ON THE GENERATING GRAPHS OF THE SYMMETRIC AND ALTERNATING GROUPS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

FUAT ERDEM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

SEPTEMBER 2018

Approval of the thesis:

ON THE GENERATING GRAPHS OF THE SYMMETRIC AND ALTERNATING GROUPS

submitted by **FUAT ERDEM** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** ______________

Prof. Dr. Yıldıray Ozan
Head of Department, **Mathematics** ______________

Prof. Dr. Gülin Ercan
Supervisor, **Mathematics Department, METU** ______________

Dr. Attila Maróti
Co-supervisor, **Alfréd Rényi Inst. of Mathematics, Hungary** ______________

Examining Committee Members:

Prof. Dr. İsmail Şuayip Güloğlu
Mathematics Department, Doğuş University ______________

Prof. Dr. Gülin Ercan
Mathematics Department, METU ______________

Prof. Dr. Yücel Tıraş
Mathematics Department, Hacettepe University ______________

Assoc. Prof. Dr. Ebru Solak
Mathematics Department, METU ______________

Assoc. Prof. Dr. Mustafa Gökhan Benli
Mathematics Department, METU ______________

Date: ______________

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name:	FUAT ERDEM
Signature :	

ABSTRACT

ON THE GENERATING GRAPHS OF THE SYMMETRIC AND ALTERNATING GROUPS

Erdem, Fuat
Ph.D., Department of Mathematics
Supervisor : Prof. Dr. Gülin Ercan
Co-Supervisor : Dr. Attila Maróti

September 2018, 58 pages

Dixon showed that the probability that a random pair of elements in the symmetric group S_n generates S_n or the alternating group A_n tends to 1 as $n \to \infty$. (A generalization of this result was given by Babai and Hayes.) The generating graph $\Gamma(G)$ of a finite group G is defined to be the simple graph on the set of non-identity elements of G with the property that two elements are connected by and edge if and only if they generate G. The purpose of this thesis is to study the graphs $\Gamma(S_n)$ and $\Gamma(A_n)$. We prove that the graphs $\Gamma(S_n)$ and $\Gamma(A_n)$ contain Hamiltonian cycles provided that $n \geq 107$. This improves a recent result of Breuer, Guralnick, Lucchini, Maróti and Nagy. Our result can be viewed as another step towards the conjecture of Breuer, Guralnick, Lucchini, Maróti and Nagy stating that for an arbitary finite group G of order at least 4 the generating graph $\Gamma(G)$ contains a Hamiltonian cycle if and only if G/N is cyclic for every non-trivial normal subgroup N of G. (This is a stronger form of an older conjecture of Breuer, Guralnick and Kantor.) Our results may have applications to dimensions of fixed point spaces of elements of a finite group G acting on a finite dimensional vector space V with $C_V(G) = 0$.

Keywords: generating graph, hamiltonian cycle, symmetric group, alternating group.

ÖZ

SİMETRİK VE ALTERNE GRUPLARIN ÜRETİCİ GRAFLARI ÜZERİNE

Erdem, Fuat
Doktora, Matematik Bölümü
Tez Yöneticisi : Prof. Dr. Gülin Ercan
Ortak Tez Yöneticisi : Dr. Attila Maróti

Eylül 2018 , 58 sayfa

Dixon, simetrik grup S_n'den rastgele alınan bir permutasyon ikilisinin S_n'i ya da alterne grup A_n'i üretme olasılığının n sonsuza giderken limitinin 1 olduğunu göstermiştir. Sonlu bir G grubunun üretici grafı $\Gamma(G)$, köşenoktaları G grubunun birim elemanından farklı elemanları olan ve herhangi farklı iki köşenoktanın birbirine bir kenar ile bağlı olmalarının bu iki köşenoktanın G grubunu üretmesi koşuluna bağlı olduğu graf olarak tanımlanmaktadır. Bu tezde esas amaç $\Gamma(S_n)$ ve $\Gamma(A_n)$ graflarını çalışmaktır. Bu tezde $\Gamma(S_n)$ ve $\Gamma(A_n)$ graflarının $n \geq 107$ koşulu altında Hamilton döngüler içerdiğini gösteriyoruz. Bu sonuç, Breuer, Guralnick, Lucchini, Maróti and Nagy'nin kısa bir süre önce elde ettikleri bir sonucunun iyileştirmesidir. Bu sonuç ayrıca şu sanının ispatlanmasına yönelik bir adım olarak görülebilir: Mertebesi en az 4 olan her sonlu G grubu için, G'nin üretici grafı olan $\Gamma(G)$'nin bir Hamilton döngü içermesi ancak ve ancak G grubunun birim gruptan farklı her bir N normal altgrubu için G/N grubunun devirli olmasıyla mümkündür. (Bu sanı, Breuer, Guralnick and Kantor'un daha önceki bir sanısının daha güçlü bir halidir.) Elde ettiğimiz sonuçların, sonlu boyutlu bir V vektör uzayına $C_V(G) = 0$ olacak şekilde etki eden sonlu bir G grubunun elemanlarının sabit nokta uzaylarının boyutlarına ilişkin uygulamasının olabileceği muhtemel görünmektedir.

Anahtar Kelimeler: üretici graf, hamilton döngü, simetrik grup, alterne grup.

To my parents

ACKNOWLEDGMENTS

First and foremost, I would like to extend my best regards and sincere thanks to my supervisor, Professor Gülin Ercan, for her encouragement and assistance to achieve my full potential and for keeping my spirits high in the face of difficulties. This thesis would have never seen the light of day without her wisdom and guidance. I would not be able to reciprocate her personal favours on me at all, however, her praiseworthy contributions to my maturing into a young intellectual will very much be appreciated in my entire life.

My heartfelt thanks are also due to my co-supervisor, Dr Attila Maróti, for his substantial and generous contributions to my thesis and his unceasing efforts to keep me motivated from the very beginning. This thesis would be nowhere near complete in his absence. Among many memories I hold dear are the friendly discussions we had and the social times we spent during my visits to Budapest and Kaiserslautern. I also very highly value the email correspondence we kept up for many years.

My humble thanks go to Professor Gunter Malle for having me as a guest visitor in TU Kaiserslautern, Germany for one year. I also thank him for the regular seminars there, which had a great influence on me.

I am deeply indebted to my parents for their endless support.

I also owe a debt of gratitude to all my friends, especially to Ahmet Sınak and Şükran Gül for their genuine friendship over the years.

Finally, I acknowledge financial support from TÜBİTAK during my PhD years.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Hamiltonian cycles in Cayley graphs

We say that a group G is generated by a subset X if the only subgroup of G containing X is G itself. Generating sets play an important role in group theory and combinatorics. One of the most important related construction is the (directed) Cayley graph. This is the graph whose vertex set is G and two elements g and h are connected by a directed edge (labelled by x) if $g = hx$ where $x \in X$. The corresponding undirected and unlabelled graph is called a Cayley graph. There are many interesting conjectures on Cayley graphs. For example, a weaker form of a conjecture of Lovász, stated in 1969, states that in a finite and connected Cayley graph there always exists a Hamiltonian cycle. In 1996 Babai [3] published a conjecture sharply contradicting this conjecture. In this thesis we will also consider Hamiltonian cycles but in a slightly different setting.

