrm{Sym}(p)}$: the cyclic closed subgroups of $\mathrm{Sym}(p)$ have order 2, and fix $p-2$ elements; if H has order 2, it fix only one element. From (3.2)

$$\mu(H, \mathrm{Sym}(p)) = -\mu(H, \mathrm{Alt}(p)) - \sum_{\substack{T \ trans. \\ H \leq T < \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(H, T) \tag{3.3}$$

We are considering $H < A$; the transitive subgroups containing H and contained in A are of the form $P \rtimes R$, with $H \leq R \leq K^s$ for some $s \in P$. The subgroup P has p complements in A pairwise disjoint. Then H is contained only in one complement of P; without lost of generality we may assume $H \leq K$ and $H \leq R \leq K$.
Any maximal affine subgroup $\bar{A}$ of $\mathrm{Sym}(p)$ containing H is conjugated to A in $\mathrm{Sym}(p)$. We can repeat for $\bar{A} = \bar{P} \rtimes \bar{K}$ the same procedure; so we may assume $H \leq \bar{K}$, with $\bar{K} \cong C_{p-1}$. Denote by t the number of the maximal affine subgroups of $\mathrm{Sym}(p)$ containing H, that is equivalent to the number of subgroups of order p normalized by H. We recall that the intersection of two maximal affine subgroups is intransitive; then any transitive subgroup T that appears in (3.3), is contained in only one maximal affine subgroup of $\mathrm{Sym}(p)$. It follows

$$\sum_{\substack{T \text{ trans.} \\ H \leq T < \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(H,T) = t \cdot \sum_{\substack{T \text{ trans.} \\ H \leq T \leq A}} \mu(H,T) = t \cdot \sum_{H \leq R \leq K} \mu(H,PR).$$

Fix R; we proceed to calculate $\mu(H,PR)$. We consider the lattice L of subgroups of PR containing H: in this lattice $\hat{0} = H$ and $\hat{1} = PR$. We notice that the set $(PH)^{\perp} = \{X \in L \,|\, X \cap PH = H \text{ and } \langle X, PH \rangle = PR\}$ of the complements to PH in L is reduced to the element R; applying the complement theorem of Crapo to L (see Section 1.1), we obtain

$$\mu(H,PR) = \sum_{\bar{R} \in (PH)^{\perp}} \mu(H,\bar{R}) \cdot \mu(\bar{R},PR) = \mu(H,R) \cdot \mu(R,PR).$$

We are supposing $H \neq \langle 1 \rangle$; then $R \neq \langle 1 \rangle$ and R is a maximal subgroup of PR. It holds $\mu(R,PR) = -1$; hence

$$\mu(H,PR) = -\mu(H,R).$$

$H \lhd R$, then $\mu(H,R) = \mu(\langle 1 \rangle, R/H)$. Let $|H| = h$ and $|R| = r$; R/H is cyclic, then, by Lemma 1.2.7, it follows

$$\mu(H,PR) = -\mu(\langle 1 \rangle, R/H) = -\mu(r/h).$$

We obtain

$$\sum_{\substack{T \text{ trans.} \\ H \leq T < \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(H,T) = -t \cdot \sum_{h|r \text{ and } r|p-1} \mu(r/h).$$

Set $\bar{r} = r/h$, for any r such that $h|r$ and $r|p-1$; then we observe that holds $\sum_{h|r \text{ and } r|p-1} \mu(r/h) = \sum_{\bar{r}|((p-1)/h)} \mu(\bar{r})$. Moreover $(p-1)/h \neq 1$, because $H \leq \mathrm{Alt}(p)$, and so, as observed in Remark 1.2.6, it follows

$$\sum_{\bar{r}|((p-1)/h)} \mu(\bar{r}) = 0.$$

Then, from (3.3), we may conclude $\mu(H, \mathrm{Sym}(p)) + \mu(H, \mathrm{Alt}(p)) = 0$. □

Suppose $p \neq 11, 23$ and $p \neq (q^d - 1)/(q-1)$ (with $q > 4$ if $d = 2$). Then $\mathrm{Alt}(p)$ does not contain any almost simple transitive subgroup; each maximal subgroup M of $\mathrm{Alt}(p)$ is intransitive or affine (see [29]). Then $\mathcal{M}_{\mathrm{Alt}(p)}$ is the set of all maximal subgroups of $\mathrm{Alt}(p)$, and each maximal subgroup of $\mathrm{Alt}(p)$ doesn't coincide with its normalizer in $\mathrm{Sym}(p)$. Hence to verify the validity of the conjecture, we have to prove the following.

Theorem 3.2.3 *Let $p \geq 5$ prime, with $p \neq 11, 23$ and $p \neq (q^d - 1)/(q-1)$, for any couple of natural numbers (q, d), with $q > 4$ if $d = 2$. Then*

$$P_{\mathrm{Sym}(p),\, \mathrm{Alt}(p)}(s) = P_{\mathrm{Alt}(p)}(s).$$

Proof. Applying Corollary 2.1.4, we observe that it suffices to prove the equality $\mu(H, \mathrm{Sym}(p)) = -\mu(H, \mathrm{Alt}(p))$ for any $H \leq \mathrm{Alt}(p)$. We recall that, with our hypothesis, $\mathrm{Alt}(p)$ has only affine and intransitive maximal subgroups; then, using Lemma 3.2.2, it remains to prove this equality when $H = \mathrm{Alt}(p)$ and $H = \langle 1 \rangle$.
If $H = \mathrm{Alt}(p)$, then it holds $\mu(\mathrm{Alt}(p), \mathrm{Sym}(p)) = -\mu(\mathrm{Alt}(p), \mathrm{Alt}(p))$: in fact $\mathrm{Alt}(p)$ is a maximal subgroup of $\mathrm{Sym}(p)$ and $\mu(\mathrm{Alt}(p), \mathrm{Sym}(p)) = -1$, from the definition of μ.

Let now $H = \langle 1 \rangle$. H is closed in $\mathcal{L}_{\mathrm{Sym}(p)}$; then from (3.2) we have

$$\sum_{\substack{T \leq \mathrm{Sym}(p) \\ \bar{T} = \mathrm{Sym}(p)}} \mu(\langle 1 \rangle, T) = \bar{\mu}(\langle 1 \rangle, \mathrm{Sym}(p)).$$

It is a known result that (see for example [35], p.128)

$$\bar{\mu}(\langle 1 \rangle, \mathrm{Sym}(p)) = (-1)^{p-1}(p-1)! = (p-1)!.$$

Then $\sum_{T \text{ trans.}, T \leq \mathrm{Sym}(p)} \mu(\langle 1 \rangle, T) = (p-1)!$, and so

$$\mu(\langle 1 \rangle, \mathrm{Sym}(p)) + \mu(\langle 1 \rangle, \mathrm{Alt}(p)) = - \sum_{\substack{T \text{ trans.}, T \leq \mathrm{Sym}(p) \\ T \neq \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(\langle 1 \rangle, T) + (p-1)!.$$

T is a transitive subgroup of $\mathrm{Sym}(p)$, then, by hypothesis, T is contained in a maximal affine subgroup. The number of the maximal affine subgroups of $\mathrm{Sym}(p)$ is equal to the number of the subgroups of $\mathrm{Sym}(p)$ with order p; it is $(p-2)!$. These maximal subgroups are all conjugated in $\mathrm{Sym}(p)$. Then, without lost of generality, we consider one of these maximal subgroups, that we denote by A; we calculate $\sum_{T \text{ trans.}, T \leq A} \mu(\langle 1 \rangle, T)$, and then we multiply the result by $(p-2)!$:

$$\sum_{\substack{T \text{ trans.}, T \leq \mathrm{Sym}(p) \\ T \neq \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(\langle 1 \rangle, T) = (p-2)! \cdot \sum_{T \text{ trans.}, T \leq A} \mu(\langle 1 \rangle, T) \qquad (3.4)$$

Let $A = P \rtimes K$, with $P \cong C_p$ and $K \cong C_{p-1}$; hence we may consider $T = P \rtimes R$, with $R \leq K$. Then

$$\sum_{\substack{T \text{ trans.} \\ T \leq A}} \mu(\langle 1 \rangle, T) = \sum_{PR \leq A} \mu(\langle 1 \rangle, PR) = \sum_{R \leq K} \mu(\langle 1 \rangle, PR).$$

Fix $R \neq \langle 1 \rangle$; we observe that the p complements to P in $\mathcal{L}_{PR}$ are pairwise disjoint. We apply the complement theorem of Crapo to the lattice $\mathcal{L}_{PR}$:

$$\begin{aligned}\mu(\langle 1 \rangle, PR) = & \sum_{\bar{R} \in P^{\perp}} \mu(\langle 1 \rangle, \bar{R}) \cdot \mu(\bar{R}, PR) = \\ = & \; p \cdot \mu(\langle 1 \rangle, R) \cdot (-1) = -p \cdot \mu(\langle 1 \rangle, R).\end{aligned}$$

Let $|R| = r$; R is cyclic, then, by Lemma 1.2.7, it follows $\mu(\langle 1 \rangle, R) = \mu(r)$. Then, if $R \neq \langle 1 \rangle$,

$$\mu(\langle 1 \rangle, PR) = -p \cdot \mu(r).$$

If $R = \langle 1 \rangle$, obviously $\mu(\langle 1 \rangle, P) = -1$. Hence we obtain

$$\sum_{R \leq K} \mu(\langle 1 \rangle, PR) = -1 - p \cdot \sum_{\substack{r \mid p-1 \\ r \neq 1}} \mu(r).$$

We have: $\displaystyle\sum_{\substack{r \mid p-1 \\ r \neq 1}} \mu(r) = \underbrace{\sum_{r \mid p-1} \mu(r)}_{=0} - \mu(1) = -\mu(1) = -1$. Then

$$\sum_{R \leq K} \mu(\langle 1 \rangle, PR) = -1 + p.$$

From (3.4)

$$\sum_{\substack{T \text{ } trans., \; T \leq \mathrm{Sym}(p) \\ T \neq \mathrm{Sym}(p) \\ T \neq \mathrm{Alt}(p)}} \mu(\langle 1 \rangle, T) = (p-2)! \cdot (p-1) = (p-1)!$$

and we may conclude $\mu(\langle 1 \rangle, \mathrm{Sym}(p)) + \mu(\langle 1 \rangle, \mathrm{Alt}(p)) = 0$. □

So we have proved that, if $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$ (with $q > 4$ if $d = 2$), $\mathrm{Sym}(p)$ satisfies the conjecture of Boston and Mann. We are going to analize the remained cases. If $p = 11$, $p = 23$ or $p = (q^d - 1)/(q - 1) > 5$, then $\mathrm{Alt}(p)$ contains some almost simple maximal subgroups, which coincide with their normalizers in $\mathrm{Sym}(p)$ (see Corollary 3 and Table I in [29]). We verify that the conjecture holds in all these cases; in fact we are going to prove the following statement.

Theorem 3.2.4 *If $p = 11$, $p = 23$ or $p = (q^d - 1)/(q - 1) > 5$, then*

$$P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) \neq P_{\mathrm{Alt}(p)}(s).$$

Proof. We recall (see Section 2.1) that

$$P_{\mathrm{Alt}(p)}(s) - P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) = \sum_{H \leq \mathrm{Alt}(p)} \frac{\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p))}{|\,\mathrm{Sym}(p) : H|^s} \quad (3.5)$$

Let $p \in \{11, 23\}$. By [29, Corollary 3], we know that, if $p = 11$ or $p = 23$, the only almost simple maximal subgroups of $\mathrm{Alt}(p)$ are those isomorphic to the Mathieu group M_p; these subgroups coincide with their normalizers in $\mathrm{Sym}(p)$. We consider all the subgroups H of $\mathrm{Alt}(p)$ having the same order of M_p; we want to calculate the following term of the sum (3.5)

$$\sum_{\substack{H \leq \mathrm{Alt}(p) \\ |H| = |\,\mathrm{M}_p\,|}} \frac{\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p))}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{M}_p\,|)^s} \quad (3.6)$$

Suppose H such that if N is a maximal subgroup of $\mathrm{Alt}(p)$ and $H \leq N$, then $N \in \mathcal{M}_{\mathrm{Alt}(p)}$; in other words, H is contained only in affine or intransitive maximal subgroups of $\mathrm{Alt}(p)$. Hence, by Lemma 3.2.2, we may conclude $\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p)) = 0$.

Then we may assume that H is contained in at least one almost simple maximal subgroup of $\mathrm{Alt}(p)$; hence $H \leq M$, with M isomorphic to M_p. But $|H| = |\,\mathrm{M}_p\,| = |M|$, then H has to coincide with the maximal subgroup M. We deduce $H = N_{\mathrm{Sym}(p)}(H)$ and, as observed in Remark 3.1.2, it follows $\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p)) = -1$. Denote by m the number of all maximal subgroups of $\mathrm{Alt}(p)$ isomorphic to M_p; from (3.6) we have

$$\sum_{\substack{H \leq \mathrm{Alt}(p) \\ |H| = |\,\mathrm{M}_p\,|}} \frac{\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p))}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{M}_p\,|)^s} = -\frac{m}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{M}_p\,|)^s} \neq 0.$$

Hence the term in (3.5) with denominator equal to $(|\,\mathrm{Sym}(p)|/|\,\mathrm{M}_p\,|)^s$ is different from 0; it follows

$$P_{\mathrm{Alt}(p)}(s) - P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) \neq 0.$$

We suppose now $p = (q^d - 1)/(q - 1) > 5$ for some $q, d \in \mathbb{N}$; we consider the set $\mathcal{Q}$ of all the couples (d, q) with $(q^d - 1)/(q - 1) = p$. For any $(d, q) \in \mathcal{Q}$, $\mathrm{Alt}(p)$ contains some maximal transitive subgroups isomorphic to $\mathrm{P\Gamma L}(d, q)$, that coincide with their normalizers in $\mathrm{Sym}(p)$. The set $\mathcal{Q}$ is finite, hence we can consider $(\hat{d}, \hat{q}) \in \mathcal{Q}$ such that $|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})| \geq |\,\mathrm{P\Gamma L}(d, q)|$, for any $(q, d) \in \mathcal{Q}$. We proceed in analoug way to the cases $p = 11, 23$ to prove $P_{\mathrm{Alt}(p)}(s) \neq P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s)$. We consider all the subgroups H of $\mathrm{Alt}(p)$ having the same order of $\mathrm{P\Gamma L}(\hat{d}, \hat{q})$; we want to calculate the following term of the sum (3.5):

$$\sum_{\substack{H \leq \mathrm{Alt}(p) \\ |H| = |\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|}} \frac{\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p))}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|)^s} \tag{3.7}$$

Let H be such that if N is a maximal subgroup of $\mathrm{Alt}(p)$ and $H \leq N$, then $N \in \mathcal{M}_{\mathrm{Alt}(p)}$; by Lemma 3.2.2, we conclude $\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p)) = 0$. Then we may assume that H is contained in at least one almost simple maximal subgroup of $\mathrm{Alt}(p)$; hence $H \leq \mathrm{P\Gamma L}(d, q)$, for some $(d, q) \in \mathcal{Q}$. But we are supposing $|H| = |\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|$, and $|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|$ is maximum between the orders of the maximal almost simple subgroups of $\mathrm{Alt}(p)$; therefore, if $H \leq \mathrm{P\Gamma L}(d, q)$, it follows $|\,\mathrm{P\Gamma L}(d, q)| = |\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|$, and H has to coincide with $\mathrm{P\Gamma L}(d, q)$. So we obtain that $H = N_{\mathrm{Sym}(p)}(H)$ and, by Remark 3.1.2, $\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p)) = -1$. Denote by γ the number of the maximal subgroups of $\mathrm{Alt}(p)$ with order equal to $|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|$; from (3.7) we have

$$\sum_{\substack{H \leq \mathrm{Alt}(p) \\ |H| = |\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|}} \frac{\mu(H, \mathrm{Alt}(p)) + \mu(H, \mathrm{Sym}(p))}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|)^s} = -\frac{\gamma}{(|\,\mathrm{Sym}(p)|/|\,\mathrm{P\Gamma L}(\hat{d}, \hat{q})|)^s} \neq 0.$$

It follows

$$P_{\mathrm{Alt}(p)}(s) - P_{\mathrm{Sym}(p),\,\mathrm{Alt}(p)}(s) \neq 0.$$

□

3.3 Some counterexamples

We have shown in the previous section that the conjecture of Boston and Mann is true when n is a prime. In this section we will show that this

conjecture doesn't hold in general for $n \geq 5$.