1.2 Generation of symmetric groups

The other mathematical structure this thesis is concerned with is a finite group which can be generated by 2 elements. Many interesting groups have this property. For example, it is easy to see that the symmetric group S_n of degree n can be generated by 2 elements. In 1882 Netto conjectured that almost all pairs of permutations in S_n generate S_n or the alternating group A_n. This conjecture was proved almost a century later by Dixon [25]. Dixon considered the probability $p(S_n)$ that a random pair of elements from the symmetric group S_n (with respect to the uniform distribution) generates either S_n or the alternating group A_n. He proved that this probability tends to 1 as n tends to infinity. More precisely, he proved that for sufficiently large n we have $1-2/(\ln\ln n)^2 < p(S_n)$. This estimate was improved by Bovey and Williamson [7] to $1 - e^{-\sqrt{\ln n}} < p(S_n)$ for sufficiently large n. In 1980 a better lower bound of the form $1 - n^{-1+o(1)}$ was given by Bovey [8]. Then, proving a conjecture of Dixon, Babai [2] showed that $p(S_n) = 1 - (1/n) + O(1/n^2)$. Finally, Dixon [25] established an even better asymptotic formula for $p(S_n)$ namely

$$1 - \frac{1}{n} - \frac{1}{n^2} - \frac{4}{n^3} - \frac{23}{n^4} - \frac{171}{n^5} - \frac{1542}{n^6} + O(1/n^7).$$

For an alternative proof of this asymptotic formula using [19] see [20]. The latter two results depend on the Classification of Finite Simple Groups. Everything said above about $p(S_n)$ is also true for the probability $p(A_n)$ of a random pair of elements of A_n (with respect to the uniform distribution) that generates A_n. For an explicit, asymptotically sharp lower and upper bound for $p(A_n)$ and $p(S_n)$ see [49] and [50]. The most recent result on the probability of generating the symmetric or alternating groups is obtained by Virchow [58]. His proof does not depend on the Classification of Finite Simple Groups.

1.3 The probability to generate a simple group

The alternating group A_n is a non-abelian simple group for $n \geq 5$. All non-abelian finite simple groups can be generated by 2 elements. This was proved by Steinberg [54] and Aschbacher and Guralnick [1]. Thus it makes sense to consider, for a non-abelian finite simple group G, the probability $p(G)$ that a random pair of elements from G generate G. Dixon [26] conjectured that $p(G)$ tends to 1 as the size of the non-abelian finite simple group G tends to infinity.

Kantor and Lubotzky [37] confirmed Dixon's conjecture for classical (and small rank exceptional) groups. Later the proof of Dixon's conjecture was completed by Liebeck and Shalev in [40], where the large rank exceptional groups of Lie type were dealt with.

1.4 $3/2$-generated groups

Steinberg [54] introduced a stronger generation property for finite groups than that of 2-generation. A finite group G is said to be $3/2$-generated if for every non-identity element g in G there exists an $h \in G$ such that g and h generate G; that is, $G = \langle g, h \rangle$. Steinberg conjectured that every non-abelian finite simple group is $3/2$-generated. This was proved by Guralnick and Kantor in [35]. In fact, there is a related more general notion, the notion of spread. A group G is said to have spread k if for any non-identity elements $g_1, \dots, g_k$ there exists an element $g \in G$ such that $\langle g, g_i \rangle = G$ for every i with $1 \leq i \leq k$. In this language a group is $3/2$-generated if and only if it has spread 1. Later, Breuer, Guralnick, Kantor [10] proved that every non-abelian finite simple group has spread 2. In the same paper they conjectured that every finite group of spread 1 is also a group of spread 2. This conjecture has been reduced by Guralnick [34] to the case of almost simple groups and work on such group was carried out by Burness and Guest [16].

1.5 The notion of the generating graph

In another paper on the probability $p(G)$ to generate a non-abelian finite simple group G Liebeck and Shalev [41] proved that

$$1 - \frac{c_1}{m(G)} < p(G) < 1 - \frac{c_2}{m(G)}$$

for some universal positive constants c_1 and c_2 where $m(G)$ denotes the minimal index of a proper subgroup in G. (In case G is an alternating group, this was conjectured earlier by Dixon and proved by Babai [2].) This result has an interesting corollary. To state the result we need to introduce the notion of the generating graph.

Definition 1.5.1. Let G be a finite group that can be generated by 2 elements. The generating graph $\Gamma(G)$ of G is the graph whose vertex set consists of the non-identity elements of G and two vertices are connected by an edge if and only if they generate G.

By a result of Turán [57] in graph theory, there exists a positive universal constant c such that whenever G is a non-abelian simple group the graph $\Gamma(G)$ contains a clique of size at least $c \cdot m(G)$ (see [41, Corollary 1.7]). This was the first point when the generating graph was (at least) implicitly defined (and used).

It is an easy observation that the clique number $\omega(\Gamma(G))$ of the generating graph $\Gamma(G)$ of a finite group G is a lower bound for the minimal number $\sigma(G)$ of proper subgroups of G whose (set-theoretic) union is the whole group G. This invariant $\sigma(G)$ has been much investigated in the literature. For example, Tomkinson [56] showed that $\sigma(G) - 1$ is always a prime power when G is a finite (non-cyclic) solvable group and there is no group G (finite or infinite) such that $\sigma(G) = 7$.

The name "generating graph" comes from the well-known notion of the commuting graph. The commuting graph of a group G is the graph defined on the elements of G in such a way that two elements are connected by an edge if and only if they commute. This graph has much been investigated in group theory. Here we only mention two papers which are in some sense related to the present thesis. Brown [12,13] investigated the minimal number of abelian subgroups of the symmetric group S_n whose union is S_n in connection with the largest size of a clique in the commuting graph of S_n.

1.6 The study of generating graphs

The generating graph was investigated by Lucchini and Maróti in [44], [45], and [43]. For example, in [44], it is shown that for a nilpotent by nilpotent finite group G the clique number of $\Gamma(G)$ is equal to the chromatic number of $\Gamma(G)$. It would be nice to know whether this last statement holds for any solvable group G. In some sense this would generalize the above mentioned result of Tomkinson on $\sigma(G)$ when G is solvable.

Let G be a finite group that can be generated by 2 elements. Obviously the Frattini subgroup $\Phi(G)$ of G induces an empty subgraph in $\Gamma(G)$. Let $\Delta(G)$ be the subgraph of $\Gamma(G)$ induced by all non-isolated vertices in $\Gamma(G)$. A very interesting result of Crestani and Lucchini [21] is that $\Delta(G)$ is a connected graph in case G is a solvable group. In fact, Lucchini [42] established that for a solvable group G the diameter of $\Delta(G)$ is at most 3. The question arises: is $\Delta(G)$ a connected graph for an arbitrary finite group G, and if so, what can be said about its diameter?

This question has already been answered by Breuer, Guralnick and Kantor [10] in case G is a non-abelian finite simple group, since the spread of such a G is 2. Another interesting case is when G is a direct product of n copies of a non-abelian finite simple group S. Such a group need not be 2-generated. Let $\delta = \delta(S)$ be the largest integer n such that $G = S^n$ can be generated by 2 elements. Crestani and Lucchini [22] showed that $\Delta(S^\delta)$ is a 1-transitive connected graph. They also proved that the diameter of $\Delta(S^\delta)$ is at most 4δ if $|S|$ is large enough. Later Burness and Crestani [15] showed that $\operatorname{diam}(\Delta(S^2)) = 2$. This generalizes the previously mentioned result in [10]. There are some further investigations in [22] on the clique number of $\Delta(S^\delta)$. For example, for $S = A_5$ we have $\delta = 19$ and $\operatorname{diam}(\Delta((A_5)^{19})) = 4$.