Remark 3.3.1 *It is in general very difficult to estabilish whether* $\mathrm{Sym}(n)$*, for a generic* n *not prime, satisfies or not the conjecture. Suppose that any maximal subgroup of* $\mathrm{Alt}(n)$ *does not coincide with its normalizer in* $\mathrm{Sym}(n)$*; this condition is necessary but not sufficient to guarantee the existence of a bijection between the set of the maximal subgroups of* $\mathrm{Alt}(n)$ *and the set of the maximal subgroups of* $\mathrm{Sym}(n)$*, different from* $\mathrm{Alt}(n)$*. In fact we know that there exists an one-to-one correspondence between the maximal subgroups of* $\mathrm{Alt}(n)$ *and* $\mathrm{Sym}(n)$ *of types intransitive and imprimitive (see Remark 3.1.3), but* $\mathrm{Sym}(n)$ *can contain a maximal primitive subgroup, different from* $\mathrm{Alt}(n)$*, that intersects* $\mathrm{Alt}(n)$ *in a subgroup which is not maximal in* $\mathrm{Alt}(n)$*. In this situation the Möbius numbers in* $\mathrm{Alt}(n)$ *and in* $\mathrm{Sym}(n)$ *of this subgroup can be not opposite, and it could follow* $P_{\mathrm{Alt}(n)}(s) \neq P_{\mathrm{Sym}(n),\,\mathrm{Alt}(n)}(s)$*.*

Remark 3.3.2 *Even if* n *is chosen such that the map* $M \mapsto M \cap \mathrm{Alt}(n)$ *induces a bijection between the set* $\mathcal{S}$ *of the maximal supplements of* $\mathrm{Alt}(n)$ *in* $\mathrm{Sym}(n)$ *and the set* $\mathcal{A}$ *of the maximal subgroups of* $\mathrm{Alt}(n)$*, it is not clear whether and why this could imply* $P_{\mathrm{Alt}(n)}(s) = P_{\mathrm{Sym}(n),\mathrm{Alt}(n)}(s)$*. The problem is that there is no hope that this bijection can be extended to a bijection between the subgroups that can be obtained as intersection of elements of* $\mathcal{A}$ *and those that are intersection of elements of* $\mathcal{S}$*. For example, we have* $n(n-1)/2$ *subgroups of order 2 that can be obtained as intersection of* $n-2$ *distinct point stabilizers (which are in* $\mathcal{S}$*), but each of them has trivial intersection with* $\mathrm{Alt}(n)$*. In particular it is very difficult to study what happens when we consider the imprimitive subgroups. Indeed, it is possible that the intersection of few (even two) imprimitive maximal subgroups of* $\mathrm{Sym}(n)$ *is already contained in* $\mathrm{Alt}(n)$*.*

Remark 3.3.3 *The case* $n = 21$ *is very interesting, because it realizes the situations explained in the previous remarks: in fact we will prove that there isn't a bijection between the maximal subgroups of* $\mathrm{Alt}(21)$ *and the maximal supplements of* $\mathrm{Alt}(21)$ *in* $\mathrm{Sym}(21)$*, and two maximal imprimitive subgroups of* $\mathrm{Sym}(21)$ *can have intersection in* $\mathrm{Alt}(21)$*. In particular we will verify that* $n = 21$ *is a counterexample to the conjecture.*

3.3.1 n=21

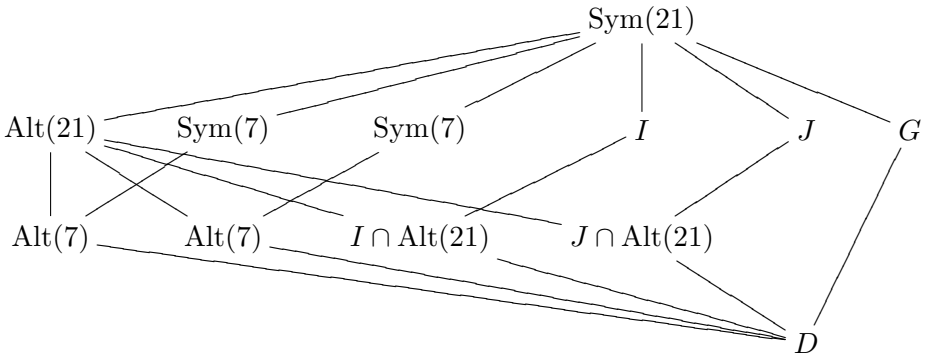
We denote by G a primitive subgroup of Sym(21) isomorphic to PGL$(2,7)$; we verify with GAP that G is a maximal subgroup of Sym(21). Let D be the derived subgroup of G; hence $D \cong \mathrm{PSL}(2,7)$, and D is transitive on $\{1,\dots,21\}$. Notice that $D = G \cap \mathrm{Alt}(21)$; we will prove that D is not maximal in Alt(21) and it corresponds to the intersection of two maximal imprimitive subgroups of Sym(21). Moreover we will verify that

$$\mu(D, \mathrm{Alt}(21)) \neq -\mu(D, \mathrm{Sym}(21)) \tag{3.8}$$

We proceed to estabilish the non-trivial systems of imprimitivity of D on $\{1,\dots,21\}$: D has two distinct systems of imprimitivity; each of these has 7 blocks, with any block with cardinality 3. Then D is contained in two maximal imprimitive subgroup of Sym(21) isomorphic to $\mathrm{Sym}(3) \wr \mathrm{Sym}(7)$, that we denote by I and J; they are the only maximal imprimitive subgroups of Sym(21) containing D. Using Remark 3.1.3, we can also conclude that D is contained in $I \cap \mathrm{Alt}(21)$ and $J \cap \mathrm{Alt}(21)$, that are the unique maximal imprimitive subgroups of Alt(21) containing D. Moreover we obtain that $D = I \cap J = I \cap J \cap \mathrm{Alt}(21)$.

We have now to determine the maximal primitive subgroups of Alt(21) and Sym(21) containing D. As shown in [10], the maximal primitive subgroups of Sym(21) are isomorphic to Sym(7) or to PΓL$(3,4)$ or to PGL$(2,7)$, and the maximal primitive subgroups of Alt(21) are isomorphic to Alt(7) or to PGL$(3,4)$. We have already observed that D is contained in one maximal subgroup isomorphic to PGL$(2,7)$, that is G. The maximal subgroups isomorphic to Sym(7) or PΓL$(3,4)$ are the normalizers of some maximal subgroups of Alt(21); therefore it suffices to check the maximal subgroups containing D in Alt(21). First of all we consider a maximal M isomorphic to Alt(7); by GAP we verify that M contains 30 subgroups of order 168, conjugated to D in Sym(21). Each maximal subgroup isomorphic to Alt(7) is conjugated to M in Sym(21), hence it contains 30 subgroups conjugated to D. But $|\mathrm{Cl}_{\mathrm{Sym}(21)}(D)| = 15 \cdot |\mathrm{Cl}_{\mathrm{Sym}(21)}(M)|$; therefore we may conclude that each subgroup conjugated to D in Sym(21), and in particular D itself, is contained in two maximal subgroups of Alt(21) isomorphic to Alt(7). Moreover we notice that Alt(7) is the unique maximal subgroup of Sym(7) containing subgroups with order equal to $|D|$; then D corresponds to the

intersection of two maximal subgroups of Sym(21) isomorphic to Sym(7). We observe that the maximal subgroups of Alt(21) isomorphic to PGL(3, 4) are all conjugated in Alt(21); we consider M one of these maximal subgroups. By GAP we verify that M does not contain any subgroup conjugated to D in Sym(21); then D is not contained in any maximal subgroup of Alt(21) isomorphic to PGL(3, 4), and also in any maximal subgroup of Sym(21) isomorphic to PΓL(3, 4). We are now able to represent the lattice of subgroups of Sym(21) containing D:



Note that there isn't a bijection between maximal subgroups of Alt(21) and maximal supplements of Alt(21) in Sym(21). From the diagram it is easy to calculate the Möbius numbers of D in Alt(21) and in Sym(21):

$$\mu(D, \mathrm{Alt}(21)) = 3 \quad \text{and} \quad \mu(D, \mathrm{Sym}(21)) = 1.$$

Then the inequality (3.8) holds. We recall

$$P_{\mathrm{Alt}(21)}(s) - P_{\mathrm{Sym}(21),\,\mathrm{Alt}(21)}(s) = \sum_{H \leq \mathrm{Alt}(21)} \frac{\mu(H, \mathrm{Alt}(21)) + \mu(H, \mathrm{Sym}(21))}{|\,\mathrm{Sym}(21) : H|^s} \tag{3.9}$$

We consider all subgroups H of Alt(21) having the same order of D, that is 168; we want to calculate the following term of the previous sum (3.9):

$$\sum_{\substack{H \leq \mathrm{Alt}(21) \\ |H| = |D|}} \frac{\mu(H, \mathrm{Alt}(21)) + \mu(H, \mathrm{Sym}(21))}{(|\,\mathrm{Sym}(21)|/|D|)^s}.$$

First of all we suppose that H is contained in a maximal primitive subgroup P of Alt(21). If $P \cong \mathrm{Alt}(7)$ then H is conjugated to D in Sym(21), and it has

Möbius numbers in Alt(21) and Sym(21) equal to D. Let $P \cong \mathrm{PGL}(3,4)$; with GAP we verify that P contains 360 subgroups of order 168, isomorphic to $\mathrm{PSL}(2,7)$, all conjugated in Sym(21), but not conjugated to D in Sym(21). Let H be one of these subgroups isomorphic to $\mathrm{PSL}(2,7)$; with some calculations we verify that $\mu(H, \mathrm{Alt}(21)) = -\mu(H, \mathrm{Sym}(21))$. If H is an intersection of some maximal intransitive subgroups of Alt(21) then, using the closure theorem of Crapo, it is easy to prove $\mu(H, \mathrm{Alt}(21)) = -\mu(H, \mathrm{Sym}(21))$. Moreover we are able to verify that the intersection H of some maximal imprimitive subgroups of $\mathrm{Alt}(n)$ has order 168 only if we intersect two maximal imprimitive subgroups isomorphic to $(\mathrm{Sym}(3) \wr \mathrm{Sym}(7)) \cap \mathrm{Alt}(21)$; in this case it follows that H is conjugated to D in Sym(21). Finally we may prove that the intersection of maximal intransitive and imprimitive subgroups of Alt(21) has never order 168. Hence

$$\sum_{\substack{H \leq \mathrm{Alt}(21) \\ |H|=|D|}} \frac{\mu(H, \mathrm{Alt}(21)) + \mu(H, \mathrm{Sym}(21))}{(|\mathrm{Sym}(21)|/|D|)^s} = \frac{4 \cdot |\mathrm{Cl}_{\mathrm{Sym}(21)}(D)|}{(|\mathrm{Sym}(21)|/|D|)^s} \neq 0$$

and then

$$P_{\mathrm{Alt}(21)}(s) - P_{\mathrm{Sym}(21),\, \mathrm{Alt}(21)}(s) \neq 0.$$

But we may verify that each maximal subgroup of Alt(21) doesn't coincide with its normalizer in Sym(21): by Remark 3.1.3, we know that doesn't exist any maximal intransitive or imprimitive subgroup of Alt(21) that coincide with its normalizer in Sym(21); moreover the maximal primitive subgroups isomorphic to Alt(7) have normalizer in Sym(21) isomorphic to Sym(7), and the maximal subgroups isomorphic to $\mathrm{PGL}(3,4)$ are normalized by $\mathrm{P\Gamma L}(3,4)$ in Sym(21). Therefore we conclude that the conjecture of Boston and Mann does not hold if $n = 21$.

Remark 3.3.4 *Then we have found a counterexample to the conjecture of Boston and Mann. In the case $n = 21$ does not exist an one-to-one correspondence between maximal subgroups of* Alt(21) *and maximal supplements of* Alt(21) *in* Sym(21)*; this fact makes the failure of the conjecture. We ask if the conjecture always holds when a bijective correspondence exists. As we have anticipated in Remark 3.3.2, the answer is negative; in fact we show now a counterexample ($n = 62$), in which* Sym(n) *contains some primitive*

proper subgroups different from $\mathrm{Alt}(n)$*, and there exists a bijection between maximal subgroups of* $\mathrm{Alt}(n)$ *and maximal subgroups of* $\mathrm{Sym}(n)$*, different from* $\mathrm{Alt}(n)$*.*

3.3.2 n=62

Using a result of Shareshian (see [33, Corollary 4.14]), we know that

$$\mu(\langle 1\rangle, \mathrm{Sym}(62)) + \mu(\langle 1\rangle, \mathrm{Alt}(62)) = -62\,!.$$

We have

$$P_{\mathrm{Alt}(62)}(s) - P_{\mathrm{Sym}(62),\,\mathrm{Alt}(62)}(s) = \sum_{H \leq \mathrm{Alt}(62)} \frac{\mu(H, \mathrm{Alt}(62)) + \mu(H, \mathrm{Sym}(62))}{|\,\mathrm{Sym}(62) : H|^s};$$

we consider the term in this sum with denominator equal to $|\,\mathrm{Sym}(62)|^s$. It is the following

$$\frac{\mu(\langle 1\rangle, \mathrm{Sym}(62)) + \mu(\langle 1\rangle, \mathrm{Alt}(62))}{|\,\mathrm{Sym}(62)|^s} = -\frac{62\,!}{(62\,!)^s} \neq 0.$$

Then

$$P_{\mathrm{Alt}(62)}(s) \neq P_{\mathrm{Sym}(62),\,\mathrm{Alt}(62)}(s).$$

But, there exists a bijection between the maximal subgroups of Alt(62) and the maximal subgroups of Sym(62), different from Alt(62). This bijection maps each maximal subgroup M of Sym(62) to $M \cap \mathrm{Alt}(62)$; if M is primitive then it is isomorphic to $\mathrm{PGL}(2, 61)$ (see [10]), and $M \cap \mathrm{Alt}(62) \cong \mathrm{PSL}(2, 61)$. Hence the conjecture is not true.

3.3.3 Open problem

The natural next step in our investigation is to consider Symmetric groups that do not contain primitive subgroups, different from $\mathrm{Alt}(n)$. Cameron has proved (see [4]) that the set of positive integers n for which does not exist a primitive group of degree n other than $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ has density 1. This means that there exists an important infinite family $\mathcal{F}$ of positive integers such that, if $n \in \mathcal{F}$, then $\mathrm{Sym}(n)$ doesn't contain any primitive proper subgroup, different from $\mathrm{Alt}(n)$, and then there exists a bijective correspondence between maximal subgroups of $\mathrm{Alt}(n)$ and maximal supplements of $\mathrm{Alt}(n)$ in $\mathrm{Sym}(n)$. In this case we ask if $\mathrm{Sym}(n)$ satisfies or not the

conjecture of Boston and Mann, and if all the Symmetric groups with degree in $\mathcal{F}$ have the same behaviour. We have not yet obtained an answer to this question. We think that the possibility of expressing subgroups of the Alternating group as intersection of two (or few) imprimitive maximal subgroups of the Symmetric group, could imply the existence of a counterexample to the conjecture of Boston and Mann, even among the groups with degree in $\mathcal{F}$. On the other hand, different considerations and partial results seem to indicate that if such a counterexample exists, then the degree must be quite large.

Chapter 4

Subgroups with non trivial Möbius number in the Alternating and Symmetric groups

4.1 Statement of the main results

Let n be a natural number. In this chapter we will work with $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$, respectively the Symmetric group and the Alternating group of degree n. Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$; denote by $b_m(G)$ the number of subgroups H of G with $|G : H| = m$ and $\mu(H, G) \neq 0$. Then, as anticipated in Section 2.2, we will prove the following statements.

Theorem 4.1.1 *There exists an absolute constant α such that $\forall\, n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $m \in \mathbb{N}$, then*

$$b_m(G) \leq m^{\alpha} \tag{4.1}$$

Theorem 4.1.2 *There exists an absolute constant β such that $\forall\, n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $H \leq G$, then*

$$|\mu(H, G)| \leq |G : H|^{\beta} \tag{4.2}$$

We proceed to prove these two theorems asymptotically on n.