1.7 A conjecture on the spread of finite groups

Breuer, Guralnick, Kantor proposed the following conjecture [10, Conjecture 1.8].

Conjecture 1.7.1 (Breuer, Guralnick, Kantor)**.** *A finite group G has spread 1 (or equivalently is $3/2$-generated) if and only if G/N is cyclic for every non-trivial normal subgroup N of G.*

Note that one direction of this conjecture is trivial, since if G is a finite group with a non-trivial normal subgroup N of G with the property that G/N is non-cyclic, then for any non-identity element n of N and any element $g \in G$ we have $\langle n, g\rangle < G$. Conjecture 1.7.1 has been reduced by Guralnick [34] to the case of almost simple groups G and work on almost simple groups has been carried out by Burness and Guest in [16]. In the language of generating graphs the conjecture states that $\Gamma(G)$ has a unique isolated vertex if and only if G/N is cyclic for every non-trivial normal subgroup N of G.

1.8 Hamiltonian cycles in generating graphs

In this thesis we consider the following stronger conjecture [11, Conjecture 1.6] than Conjecture 1.7.1.

Conjecture 1.8.1 (Breuer, Guralnick, Lucchini, Maróti, Nagy)**.** *Let G be a finite group of order at least 4. There is a Hamiltonian cycle in the generating graph $\Gamma(G)$ of G if and only if G/N is cyclic for every non-trivial normal subgroup N of G.*

This conjecture is known to be true for solvable groups [11, Proposition 1.1], for sufficiently large non-abelian simple groups [11, Theorem 1.2], for sufficiently large symmetric groups [11, Theorem 1.3], for certain wreath products [11, Theorem 1.4], for all almost simple groups whose socle is a sporadic simple group [11, Theorem 1.5], and for some small groups including all non-abelian simple groups of orders at most 10^7 (see [11, Section 8]).

1.9 The main theorem

One purpose of this thesis was to study Conjecture 1.8.1 for alternating and symmetric groups. In the work of Breuer, Guralnick, Lucchini, Maróti, Nagy [11] no explicit bound was given for the degree n of an alternating group A_n and a symmetric group S_n such that $\Gamma(A_n)$ and $\Gamma(S_n)$ are Hamiltonian. In fact only the existence of such a bound was established with no information at all on its possible size.

In this thesis we prove the following.

Theorem 1.9.1 (The main theorem). *The generating graphs $\Gamma(S_n)$ and $\Gamma(A_n)$ are Hamiltonian for $n \geq 107$.*

Note that the generating graph of S_n and of A_n is known to be Hamiltonian for integers n with $5 \leq n \leq 13$. This was established by computer calculations in [9].

The proof of Theorem 1.9.1 has two parts. The first part is group theoretic and uses deep results on generation properties of alternating and symmetric groups. A main tool is a result of Babai and Hayes [4] which in turn depends on a complicated theorem of Łuczak and Pyber [47]. One of the difficulties of our proof was to replace the full power of [47] with a more direct argument. We relied on basic properties of fixed point ratios, a subject much investigated in recent years. The proof of Theorem 1.9.1 relies on a structure theorem for primitive permutation groups, called the O'Nan–Scott theorem. We apply a bound on the orders of primitive permutation groups $G \leq S_n$ and a bound on the number of conjugacy classes of primitive permutation groups in S_n and A_n. As a by-product of these investigations we obtain explicit bounds in the paper by Babai and Hayes [4], and we believe that these bounds could be applied in future works. The second part of the proof uses results from graph theory. In general if the list of vertex degrees of a finite simple graph is given, then a lot of information can be deduced about the graph. For example, in certain cases, it can be decided whether the graph contains a Hamiltonian cycle or not.

1.10 An application to fixed point spaces

Let F be an arbitrary field and G a finite group. Let V be a finite dimensional FG-module. Assume that no non-zero vector in V is fixed by all elements of G. In other words, assume that $C_V(G) = 0$. For an element g in G denote the fixed point space of g acting on V by $C_V(g)$. This is a subspace of V. Let the F-dimension of $C_V(g)$ be denoted by $\dim(C_V(g))$.

In group theory it was important to establish a bound on the average dimension of fixed point spaces of elements of a finite group acting on a vector space. For this purpose set $\mathrm{avgdim}(G,V) = (1/|G|)\sum_{g\in G}\dim(C_V(g))$. In his 1966 PhD thesis Neumann [51] conjectured that if V is a non-trivial irreducible FG-module, then $\mathrm{avgdim}(G,V) \leq (1/2)\dim(V)$. This was eventually proved by Guralnick and Maróti in [36].

Neumann [51] showed that if V is a non-trivial irreducible FG-module for a field F and a finite solvable group G then there exists an element g of G with $\dim(C_V(g)) \leq (7/18)\dim(V)$. In fact, Neumann conjectured that for any finite group G there should exist $g \in G$ such that $\dim(C_V(g)) \leq (1/3)\dim(V)$. This was eventually proved by

Guralnick and Malle in [33].

Assume that G is a finite group with the property that $\Gamma(G)$ contains a Hamiltonian cycle. By [11, Proposition 1.7], we have

$$\frac{1}{|G|-1}\sum_{1\neq g}\dim(C_V(g)) \leq \frac{1}{2}\dim(V),$$

which is slightly weaker than the above-mentioned result of Guralnick and Maróti [36]. However, by the same argument, it follows that there are at least $(|G|-1)/2$ elements in G with fixed point space of dimension at most $\dim(V)/2$. In particular, for sufficiently large non-abelian finite simple groups G there are at least $|G|/2$ elements g of G with the property that $\dim(C_V(g)) \leq (1/2)\dim(V)$.

1.11 On recent results

Finally we mention two more recent papers on the generating graph of a finite group. Lucchini, Maróti, Roney-Dougal [46] investigated the extent to which the generating graph $\Gamma(G)$ determines the isomorphism type of G provided that $\Gamma(G)$ has no isolated vertex. For example, if S is a sufficiently large non-abelian finite group and G is a finite group with $\Gamma(G) \cong \Gamma(S)$, then $G \cong S$. The same conclusion holds in case S is a sufficiently large symmetric group. Recently, Cameron, Lucchini, Roney-Dougal [17] investigated a new graph defined on a d-generated finite group G where d is any fixed integer, not necessarily 2. As an application of their results they described the automorphism groups of those generating graphs $\Gamma(G)$ which are connected.

CHAPTER 2

PERMUTATION GROUPS

2.1 Permutations

Let Ω be a set. Then the bijections from Ω to itself form a group under composition of maps. This group is called the **symmetric group** on Ω and is denoted $\mathrm{Sym}\,(\Omega)$. The set Ω is called the **permutation domain**. It is easy to see that $\mathrm{Sym}\,(\Omega) \cong \mathrm{Sym}\,(\Sigma)$ whenever Ω and Σ are sets having the same cardinality. Throughout the thesis Ω will be finite. When Ω has size n, we will take $\Omega = \{1, 2, \ldots, n\}$ unless explicitly stated otherwise and denote the resulting symmetric group by S_n.

An element of the symmetric group is called a **permutation** and a subgroup of the symmetric group is called a **permutation group**. A permutation $g \in S_n$ **fixes** an element $a \in \Omega$ if g maps a to itself, i.e., $g(a) = a$. A **cycle of length** k (or simply a k**-cycle**) is a permutation which permutes k elements cyclically and fixes all the other elements. More precisely, a permutation $g \in S_n$ is a k**-cycle** if $g(a_i) = a_{i+1}$ for $1 \leq i < k$, $g(a_k) = a_1$, and $g(a_j) = a_j$ for $k < j \leq n$, where the a_r are the elements of Ω. In this case g is written as $(a_1, a_2, \ldots, a_k)$. Two cycles are said to be **disjoint** if they have no element in common. Any permutation can be written as a product of disjoint cycles and this writing is unique up to an ordering of the cycles and the cyclic ordering of the elements within each cycle. This is called the **cycle decomposition** of the permutation. The cycles appearing in the decomposition will be referred to as **the cycles** of the permutation. (In fact, the cycles of a permutation are essentially its orbits in the natural action of the symmetric group.) We will often omit 1-cycles in the cycle decomposition unless no confusion arises as to which permutation group we are working in. For example, the permutation in S_6 sending 1 to 2, 2 to 1, 3 to 4, 4 to 5, 5 to 3, and 6 to itself can be written as $(1, 2)(3, 4, 5)(6)$ (or simply as $(1, 2)(3, 4, 5)$). The same permutation can also be written as $(4, 5, 3)(6)(2, 1)$ (or simply as $(4, 5, 3)(2, 1)$). A permutation is said to have **cycle type** $(1^{k_1}, 2^{k_2}, \ldots, n^{k_n})$ if its cycle decomposition consists of k_i distinct i-cycles for each $i = 1, \ldots, n$. Here we omit i^{k_i} if $k_i = 0$, and simply write i in place of i^{k_i} if $k_i = 1$. For example, the permutation above has cycle type $(1, 2, 3)$.

A 2-cycle is called a **transposition**. Under this terminology any cycle (hence any permutation) can be written as a product of transpositions: for example, the identity permutation (the only 1-cycle) can be written as $(1, 2)(1, 2)$ and for any integer $k \geq 2$ we have $(a_1, a_2, \ldots, a_k) = (a_1, a_2) \cdots (a_1, a_{k-1})(a_1, a_k)$. There are various ways of expressing a permutation as a product of transpositions (for example, we can include in the product the identity element $(1, 2)(1, 2)$ as many times as we want), however, if a permutation is written as a product of transpositions in two different ways, then either the number of transpositions in both cases is even or it is odd in both cases. A permutation is called **even** if it can be written as a product of an even number of transpositions and **odd** if it can be written as a product of an odd number of transpositions. It follows that a permutation must be either even or odd. The even permutations clearly form a subgroup of the symmetric group. This group is called the alternating group and is denoted A_n. The map from S_n to the group $\{1, -1\}$ defined by sending an even permutation to 1 and an odd permutation to -1 is a well-defined homomorphism and A_n arises as the kernel of this homomorphism. In particular, $|S_n : A_n| = 2$ and $A_n \trianglelefteq S_n$.

2.2 Group actions

Let G be a group and let Ω be a set. An action of G on Ω is a map φ from $\Omega \times G$ to Ω with the following properties:

(i) $\varphi(a, 1_G) = a$ for all $a \in \Omega$;

(ii) $\varphi(\varphi(a, g), h) = \varphi(a, gh)$ for all $a \in \Omega$ and all $g, h \in G$.

For simplicity, we suppress the name of the map and write a^g in place of $\varphi(a, g)$. Given an action of G on Ω we can define a group homomorphism from G to $\mathrm{Sym}(\Omega)$ by setting the image of $g \in G$ to be the permutation sending a to a^g, and this homomorphism is uniquely determined by the given action. Conversely, given any group homomorphism $\phi : G \to \mathrm{Sym}(\Omega)$ we can define an action of G on Ω by defining $a^g := \phi(g)(a)$. The homomorphism ϕ is called the **permutation representation** of G corresponding to the action. Therefore, there is a bijection between the set of group homomorphisms from G to $\mathrm{Sym}(\Omega)$ and the set of actions of G on Ω. In view of this identification, the actions of G on Ω are essentially the group homomorphisms from G to $\mathrm{Sym}(\Omega)$.

For a subset $S \subseteq \Omega$ and a subset $H \subseteq G$, we write $S^H = \{s^h \mid s \in S,\ h \in H\}$.

Definition 2.2.1. Let G be a group acting on a set Ω and let $S \subseteq \Omega$ be a subset.

(i) For $a \in \Omega$, the set $a^G = \{a^g \mid g \in G\}$ is called the **orbit** (more precisely, the G-orbit) containing a.

(ii) The set $\{g \in G \mid s^g = s \text{ for all } s \in S\}$ is called the **pointwise stabilizer** of S in G and is denoted $\mathrm{Stab}_G(S)$ or $G_{(S)}$. If $S = \{a\}$ for some $a \in \Omega$ then we simply write G_a in place of $G_{(S)}$.

(iii) The set $\{g \in G \mid S^g = S\}$ is called the **setwise stabilizer** of S in G and is denoted $\mathrm{Stab}_G(\{S\})$ or $G_{\{S\}}$.

(iv) S is called G**-invariant** if $S^G = S$ or equivalently $G = \mathrm{Stab}_G(\{S\})$.

(v) For $g \in G$, the set $\{s \in S \mid s^g = s\}$ is called the **fixed point subset** of g in S and is denoted $\mathrm{fix}_S(g)$.

Proposition 2.2.2 ([27, pp. 8, 13, 24])**.** *Let G be a group acting on a set Ω. Then the following hold.*

(i) *The distinct orbits form a partition of the underlying set Ω.*

(ii) *G-invariant subsets of Ω are exactly the unions of some G-orbits.*

(iii) *$G_{(S)}$ and $G_{\{S\}}$ are subgroups of G for any subset $S \subseteq \Omega$.*

(iv) *If $a, b \in \Omega$ such that $a = b^g$ for some $g \in G$, then $G_a = g^{-1}G_bg$.*

(v) ***(The orbit-stabilizer property)*** *$|a^G| = |G : G_a|$ for any $a \in \Omega$.*

(vi) ***(Orbit Counting Lemma)*** *The number of distinct orbits of the action of G on Ω is $(1/|G|) \cdot \sum_{g \in G} |\operatorname{fix}_\Omega(g)|$.*

Corollary 2.2.3. *Let G be a group and let $g \in G$. Then $|g^G| = |G : C_G(g)|$.*

We say that G is **transitive** on Ω (or G acts **transitively** on Ω) if there is only one orbit, i.e., for any $a, b \in \Omega$ there exists $g \in G$ such that $a^g = b$. The group G is called **intransitive** if it is not transitive. We say that G is **faithful** if the kernel of the permutation representation corresponding to the action is trivial, i.e., the identity element is the only element fixing all $a \in \Omega$.