4.2 Proof of Theorem 4.1.1

First of all we are going to state some results that will be used in the proof of Theorem 4.1.1.

Lemma 4.2.1 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and let*

$$\mathcal{C} := \{T \leq G \,|\, T \text{ transitive}, \mu(T, G) \neq 0\}.$$

There exists d, independent from n, such that $|\mathcal{C}| \leq (n!)^d$.

Proof. Let $T \in \mathcal{C}$. As we have already noted in Remark 1.4.4, G is a transitive permutation group on the set $\Delta_n = \{(a, b) \,|\, 1 \leq a, b \leq n,\ a \neq b\}$. We can apply Lemma 1.3.6 to G, acting on Δ_n, and we obtain

$$\mu(T, G) = \sum_{R \in \mathcal{S}_T} \mu(R, G) g(T, R)$$

where $\mathcal{S}_T = \{R \leq G \,|\, R \text{ transitive on } \Delta_n, R \geq T\}$. Since $\mu(T, G) \neq 0$, there exists $R \in \mathcal{S}_T$ such that $g(T, R) \neq 0$. Hence T is closed in $\mathcal{L}_R$, with respect to the action on Δ_n, and $T = C \cap R$ with $C = \overline{T}$, the Δ_n-closure of T in $\mathcal{L}_G$. We observe that transitivity on Δ_n is equivalent to 2-transitivity on $I_n = \{1, \ldots, n\}$; hence R is 2-transitive. Therefore any $T \in \mathcal{C}$ can be obtained as the intersection of a 2-transitive subgroup of G and a Δ_n-closed transitive subgroup of G. Hence to give an upper bound on $|\mathcal{C}|$, we may calculate the number of the Δ_n-closed transitive subgroups of G, and the number of the 2-transitive subgroups of G.
Denote by $\mathcal{P}$ the subset of partitions of Δ_n whose parts are orbits of some transitive subgroup of G in its action on Δ_n. Then the number of the Δ_n-closed transitive subgroups of G is equal to the cardinality of $\mathcal{P}$; by Corollary 1.4.6, there exists δ, independent from n, such that

$$|\mathcal{P}| \leq (n\,!)^\delta.$$

We want now to calculate the number of the 2-transitive subgroups of G; notice that a 2-transitive group is primitive. So we can use a result by Jaikin and Pyber (see [15, Corollary 8.2.]): they proved that the number of conjugacy classes of primitive groups of degree n in $\mathrm{Sym}(n)$ is smaller or

equal than $n^{\frac{a \log n}{\sqrt{\log \log n}}}$, with $a \in \mathbb{N}$ an absolute constant. For n sufficiently large, there exists b such that

$$n^{\frac{a \log n}{\sqrt{\log \log n}}} \leq (n!)^b$$

Obviously each conjugacy class of subgroups in $\mathrm{Sym}(n)$ has cardinality smaller than $n!$; then we obtain that the number of 2-transitive subgroups of G is at most $(n\,!)^{b+1}$. We can so conclude $|\mathcal{C}| \leq (n!)^{\delta+b+1}$. □

In the following proposition we will give a bound on the number of the transitive subgroups of G of index m and with Möbius number different from zero.

Lemma 4.2.2 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and denote by $t_m(G)$ the number transitive subgroups T of G with $|G : T| = m$ and $\mu(T, G) \neq 0$. Then there exists an absolute constant η such that*

$$t_m(G) \leq m^\eta$$

for each $m \in \mathbb{N}$.

Proof. Let $f = \max\{2, c\}$, where c is the constant which appears in the statement of Lemma 1.4.10. By Lemma 4.2.1, if $m^f \geq n!$, then it follows $t_m(G) \leq (n!)^d \leq m^{fd}$. Therefore, in order to conclude the proof, it suffices to find a polynomial bound for $t_m(G)$ which holds when $m^f < n!$. Clearly $t_m(G) \leq 1$ if $m \leq 2$, so we may assume $m > 2$. Let

$$\mathcal{D}_m := \{T \leq G \,|\, T \text{ transitive}, |G : T| = m,\ \mu(T, G) \neq 0\}\,;$$

obviously we have $t_m(G) = |\mathcal{D}_m|$. By Lemma 1.4.7 and Lemma 1.4.10, if $T \in \mathcal{D}_m$, then T is imprimitive and, up to conjugacy in $\mathrm{Sym}(n)$,

$$N = (\mathrm{Alt}(a))^b \leq T \leq \mathrm{Sym}(a) \wr \mathrm{Sym}(b)$$

with $1 < b < a < n$ and $ab = n$. Since $N \leq T$ and $\mathrm{Sym}(a) = \mathrm{Alt}(a)\langle(1, 2)\rangle$, $T = NX$ with $X \leq \langle(1, 2)\rangle \wr \mathrm{Sym}(b)$. Notice that $X \leq \langle(1, 2)\rangle \wr \mathrm{Sym}(b)$ can be viewed as subgroup of $\mathrm{Sym}(2b)$ and recall ([32, Theorem 4.2]) that $\mathrm{Sym}(2b)$ contains at most $2^{4c_1b^2}$ different subgroups for some absolute constant c_1. Summarizing we have at most $\sqrt{n}$ possibilities for b and,

for a fixed b, at most $2^{4c_1b^2}$ choices for X and, consequently, for T up to conjugacy in $\mathrm{Sym}(n)$. Moreover the number of the conjugates of T in $\mathrm{Sym}(n)$ is at most $|\mathrm{Sym}(n) : T| \leq 2|G : T| = 2m$. This implies that $t_m(G) \leq 2m\sqrt{n}2^{4c_1b^2} \leq 2m\sqrt{n}2^{4c_1n} \leq m^{c_2}$ for a suitable c_2, since, by Lemma 1.4.8, $m \geq 2^{\sigma n}$. □

We prove now that the number of closed subgroups of G of index m can be bounded polynomially on m.

Lemma 4.2.3 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and denote by $c_m(G)$ the number of the subgroups of G with index m and closed in $\mathcal{L}_G$ with respect to the action on $\{1, \ldots, n\}$. Then*

$$c_m(G) \leq m^4$$

for each $m \in \mathbb{N}$.

Proof. As we have observed in Remark 1.3.5, the closed subgroups of G are precisely the conjugates of $(\mathrm{Sym}(x_1)\times\cdots\times\mathrm{Sym}(x_r))\cap G$ with $x_1+\cdots+x_r = n$ and $r \neq n-1$ if $G = \mathrm{Alt}(n)$. Except in the case $r = n$ and $G = \mathrm{Alt}(n)$, such a subgroups has index

$$m = \frac{n\,!}{x_1\,!x_2\,!\cdots x_r\,!}.$$

We need to count the number of possible choices for $x_1, \ldots, x_r$ giving the same index m. We consider m as the multinomial coefficient

$$m = \binom{n}{x_1\ x_2 \cdots\ x_r} = \binom{n}{x_1}\binom{n-x_1}{x_2}\cdots\binom{n-x_1-\cdots-x_{r-2}}{x_{r-1}}.$$

We know that the ordered factorizations of m are at most m^2 (see [14]). Fix a factorization $m = \beta_1\beta_2\cdots\beta_{r-1}$. Each factor β_i is a binomial coefficient and, given $y_i = n - x_1 - \cdots - x_{i-1}$, there are two possible values of x_i for which $\beta_i = \binom{y_i}{x_i}$, for any $i \in \{1, \ldots, r-1\}$; hence there at most $2^{r-1} \leq m$ possibilities for $x_1, \ldots, x_r$ corresponding to the given factorization. So there are at most m^3 choices of $x_1, \ldots, x_r$ giving the same m. Hence there are at most m^3 conjugacy classes of closed subgroups with index m. Each of these subgroups has at most m conjugates, so $c_m(G) \leq m^4$.

□

We can now complete the proof of Theorem 4.1.1.