2.3 Wreath products

Let H and K be groups, and let K act on a set of size n. Set $B := H \times \ldots \times H$ (n factors). We define the **wreath product** of H by K to be the semidirect product $B \rtimes K$ where the action of K on B is given by permuting the components:

$$(h_1, \ldots, h_n)^k = (h_{1^k}, \ldots, h_{n^k})$$

for all $(h_1, \ldots, h_n) \in B$ and $k \in K$.

This group is denoted by $H \wr K$, and the subgroup B is called the **base group** of the wreath product. Clearly, $|H \wr K| = |H|^n|K|$ provided that both H and K are finite.

2.4 Conjugacy classes and centralizers in S_n and A_n

In this section we investigate the conjugacy classes and centralizers in the symmetric and alternating groups.

Given groups $G_1, G_2, \ldots, G_n$ we denote their direct product by $\prod_{i=1}^n G_i$. Also, we denote the cyclic group of order n by C_n.

Proposition 2.4.1 ([59, p. 16])**.** ***(Centralizer of a permutation in*** S_n***)*** *Let g be a permutation of type $(1^{k_1}, 2^{k_2}, \ldots, n^{k_n})$. Then $C_{S_n}(g) \cong \prod_{i=1}^{n} C_i \wr S_{k_i}$, where the action of the wreath product is given by permuting the subscripts in the direct product of k_i copies of the group C_i. In particular, $|C_{S_n}(g)| = \prod_{i=1}^{n} i^{k_i} k_i!$.*

Proposition 2.4.2 ([59, p. 16])**.** ***(Conjugacy classes in*** S_n***)*** *Two permutations in S_n are conjugate if and only if they have the same cycle type.*

Since all permutations having the same cycle type form a single conjugacy class, the number of permutations in S_n having cycle type $(1^{k_1}, 2^{k_2}, \ldots, n^{k_n})$ is equal to $n!/\prod_{i=1}^{n} i^{k_i} k_i!$ by Corollary 2.2.3.

Let G be a group and $A \subseteq G$ be a subset. Then for $g \in G$ we denote by g^A the set of conjugates of g by the elements of A, i.e., $g^A = \{a^{-1}ga \mid a \in A\}$.

Proposition 2.4.3 ([59, pp. 16–17])**.** ***(Conjugacy classes in*** A_n***)*** *Let $g \in A_n$. Then the following hold.*

(i) $g^{S_n} = g^{A_n}$ *if g has a cycle of even length or two cycles of equal odd length.*

(ii) $g^{S_n} = g^{A_n} \sqcup g^{S_n \setminus A_n}$ *if all cycles of g have distinct odd lengths.*

It follows from Corollary 2.2.3 that in case (i) of the above proposition we have $|C_{S_n}(g) : C_{A_n}(g)| = 2$, and in case (ii) we have $C_{S_n}(g) = C_{A_n}(g)$.

The following result provides a tool for determining the cycle type of an integer power of a permutation.

Proposition 2.4.4. *Let g be a k-cycle. Let $m \in \mathbb{Z}$ and $d = \gcd(m, k)$. Then g^m is a product of d disjoint cycles of length k/d.*

2.5 Primitive permutation groups

Let G be a group acting on a set Ω. Then G also acts on the set of all partitions of Ω in the obvious way. This naturally leads to the following. A partition $\{\Omega_i \mid i \in I\}$ of Ω is called a **block system** if it is preserved under the action of G, i.e., $\{\Omega_i \mid i \in$

$I\} = \{\Omega_i^g \mid i \in I\}$ for all $g \in G$. The elements of the partition are called **blocks**. The partition consisting of the singletons and the partition consisting of the set Ω itself are preserved under any group action and hence are called the **trivial** block systems. Any other partition is called a **system of imprimitivity** for G. The group G is called **imprimitive** if it has a non-trivial system of imprimitivity, and is called **primitive** otherwise. The orbits of an intransitive group clearly form a block system, and hence any intransitive group acting faithfully on a set is imprimitive.

It is known that every normal subgroup of a primitive permutation group G is transitive.

A **minimal normal** subgroup of a finite group G is a non-trivial normal subgroup of G which does not properly contain any other non-trivial normal subgroup of G. The **socle** $\mathrm{soc}(G)$ of G is defined to be the subgroup generated by all the minimal normal subgroups of G. It turns out that a primitive permutation group G has at most two minimal normal subgroups.

Let G and H be two groups acting on the sets Ω and Σ, respectively. Then we say that the action of G on Ω is **isomorphic** to the action of H on Σ if there exist a bijection $f : \Omega \longrightarrow \Sigma$ and a group isomorphism $\phi : G \longrightarrow H$ such that $f(\alpha^g) = f(\alpha)^{\phi(g)}$ for all $\alpha \in \Omega$ and all $g \in G$.

A transitive action of a group G is isomorphic to the right multiplication action on the set of right cosets of a subgroup H of G (here H can be taken as the stabilizer of a point). Furthermore, the actions on the sets of cosets of two subgroups H and K are isomorphic if and only if H and K are conjugate in G.

It follows that determining all the transitive actions of G is the same as determining the conjugacy classes of subgroups of G.

Proposition 2.5.1 ([27, Corollary 1.5A]). *Let G be a group acting transitively on a set Ω of size at least 2. Then G is primitive if and only if one (and hence every since all point stabilizers are conjugate) point stabilizer is a maximal subgroup of G.*

It follows that determining the primitive actions of G is the same as determining the conjugacy classes of maximal subgroups of G. The O'Nan–Scott Theorem shows that many cases of this problem can be reduced to investigating almost simple groups G. For the definition of a group of diagonal type, of product action and more information on the O'Nan–Scott Theorem see [27, Chapter 4].

Theorem 2.5.2 ([27, Theorem 4.1A]). ***(O'Nan–Scott Theorem)*** *Let G be a finite primitive group of degree n. Let H be the socle of G. Then either*

1. *H is a regular elementary abelian p-group for some prime p, $n = p^m := |H|$, and G is isomorphic to a subgroup of the affine group $\mathrm{AGL}_m(p)$; or*

2. *H is isomorphic to a direct power T^m of a non-abelian simple group T and one of the following holds:*

   (a) *$m = 1$ and G is isomorphic to a subgroup of $\mathrm{Aut}(T)$;*

   (b) *$m \geq 2$ and G is a group of diagonal type with $n = |T|^{m-1}$;*

   (c) *$m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to T^d, G is isomorphic to a subgroup of the wreath product $U \wr \mathrm{Sym}(m/d)$ with the product action, and $n = l^{m/d}$ where l is the degree of U;*

   (d) *$m \geq 6$, H is regular, and $n = |T|^m$.*

2.6 Maximal subgroups of S_n and A_n

Let $G \leq S_n$ be an intransitive subgroup. Let Ω be the permutation domain. Then G has an orbit $\mathcal{O}$ of size less than n. Note that G is a subgroup of the subgroup $\mathrm{Sym}\,(\mathcal{O}) \times \mathrm{Sym}\,(\Omega \setminus \mathcal{O})$ which is the setwise stabilizer of the set $\mathcal{O}$ in S_n. Also, it turns out that the subgroup $\mathrm{Sym}\,(\mathcal{O}) \times \mathrm{Sym}\,(\Omega \setminus \mathcal{O})$ is an intransitive maximal subgroup of S_n exactly when $|\mathcal{O}| \neq n/2$.

Let $G \leq S_n$ be a transitive imprimitive subgroup. Then G preserves a system of b blocks each of size a for some integers a, b with $a > 1$, $b > 1$. Then G is a subgroup of the subgroup $S_a \wr S_b$ which consists of all elements in S_n preserving this block system. Also, it turns out that the group $S_a \wr S_b$ is a transitive imprimitive maximal subgroup of S_n.

Thus we have the following.

Proposition 2.6.1. *Let G be a maximal subgroup of S_n. Then one of the following holds.*

(i) *$G = S_a \times S_b$ with $n = a + b$ and $a \neq b$ (intransitive case).*

(ii) *$G = S_a \wr S_b$ with $n = ab$, $a > 1$, $b > 1$ (transitive imprimitive case).*

(iii) *G is primitive.*

Conversely, the groups in cases (i) *and* (ii) *are maximal in S_n.*

The following is a similar result for the alternating groups.

Theorem 2.6.2 ([38])**.** *Let G be a maximal subgroup of A_n. Then one of the following holds.*

(i) *$G = (S_a \times S_b) \cap A_n$ with $n = a + b$ and $a \neq b$ (intransitive case).*

(ii) *$G = (S_a \wr S_b) \cap A_n$ with $n = ab$, $a > 1$, $b > 1$ (transitive imprimitive case).*

(iii) *G is primitive.*

Conversely, the groups in cases (i) *and* (ii) *are maximal in A_n for $n \neq 8$.*

We note that Liebeck, Praeger and Saxl [38] determined the types of primitive maximal subgroups of S_n and A_n, however, it is not easy to deal with the primitive maximal subgroups of S_n and A_n. For the purposes of this thesis we will not use the full power of their result.

CHAPTER 3

BOUNDING VERTEX DEGREES

Our main purpose in this chapter is to give strong lower bounds on vertex degrees in the generating graphs of S_n and A_n. The results obtained in this chapter will be used in Chapter 4 to prove that the generating graphs of S_n and A_n are Hamiltonian provided that $n \geq 107$.

3.1 The result of Babai and Hayes

In 1969, Dixon [25] proved that the probability that a random pair of permutations from the symmetric group S_n generates the alternating group A_n or S_n tends to 1 as n tends to infinity. This result was a highlight of asymptotic group theory period and has many applications. Another way to state his result is the following. Let $\{E_n\}$ be a sequence of events. It is said that E_n holds with high probability if the limit of the probability of the events E_n is 1. In this language Dixon's result states that with high probability a random pair of permutations from S_n generates either A_n or S_n.

A generalization of Dixon's result was obtained by Babai and Hayes [4]. The purpose of this subsection is to state their result. Let G be any given permutation group of degree n. Assume that there are $o(n)$ points that are fixed by all elements of G (by $o(n)$ we mean any function $f(x)$ such that $f(n)/n$ tends to 0 as n tends to infinity). Let $\sigma \in S_n$ be chosen at random. The main result of Babai and Hayes [4, Theorem 1] is that with high probability G and σ generate A_n or S_n. For the purpose of this thesis we state the before-mentioned result in a different language (see [4, Remark 2]).

Theorem 3.1.1 (Babai, Hayes, 2006)**.** *For every $\epsilon > 0$ there exists $\delta > 0$ and an integer $n_0 > 0$ such that for every integer $n \geq n_0$ if $G \leq S_n$ has fewer than δn fixed* *points then the probability that G and a random permutation in S_n generate A_n or S_n is at least $1-\epsilon$.*

In this thesis we will need an explicit version of this result.

3.2 The result of Łuczak and Pyber

The proof of Theorem 3.1.1 depends on a result of Łuczak and Pyber [47]. Let $\sigma \in S_n$ be a random permutation. Then with high probability σ does not belong to any transitive subgroup of S_n other than A_n or S_n. We state this in the following form.

Theorem 3.2.1 (Łuczak, Pyber, 1993)**.** *Let $\mathcal{M}$ be the set of transitive subgroups of S_n apart from A_n. Then $|\bigcup_{M\in\mathcal{M}} M|/|S_n| \to 0$ as n tends to infinity.*

This theorem has many applications apart from Theorem 3.1.1. For an account of these applications see [29, p.3].

Let us denote the proportion in the statement of Theorem 3.2.1 by $T(n)$. The method of Łuczak and Pyber can be used to show that $T(n) = O(n^{-c})$ for some small $c > 0$.

Denote by $P(n)$ the proportion of elements in S_n which belong to a primitive (maximal) subgroup of S_n not containing A_n. The fact that $P(n)$ tends to 0 as n tends to infinity is due to Bovey [8]. Recently this result has been improved by Diaconis, Fulman and Guralnick in [23, Theorem 7.6]. This states that $P(n) = O(n^{-2/3+\alpha})$ for any $\alpha > 0$. They conjectured that $P(n) \leq O(n^{-1})$. Eberhard, Ford and Koukoulopoulos [29] proved that $P(n) = n^{-1+o(1)}$.

Let $I(n)$ be the proportion of elements in S_n which belong to a (maximal) transitive imprimitive subgroup of S_n. The most recent upper bound for $I(n)$ can be found in [29, Theorem 1.2]. We do not state this here. We note that this is also an asymptotic estimate.

Notice that $T(n) = P(n) + I(n)$. Eberhard, Ford and Green [28] showed that if n is an even integer greater than 2 then $T(n) \geq cn^{-\delta}(\ln n)^{-3/2}$ for some constant $c > 0$.

Let X and Y be two real-valued functions. We mean by $X \ll Y$ that $|X| \leq c|Y|$ for some constant c. We also write $X \asymp Y$ to mean that $c_1|Y| \leq |X| \leq c_2|Y|$ for some constants $c_1, c_2 > 0$.

The following result of Eberhard, Ford and Green provides an asymptotic estimate for $T(n)$.

Theorem 3.2.2 (Eberhard, Ford, Green [28]). *Let $T(n)$ be the proportion of $\pi \in S_n$ contained in a transitive subgroup other than S_n or A_n, and let p be the smallest prime factor of n. Then*

$$T(n) \asymp \begin{cases} n^{-\delta_2(\log n)^{-3/2}} & \textit{if } p = 2, \\ n^{-\delta_3(\log n)^{-3/2}} & \textit{if } p = 3, \\ n^{-1+1/(p-1)} & \textit{if } 5 \leq p \ll 1, \\ n^{-1+o(1)} & \textit{if } p \to \infty, \end{cases}$$

where

$$\begin{aligned} \delta_m &= \int_1^{(m-1)/\log m} (\log t) dt \\ &= 1 - \frac{m-1}{\log m} + \frac{(m-1)\log(m-1)}{\log m} - \frac{(m-1)\log\log m}{\log m}. \end{aligned}$$

Note that all the above results are asymptotic. In this thesis we will avoid the use of such estimates since we aim for an explicit bound on the degree of a symmetric and alternating group whose generating graph contains a Hamiltonian cycle.

3.3 Fixed point ratios

Let G be a finite group acting on a finite set Ω. For a subset $S \subseteq G$ we denote by $\operatorname{fix}_\Omega(S)$ the set of elements in Ω that are fixed by all elements of S. The ratio $|\operatorname{fix}_\Omega(g)|/|\Omega|$ is called the fixed point ratio of the element g.