Proof. [Theorem 4.1.1] We are supposing $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$, and we want to prove the existence of α, independent from the choice of n, such that $b_m(G) \leq m^\alpha$ for any $m \in \mathbb{N}$.
Let $H \leq G$ with $|G : H| = m$ and $\mu(H, G) \neq 0$. Using Lemma 1.3.6 with respect to the natural action of G on $\{1, \ldots, n\}$, we obtain

$$\mu(H, G) = \sum_{T \in \mathcal{S}_H} \mu(T, G) g(H, T)$$

with $\mathcal{S}_H = \{T \leq G \,|\, T \text{ transitive}, T \geq H\}$. Since $\mu(H, G) \neq 0$, there exists $T \in \mathcal{S}_H$ such that $\mu(T, G)g(H, T) \neq 0$. This implies that H is closed in $\mathcal{L}_T$, and then $H = T \cap C$, with C the closure of H in $\mathcal{L}_G$. The element H is intersection between a transitive subgroup of G, with non zero Möbius number, and a closed subgroup of G. We want to give an upper bound on $b_m(G)$. First of all we count the number of closed subgroups of G with index dividing m. By Lemma 4.2.3, for any index smaller or equal than m there are at most m^4 closed subgroups of G with this index; hence there are at most m^5 closed subgroups of G with index dividing m. By Lemma 4.2.2, for each index smaller or equal than m, there are at most m^η transitive subgroups of G with this index and with non zero Möbius number; then there are at most $m^{\eta+1}$ transitive subgroups of G with non zero Möbius number and index dividing m. We may conclude that

$$b_m(G) \leq m^{\eta+6}.$$

□

4.3 Proof of Theorem 4.1.2

To prove Theorem 4.1.2 we will use the following lemma on the Möbius number of the transitive subgroups of G.

Lemma 4.3.1 *Let $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. Then there exists an absolute constant ν such that*

$$|\mu(T, G)| \leq |G : T|^\nu$$

for each transitive subgroup T of G.

Proof. Let T be a transitive subgroup of G; obviously we may suppose $\mu(T,G) \neq 0$. Using Lemma 1.3.6 with respect to the transitive action of G on $\Delta_n = \{(a,b) \,|\, 1 \leq a,b \leq n,\ a \neq b\}$, we obtain

$$|\mu(T,G)| \leq \sum_{R \in \mathcal{S}_T} |\mu(R,G)| \cdot |g(T,R)| \tag{4.3}$$

with $\mathcal{S}_T := \{R \leq G \,|\, R \text{ transitive on } \Delta_n, R \geq T\}$. Let $t \leq n-1$ be the number of orbits of T on Δ_n. We have to distinguish two cases.

a) Let $\mathcal{S}_T \subseteq \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. Obviously if $\operatorname{soc} T = \mathrm{Alt}(n)$ we have

$$|\mu(T,G)| = 1 \leq |G:T|.$$

Otherwise, using Theorem 1.3.8 and Lemma 1.4.5, we obtain

$$|\mu(T,G)| \leq |g(T,\mathrm{Alt}(n))| + |g(T,\mathrm{Sym}(n))| \leq (t\,!)^2 \leq 4 \cdot |G:T|^2.$$

b) Let $\mathcal{S}_T \not\subseteq \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$. In this case there exists $R \in \mathcal{S}_T$ such that $\mathrm{Alt}(n) \not\leq R$. This subgroup R is 2-transitive and consequently primitive on $\{1,\ldots,n\}$; then, by applying Lemma 1.4.7, we obtain $|G:T|^2 \geq |G:R|^2 \geq n!$ for n large enough. Hence our aim becomes bounding $|\mu(T,G)|$ polinomially on $n!$.
Since $t \leq n-1$, by Theorem 1.3.8 we get $|g(T,R)| \leq \frac{(t\,!)^2}{2} \leq \frac{(n\,!)^2}{2}$ for any $R \neq T$; also $|g(T,T)| = 1 \leq \frac{(n\,!)^2}{2}$. From (4.3), it follows

$$|\mu(T,G)| \leq (n\,!)^2 \cdot \sum_{R \in \mathcal{S}_T} |\mu(R,G)|.$$

So we have to bound the sum $\sum_{R \in \mathcal{S}_T} |\mu(R,G)|$ polinomially on $n\,!$.
As we noticed in the proof of Lemma 4.2.1, there exists b such that the number of 2-transitive subgroups of G is at most $(n\,!)^b$. In particular $|\mathcal{S}_T| \leq (n\,!)^b$. Moreover, by Theorem 1.4.1, we have $|\mu(R,G)| \leq 1$ for each $R \in \mathcal{S}_T$. We can conclude

$$|\mu(T,G)| \leq (n\,!)^2 \cdot (n\,!)^b$$

for any n large enough.

□

Now we are able to prove the theorem.

Proof. **[Theorem 4.1.2]** We are supposing $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$; we want to prove the existence of β, independent from the choice of n, such that $|\mu(H,G)| \leq |G:H|^{\beta}$ for each $H \leq G$. We may suppose $H \leq G$ with $\mu(H,G) \neq 0$. By Lemma 1.3.6

$$\mu(H,G) = \sum_{T \in \mathcal{S}_H} \mu(T,G) g(H,T) \tag{4.4}$$

with $\mathcal{S}_H$ the set of transitive subgroups of G containing H.
Let $\sigma = \{\Omega_1, \ldots, \Omega_r\}$ be the set of orbits of H on $\{1, \ldots, n\}$. Choose an element $x_i \in \Omega_i$, $\forall\ 1 \leq i \leq r$, and define the set $X := \{x_1, \ldots, x_r\}$. Since $\mathrm{Alt}(X) \cap H = \langle 1 \rangle$, we have $|G:H| \geq |\mathrm{Alt}(X)| = r\,!/2$. Moreover, applying Theorem 1.3.8, we obtain $|g(H,T)| \leq (r\,!)^2/2$ for each $T \neq H$. Hence, for each $T \in \mathcal{S}_H$,

$$|g(H,T)| \leq 2 \cdot |G:H|^2.$$

From (4.4), it follows

$$|\mu(H,G)| \leq 2 \cdot |G:H|^2 \cdot \sum_{T \in \mathcal{S}_H} |\mu(T,G)|.$$

By Lemma 4.3.1 there exists ν such that

$$|\mu(T,G)| \leq |G:T|^{\nu} \leq |G:H|^{\nu} \ \text{ for each } T \in \mathcal{S}_H.$$

It remains to give an estimate on the number s of subgroups $T \in \mathcal{S}_H$ with $\mu(T,G) \neq 0$. We notice that if $T \in \mathcal{S}_H$ then $|G:T| \leq |G:H|$. Hence, applying Lemma 4.2.2, we obtain

$$s \leq \sum_{m \leq |G:H|} t_m(G) \leq |G:H|^{\eta+1}.$$

We may conclude $|\mu(H,G)| \leq 2 \cdot |G:H|^2 \cdot |G:H|^{\nu} \cdot |G:H|^{\eta+1}$. □

We have proved the existence of two constants α and β that satisfy the statements of Theorems 4.1.1 and 4.1.2 for any $n \in \mathbb{N}$, but we have not found precise values for these constants. In fact, proving the theorems, we have realized that an extimation of α and β could need many calculations. In the particular case n prime (with some exceptions), we are able to verify that $\beta = 1$.

4.4 Bounds with n prime

From now on we consider $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$; we denote by $\mathcal{M}_G$ the set of the intransitive and affine maximal subgroups of G. We are able to prove the following statement.

Lemma 4.4.1 *Let $p \geq 5$ and let $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$. Suppose $H < G$, $H \neq \langle 1 \rangle$, such that if N is a maximal subgroup of G with $H \leq N$, then $N \in \mathcal{M}_G$. Then*

$$|\mu(H, G)| < |G : H|.$$

Proof. $H < G$; then we know that $\mu(H, G) \neq 0$ only if H is an intersection of maximal subgroups of G (see Remark 1.2.2).
If H is a maximal subgroup of G, then $|\mu(H, G)| = 1$, by the definition of μ, and the index $|G : H|$ is strictly bigger than 1; hence $|\mu(H, G)| < |G : H|$.
Now we suppose H an intersection of elements of $\mathcal{M}_G$, but H not maximal in G; H is an intersection of some maximal affine or intransitive subgroups of G. We notice that the intersection of two maximal affine subgroups of G is intransitive; then H is an intransitive subgroup of G. By applying the closure theorem of Crapo to the lattice $\mathcal{L}_G$, we obtain

$$\mu(H, G) = - \sum_{\substack{H \leq T < G \\ \bar{T} = G}} \mu(H, T) + \begin{cases} \bar{\mu}(H, G) & \text{if } H \text{ is closed in } \mathcal{L}_G \\ 0 & \text{otherwise} \end{cases}$$

and

$$|\mu(H, G)| \leq | \sum_{\substack{H \leq T < G \\ \bar{T} = G}} \mu(H, T)| + \begin{cases} |\bar{\mu}(H, G)| & \text{if } H \text{ is closed in } \mathcal{L}_G \\ 0 & \text{otherwise} \end{cases} \tag{4.5}$$

If doesn't esixts any transitive subgroup $T \neq G$ such that $H \leq T$, then H has the form

$$(\mathrm{Sym}(\Omega_1) \times \cdots \times \mathrm{Sym}(\Omega_r)) \cap G$$

where $\Omega_1, \ldots, \Omega_r$ are the orbits of H on $\{1, \ldots, p\}$, with $2 < r < p$. Then H is closed in $\mathcal{L}_G$ and, as we have already observed in Remark 1.3.9, it holds

$|\bar{\mu}(H,G)| = (r-1)!$. Hence

$$|\mu(H,G)| = (r-1)!.$$

We take $x_i \in \Omega_i$, $\forall\ 1 \leq i \leq r$, and define $X := \{x_1, \ldots, x_r\}$. The group $Y := \mathrm{Sym}(X) \cap G$ is such that $Y \cap H = \langle 1 \rangle$; then $|G : H| \geq |Y| \geq r\,!/2$. We are considering $r > 2$, then $(r-1)! < (r\,!/2)$, and it follows $(r-1)! < |G : H|$. We may conclude

$$|\mu(H,G)| < |G : H|.$$

Then we may suppose that there exists at least one transitive subgroup $T \neq G$ such that $H \leq T$. By hypothesis, we have $T \leq A$, with A a maximal affine subgroup of G; hence H is an intransitive subgroup of A. It holds $A = P \rtimes (K \cap G) = N_G(P)$, for some $P \cong C_p$ and $K \cong C_{p-1}$; then H is a cyclic subgroup of $K \cap G$. By hypothesis, $H \neq \langle 1 \rangle$, and then H is not closed in $\mathcal{L}_G$: in fact $\mathrm{Alt}(p)$ doesn't have any cyclic closed subgroup, and the only cyclic closed subgroups of $\mathrm{Sym}(p)$ have order 2, and fix $p-2$ elements. From (4.5),

$$|\mu(H,G)| \leq |\sum_{\substack{H \leq T < G \\ T \text{ trans.}}} \mu(H,T)| \tag{4.6}$$

We are considering $H < A$; the transitive subgroups containing H and contained in A are of the form $P \rtimes R$, with $H \leq R \leq (K^s \cap G)$ for some $s \in P$ (see Remark 3.2.1). The subgroup P has p complements in A pairwise disjoint. Then H is contained only in one complement of P; without lost of generality we may assume $H \leq K \cap G$ and $H \leq R \leq K \cap G$.
Any maximal affine subgroup $\bar{A}$ of G containing H is conjugated to A in $\mathrm{Sym}(p)$. Then we can repeat for $\bar{A} = \bar{P} \rtimes (\bar{K} \cap G)$ the same procedure; so we may assume $H \leq (\bar{K} \cap G)$, with $\bar{K} \cong C_{p-1}$. Denote by t the number of the maximal affine subgroups of G containing H, that is equivalent to the number of the subgroups of order p normalized by H. We recall that the intersection of two maximal affine subgroups is intransitive; then any transitive subgroup T that appears in (4.6), is contained in only one maximal

affine subgroup of G. It follows

$$\sum_{\substack{H\leq T<G \\ T \text{ trans.}}} \mu(H,T) = t \cdot \sum_{\substack{T \ trans. \\ H\leq T\leq A}} \mu(H,T) = t \cdot \sum_{H\leq R\leq K\cap G} \mu(H,PR) \quad (4.7)$$

If $H = K \cap G$, then H is a maximal subgroup of PH, and we obtain:

$$\sum_{\substack{H\leq T<G \\ T \text{ trans.}}} \mu(H,T) = t \cdot \mu(H,PH) = -t.$$

We recall that t is smaller or equal than the number of all maximal affine subgroups of G; using the bijection between the set of the maximal affine subgroups of $\mathrm{Alt}(p)$ and the set of the maximal affine subgroups of $\mathrm{Sym}(p)$, we may conclude $t \leq (p-2)!$. Then

$$|\sum_{\substack{H\leq T<G \\ T \text{ trans.}}} \mu(H,T)| \leq (p-2)!.$$

If $G = \mathrm{Alt}(p)$, then $|H| = (p-1)/2$; it follows that $|\mathrm{Alt}(p) : H| = p\cdot(p-2)!$. From (4.6), we obtain

$$|\mu(H, \mathrm{Alt}(p))| \leq (p-2)! < |\mathrm{Alt}(p) : H|.$$

At the same way, if $G = \mathrm{Sym}(p) \Rightarrow |H| = p-1$ and $|\mathrm{Sym}(p) : H| = p\cdot(p-2)!$. Hence

$$|\mu(H, \mathrm{Sym}(p))| < |\mathrm{Sym}(p) : H|.$$

Now we suppose $H < K \cap G$. We fix R in (4.7), and we calculate $\mu(H, PR)$; to do this, we proceed as in the proof of Lemma 3.2.2. By applying the complement theorem of Crapo to the lattice L of the subgroups of PR containing H, we obtain:

$$\mu(H,PR) = \sum_{\bar{R}\in (PH)^{\perp}} \mu(H,\bar{R}) \cdot \mu(\bar{R},PR) = \mu(H,R) \cdot \mu(R,PR).$$

R is a maximal subgroup of PR; it holds $\mu(R,PR) = -1$. Hence

$$\mu(H,PR) = -\mu(H,R).$$

$H \lhd R$, then $\mu(H,R) = \mu(\langle 1\rangle, R/H)$. Let $|H| = h$ and $|R| = r$; R/H is cyclic, then, by Lemma 1.2.7, it follows

$$\mu(H, PR) = -\mu(\langle 1\rangle, R/H) = -\mu(r/h).$$

If $G = \mathrm{Alt}(p)$, then $|K \cap \mathrm{Alt}(p)| = (p-1)/2$, and from (4.7) we obtain:

$$\sum_{\substack{H \leq T < \mathrm{Alt}(p) \\ T \text{ trans.}}} \mu(H,T) = -t \cdot \sum_{h|r \text{ and } r|(p-1)/2} \mu(r/h).$$

Set $\bar{r} = r/h$, for any r such that $h|r$ and $r|(p-1)/2$; then we observe that $\sum_{h|r \text{ and } r|(p-1)/2} \mu(r/h) = \sum_{\bar{r}|(p-1)/2h} \mu(\bar{r})$. Moreover $(p-1)/2h \neq 1$, because we are supposing $H < K \cap \mathrm{Alt}(p)$, and so, as observed in Remark 1.2.6, it follows

$$\sum_{\bar{r}|(p-1)/2h} \mu(\bar{r}) = 0.$$

Then, from (4.6),

$$|\mu(H, \mathrm{Alt}(p)| = 0 < |\mathrm{Alt}(p) : H|.$$

In a analoug way, let $G = \mathrm{Sym}(p)$; then $|K| = p-1$, and from (4.7) we have

$$\sum_{\substack{H \leq T < \mathrm{Sym}(p) \\ T \text{ trans.}}} \mu(H,T) = -t \cdot \sum_{h|r \text{ and } r|p-1} \mu(r/h).$$

Set $\bar{r} = r/h$, for any r such that $h|r$ and $r|p-1$; then we observe that $\sum_{h|r \text{ and } r|p-1} \mu(r/h) = \sum_{\bar{r}|p-1/h} \mu(\bar{r})$. Moreover $(p-1)/h \neq 1$, because $H < K$, and so it follows

$$\sum_{\bar{r}|p-1/h} \mu(\bar{r}) = 0.$$

Then, from (4.6),

$$|\mu(H, \mathrm{Sym}(p)| = 0 < |\mathrm{Sym}(p) : H|.$$

□

From Lemma 4.4.1 we can deduce the following theorem, that gives a bound stronger than Theorem 4.1.2, for some prime degrees.