In this thesis we will use the following lemma, which is a slight generalization of a lemma of Liebeck and Saxl on the proportion of fixed points in a transitive action [39, Lemma 2.5].

Lemma 3.3.1. *Let G be a group acting transitively on a finite set Ω. Let $H = G_\omega$,*

$\omega \in \Omega$. Let $S \subseteq G$ be a subset and set $S^G = \{s^g \mid s \in S, g \in G\}$. Then we have the following.

(i) $\dfrac{|\operatorname{fix}_\Omega(S^G)|}{|\Omega|} \leq \dfrac{|S^G \cap H|}{|S^G|}$.

(ii) $\dfrac{|\operatorname{fix}_\Omega(g)|}{|\Omega|} = \dfrac{|g^G \cap H|}{|g^G|}$ *for all $g \in G$.*

Proof. We apply a double-counting argument. Let $T = \{(\beta, x) \mid \beta \in \Omega, x \in S^G \cap G_\beta\}$. Note that for any $\beta_1, \beta_2 \in \Omega$, we have $G_{\beta_2} = (G_{\beta_1})^g$ for some $g \in G$. Thus the map $S^G \cap G_{\beta_1} \longrightarrow S^G \cap G_{\beta_2}$ defined by $h \mapsto h^g$ is a well defined bijection, and so $|S^G \cap G_{\beta_1}| = |S^G \cap G_{\beta_2}|$. Thus we have

$$|T| = \sum_{\beta \in \Omega} |S^G \cap G_\beta| = \sum_{\beta \in \Omega} |S^G \cap H| = |\Omega| \cdot |S^G \cap H|. \tag{3.1}$$

On the other hand we have $\operatorname{fix}_\Omega(S^G) \subseteq \operatorname{fix}_\Omega(x)$ for any $x \in S^G$ and hence

$$|T| = \sum_{x \in S^G} |\operatorname{fix}_\Omega(x)| \geq |S^G| \cdot |\operatorname{fix}_\Omega(S^G)|. \tag{3.2}$$

Part (i) follows by comparing (3.1) and (3.2). Note that in the case $S = \{g\}$ for some $g \in G$, each $|\operatorname{fix}_\Omega(x)|$ in (3.2) can be replaced by $|\operatorname{fix}_\Omega(g)|$ since conjugate elements have the same number of fixed points. Thus in this case we have

$$|T| = \sum_{x \in g^G} |\operatorname{fix}_\Omega(g)| = |g^G| \cdot |\operatorname{fix}_\Omega(g)|. \tag{3.3}$$

Part (ii) follows now by comparing (3.1) and (3.3). □

Fixed point ratios for finite groups have been a subject of interest in group theory. Applications of this invariant can be found in the papers of Frohardt and Magaard [30, 31], Gluck and Magaard [32], Guralnick and Kantor [35], and Burness [14].

3.4 Basic observations

Let G be one of S_n or A_n, and let Γ be the generating graph of G, that is, $\Gamma = \Gamma(G)$. Let $1 \neq g \in G$. Denote by $d(g, \Gamma)$ the degree of the vertex g of Γ. By the definition of a generating graph, the vertex g is adjacent to a vertex h in the graph Γ if and only if $\langle g, h\rangle = G$. Note that this condition is equivalent to h not being contained in any maximal subgroup of G that contains g. Therefore, we have

$$\begin{aligned} d(g,\Gamma) &= |\{h \in G \setminus \{1\} \mid \langle g, h\rangle = G\}| \\ &= \left| G \setminus \bigcup_{M \in \mathcal{M}(g)} M \right|, \end{aligned}$$

where $\mathcal{M}(g)$ is the set of maximal subgroups of G which contain g.

For the purposes of this thesis, we need lower bounds on vertex degrees in $\Gamma(G)$. Thus we are mainly interested in bounding from above the probability that a random permutation in G is contained in a maximal subgroup that contains g, that is, bounding from above the ratio

$$\frac{\left|\bigcup_{M \in \mathcal{M}(g)} M\right|}{|G|}, \tag{3.4}$$

where $\mathcal{M}(g)$ is the set of maximal subgroups of G which contain g.

The following result indicates that most permutations have a relatively small number of fixed points.

Proposition 3.4.1 (see [4, Section 2])**.** *Let k be a positive integer. Then the proportion of permutations in S_n with at least k fixed points is at most $1/k!$.*

Proof. Let $\mathfrak{I}$ be the collection of k-element subsets of the permutation domain. Note that $|\mathfrak{I}| = \binom{n}{k}$. Also, for $A \in \mathfrak{I}$, we have $|\operatorname{Stab}_{S_n}(A)| = (n-k)!$. Therefore, the proportion of permutations with at least k fixed points is given by

$$\frac{|\bigcup_{A \in \mathfrak{I}} \operatorname{Stab}_{S_n}(A)|}{|S_n|} \leq \sum_{A \in \mathfrak{I}} \frac{|\operatorname{Stab}_{S_n}(A)|}{|S_n|} = \binom{n}{k} \cdot \frac{(n-k)!}{n!} = \frac{1}{k!}.$$

□

The next proposition implies that if $g \in S_n$ has f fixed points then the probability that a random permutation and g generate S_n is at most $1 - f/(2n)$. This means that if g has a relatively large number of fixed points then we cannot expect a strong lower bound on this probability and hence on the degree of the vertex g of $\Gamma(S_n)$.

Proposition 3.4.2 ([4, Proposition 3])**.** *Let $H \leq S_n$ be a permutation group having f fixed points. Then the probability that the group generated by H and a random permutation has a fixed point is at least $f/(2n)$.*

In this thesis we will not make an explicit reference to Proposition 3.4.2, however, we include it for interest and context as well as for a justification for imposing the bound of $\sqrt{n}$ on the number of fixed points of g in Sections 3.6–3.8.

In the light of Propositions 3.4.1 and 3.4.2, in Sections 3.6–3.8 we assume that g has at most $\sqrt{n}$ fixed points and study the ratio in (3.4) in the cases where M is primitive, intransitive and transitive imprimitive (see Theorems 3.6.5, 3.7.6 and 3.8.5). Together these prove:

Theorem 3.4.3. *For $n \geq 106$, if $g \in S_n$ has at most $\sqrt{n}$ fixed points, then the probability that a random permutation and g do not generate A_n or S_n is at most*

$$\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}.$$

In Section 4.3 the bound in Theorem 3.4.3 will be used together with a corresponding but weaker bound for elements with more than $\sqrt{n}$ fixed points (see Theorems 4.3.3 and 4.3.7) to establish the Hamiltonicity of $\Gamma(A_n)$ and $\Gamma(S_n)$ for $n \geq 107$.

3.5 Basic results

We begin by introducing a notion of projection of permutations onto a subset of the permutation domain (see [4]). This notion will be useful to make a reduction to the fixed-point-free case in Section 3.7.

Definition 3.5.1. Let $T \subseteq \Omega$ be a subset. We define the **projection** map $\mathrm{pr}_T : \mathrm{Sym}(\Omega) \to \mathrm{Sym}(T)$ by setting $\mathrm{pr}_T(\sigma) = \sigma_T$ for $\sigma \in \mathrm{Sym}(\Omega)$, where σ_T is defined as follows. For $i \in T$, let $i^{\sigma_T} = i^{\sigma^k}$ where k is the smallest positive integer with $i^{\sigma^k} \in T$.