Theorem 4.4.2 *Let p be a prime, with $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$, for any couple of natural numbers (q, d), with $q > 4$ if $d = 2$.*
If $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$ and $H \leq G$, then

$$|\mu(H, G)| \leq |G : H|. \tag{4.8}$$

Proof. We may suppose $p \geq 5$: in fact if $p = 2$ or $p = 3$ the inequality (4.8) is easily verified. Consider $G \in \{\mathrm{Alt}(p), \mathrm{Sym}(p)\}$; using [29, Theorem 2, Corollary 3], we observe that if $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$ (with $q > 4$ if $d = 2$), then G contains only maximal transitive subgroups of affine type. The set $\mathcal{M}_G$ represents the set of all maximal subgroups of G, different from $\mathrm{Alt}(p)$. By applying Lemma 4.4.1, we obtain $|\mu(H, G)| < |G : H|$, for any $H < G$, $H \neq \langle 1 \rangle$, with $\mathrm{Alt}(p)H = G$.
If $G = \mathrm{Sym}(p)$ and $\langle 1 \rangle < H < \mathrm{Alt}(p)$, using Lemma 3.2.2 and Lemma 4.4.1, we may conclude $|\mu(H, \mathrm{Sym}(p)| = |\mu(H, \mathrm{Alt}(p)| < |\mathrm{Sym}(p) : H|$. If $G = \mathrm{Sym}(p)$ and $H = \mathrm{Alt}(p)$, then $|\mu(G, H)| = 1 < |G : H|$.
Hence it remains to prove that (4.8) holds for $H = G$ and $H = \langle 1 \rangle$. If $H = G$ we obtain $|\mu(H, G)| = |G : H| = 1$. Let $H = \langle 1 \rangle$; as it is shown in [33, Theorem 1.6.], it holds $|\mu(\langle 1 \rangle, \mathrm{Sym}(p))| = p!/2$. In the proof of Theorem 3.2.3, it has been proved $\mu(\langle 1 \rangle, \mathrm{Sym}(p)) = -\mu(\langle 1 \rangle, \mathrm{Alt}(p))$; then $|\mu(\langle 1 \rangle, G| = p!/2 = |G : \langle 1 \rangle|$. □

Remark 4.4.3 *If $p \geq 5$, with $p \neq 11, 23$ and $p \neq (q^d - 1)/(q - 1)$, as in the hypothesis of Theorem 4.4.2, then we observe that the inequality* (4.8) *strictly holds for any $H < G$, $H \neq \langle 1 \rangle$.*

Remark 4.4.4 *We observe that the inequality* (4.8) *does not hold in general if we consider $G = \mathrm{Alt}(n)$ and $H \leq G$. For example, as shown in [33, Corollary 4.15], it holds $\mu(\langle 1 \rangle, \mathrm{Alt}(14)) = 14!$. Instead we don't know examples of Symmetric groups for which* (4.8) *doesn't hold for some $H \leq G$.*

These considerations lead us to formulate the following:

Conjecture 4.4.5 *There exists an absolute constant γ such that $\forall\, n \in \mathbb{N}$, if $G \in \{\mathrm{Alt}(n), \mathrm{Sym}(n)\}$ and $H \leq G$, then*

$$|\mu(H, G)| \leq \gamma \cdot |G : H|.$$

Bibliography

[1] M. Aschbacher and R.M. Guralnick, *Solvable generation of groups and Sylow subgroups of the lower central series*, Journal of Algebra **77** (1982), 189–201.

[2] N. Boston, *A probabilistic generalization of the Riemann zeta function*, Analytic Number Theory vol. 1 (Allerton Park, IL, 1995) **138** (1996), 155–162.

[3] K.S. Brown, *The coset poset and probabilistic zeta function of a finite group*, Journal of Algebra **225** (2000), no. 2, 989–1012.

[4] P.J. Cameron, *Permutation groups*, London Mathematical Society Student Texts 45, Cambridge University Press, Cambridge, 1999.

[5] H. Crapo, *The Möbius function of a lattice*, J. Combin. Theory **1** (1966), 126–134.

[6] H. Crapo, *Möbius inversion in lattices*, Arch. Math. (Basel) **19** (1968), 595–607.

[7] F. DallaVolta, A. Lucchini, and F. Morini, *Some remarks on the probability of generating an almost simple group*, Glasgow Math. J. **45** (2003), 281–291.

[8] E. Detomi and A. Lucchini, *Crowns and factorization of the probabilistic zeta function of a finite group*, Journal of Algebra **265** (2003), no. 2, 651–668.

[9] J.D. Dixon, M.P.F. duSatoy, A.Mann, and D.Segal, *Analytic pro-p groups*, Cambridge University Press, Cambridge, 1991.

[10] J.D. Dixon and B. Mortimer, *Permutations groups*, Graduate Texts in Mathematics vol.163, Springer, New York, 1996.

[11] M.D. Fried and M. Jarden, *Field arithmetic*, Springer, Berlin, 1986.

[12] The GAP Group, *GAP-Groups, Algorithms, and Programming*, Version 4.4.10, 2007.

[13] P. Hall, *The Eulerian functions of a group*, Quart. J. Math. **7** (1936), 134–151.

[14] V.C. Harris and M.V. Subbarao, *On product partitions of integers*, Can. Math. Bull. **34** (1991), 474–479.

[15] A. Jaikin-Zapirain and L.Pyber, *Random generation of finite and profinite groups and group enumeration*, to appear.

[16] W. Kantor and A. Lubotzky, *The probability of generating a finite classical group*, Geom. Dedicata **36** (1990), no. 1, 67–87.

[17] M.W. Liebeck, C.E. Praeger, and J. Saxl, *A classification of the maximal subgroups of the finite Alternating and Symmetric groups*, Journal of Algebra **111** (1987), 365–383.

[18] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics vol.212, Birkhäuser Verlag, Basel, 2003.

[19] A. Lucchini, *On subgroups with non trivial Möbius number*, J. Group Theory, to appear.

[20] A. Lucchini, *On the subgroups of a monolithic group with non trivial Möbius number*, in preparation.

[21] A. Lucchini, *Profinite groups with nonabelian crowns of bounded rank and their probabilistic zeta function*, Israel J. Math., to appear.

[22] A. Lucchini, *Intervals in subgroup lattices of finite groups*, Communications in Algebra (2) **22** (1994), 529–549.

[23] A. Lucchini, *Subgroups of solvable groups with non-zero Möbius function*, J. Group Theory **10** (2007), no. 5, 633–639.

[24] A. Lucchini and M. Massa, *The probabilistic zeta function of Alternating and Symmetric groups*, Algebra Colloquium **16** (2009), no. 2, 195–210.

[25] A. Mann, *Positively finitely generated groups*, Forum Math. **8** (1996), 429–459.

[26] A. Mann, *A probabilistic zeta function for arithmetic groups*, Internat. J. Algebra Comput. **15** (2005), no. 5-6, 1053–1059.

[27] A. Mann and A. Shalev, *Simple groups, maximal subgroups and probabilistic apsects of profinite groups*, Israel J. Math. **96** (1996), 449–468.

[28] A. Maróti, *On the orders of primitive groups*, Journal of Algebra **258** (2002), 631–640.

[29] P.P. Pálfy, *On feit's examples of intervals in subgroup lattices*, Journal of Algebra **116** (1988), 471–479.

[30] C.E. Praeger, *The inclusion problem for finite primitive permutation groups*, Proc. London Math. Soc. (3) **60** (1990), 68–88.

[31] C.E. Praeger and J. Saxl, *On the order of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), 303–308.

[32] L. Pyber, *Asymptotic results for permutation groups*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **11** (1993), 197–219.

[33] J. Shareshian, *On the Möbius number of the subgroup lattice of the Symmetric group*, Journal of Combinatorial Theory, Series A **78** (1997), 236–267.

[34] J. Shareshian, *On the probabilistic zeta function for finite groups*, Journal of Algebra **210** (1998), no. 2, 703–707.

[35] R.P. Stanley, *Enumerative combinatorics. Vol.1*, Cambridge Studies in Advanced Mathematics vol.49, Cambridge University Press, Cambridge, 1997.