We next state a special case of Stirling's formula.

Theorem 3.5.2 (Stirling's bound [5, p. 216])**.** *For every positive integer n,*

$$\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \leq n! \leq e\sqrt{n} \cdot \left(\frac{n}{e}\right)^n.$$

In some cases we will need weaker bounds that are easier to apply.

Proposition 3.5.3. *Let n be a positive integer. Then the following hold.*

(i) $n! \leq (n/2)^n$ *for* $n \geq 6$.

(ii) $n! \geq (n/3)^n$.

Proposition 3.5.4. *For every positive integers n and k with $1 \leq k \leq n$, we have*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \frac{n^k}{k!} < \left(\frac{n \cdot e}{k}\right)^k.$$

We note that Propositions 3.5.3 and 3.5.4 can be easily proven by induction.

Proposition 3.5.5. *Let a, b, c, d be non-negative integers. Then the following hold.*

(i) $\binom{a}{b} \leq \binom{c}{d}$ *if* $a \leq c$ *and* $b \leq d \leq c/2$.

(ii) $\binom{a}{b}\binom{c}{d} \leq \binom{a+c}{b+d}$.

Proof. Note that the statements are trivially true if $a < b$ or $c < d$. The statements are also true if $a = 0$ or $c = 0$. Thus we may assume that $a \geq b$, $c \geq d$, $a \neq 0$, $c \neq 0$. Note that $\binom{a}{b} \leq \binom{c}{b} \leq \binom{c}{d}$, and hence (i) follows. For (ii), let $S = S_1 \cup S_2$ where $S_1 = \{1, \ldots, a\}$ and $S_2 = \{a+1, \ldots, a+c\}$. Then, $\binom{a+c}{b+d}$ is the number of all $(b+d)$-element subsets of S whereas $\binom{a}{b}\binom{c}{d}$ is the number of $(b+d)$-element subsets of S that contain b elements from S_1 and d elements from S_2. □

3.6 The primitive case

Let $G = S_n$ and let $g \in G$ be a permutation with at most $\sqrt{n}$ fixed points. In this section we consider the probability that a random permutation in G is contained in a primitive maximal subgroup of G containing g. More precisely, we consider the ratio in (3.4) in the case M is primitive.

In order to prove the main result of this section we will need upper bounds on the order of the centralizer of g in G, on the order of a primitive permutation group, and on the number of conjugacy classes of primitive maximal subgroups of G.

First, we obtain an upper bound on the order of the centralizer of g in G. We first consider the case where g is fixed-point-free.

Lemma 3.6.1. *Let $g \in S_n$ be a fixed-point-free permutation. Then we have*

$$|C_{S_n}(g)| \leq 2^{\lfloor n/2 \rfloor} \cdot \lfloor n/2 \rfloor! \quad \textit{for } n \neq 3.$$

Proof. Let g have cycle type $(k_1^{m_1}, k_2^{m_2}, \dots, k_r^{m_r})$. Write $g = g_1 g_2 \cdots g_r$ where the g_i are the products of the m_i disjoint k_i-cycles in the cycle decomposition of g. Let Ω be the permutation domain and let $\Omega_i \subseteq \Omega$ be the set of elements that appear in a cycle of g_i. Put $G = S_n$ and $G_i = \mathrm{Sym}(\Omega_i)$ for all $i = 1, 2, \dots, r$. Then viewing G_i as a subgroup of G and g_i as an element of G_i, we have

$$C_G(g) = \prod_{i=1}^{r} C_{G_i}(g_i).$$

Note that $|\Omega_i| = m_i k_i$ and $n = |\Omega| = \sum_{i=1}^{r} |\Omega_i| = \sum_{i=1}^{r} m_i k_i$. It is sufficient to show that

$$|C_{G_i}(g_i)| \leq 2^{\lfloor \frac{m_i k_i}{2} \rfloor} \cdot \lfloor \frac{m_i k_i}{2} \rfloor!$$

since then it will follow that

$$|C_G(g)| \leq \prod_{i=1}^{r} \left(2^{\lfloor \frac{m_i k_i}{2} \rfloor} \cdot \lfloor \frac{m_i k_i}{2} \rfloor! \right) \leq 2^{\lfloor \frac{n}{2} \rfloor} \cdot \lfloor \frac{n}{2} \rfloor!.$$

So we may in fact assume that g is a product of b disjoint cycles of length a. Since $C_G(g) \subseteq C_G(g^i)$ for every integer i, raising g to a suitable power we may further assume that g is of prime order, i.e. a is a prime. Now we have $n = ab$ and $|C_G(g)| = a^b b!$. Thus we need to show

$$a^b b! \leq 2^{\lfloor \frac{ab}{2} \rfloor} \cdot \lfloor \frac{ab}{2} \rfloor!. \tag{3.5}$$

Note that $a^b \leq 2^{\lfloor a/2 \rfloor b} \leq 2^{\lfloor ab/2 \rfloor}$ for $a \neq 3, 5$, and $b! \leq \lfloor ab/2 \rfloor!$. Therefore (3.5) is satisfied for $a \neq 3, 5$. We now treat the remaining cases.

$a = 3$: If $b = 2k$ for some $k \geq 1$, then we have

$$a^b b! = 3^{2k}(2k)! \leq 2^{3k} 2^k (2k)! \leq 2^{3k}(3k)! = 2^{\lfloor ab/2 \rfloor} \lfloor ab/2 \rfloor!.$$

If $b = 2k + 1$ for some $k \geq 1$ then we have

$$\begin{aligned} a^b b! = 3^{2k+1}(2k+1)! \leq 2^{4k+1}(k+1)^k(2k+1)! &= 2^{3k+1}(2k+2)^k(2k+1)! \\ &\leq 2^{3k+1}(3k+1)! \\ &= 2^{\lfloor ab/2 \rfloor} \lfloor ab/2 \rfloor!. \end{aligned}$$

$a = 5$: If $b = 1$ then (3.5) is trivially satisfied. Suppose then that $b > 1$. We have $2^{\lfloor ab/2 \rfloor} \lfloor ab/2 \rfloor ! = 2^{\lfloor 5b/2 \rfloor} \lfloor 5b/2 \rfloor ! \geq 2^{2b}(2b)! \geq 2^{2b} b^b b! = (4b)^b b! \geq 5^b b! = a^b b!$. The proof is complete. □

We next consider the general case where g has at most $\sqrt{n}$ fixed points.

Lemma 3.6.2. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Then we have*

$$|C_{S_n}(g)| \leq 2^{\lfloor n/2 \rfloor} \cdot \lfloor n/2 \rfloor ! \quad \textit{for } n \neq 3.$$

Proof. Put $G = S_n$ and let Ω be the permutation domain. Also let $\Omega_1 = \mathrm{fix}_\Omega(g)$, $\Omega_2 = \Omega \setminus \Omega_1$, and let $G_1 = \mathrm{Sym}(\Omega_1)$, $G_2 = \mathrm{Sym}(\Omega_2)$. Denote by f the number of fixed points of g, that is, $f = |\Omega_1|$. Viewing the subgroups G_1 and G_2 as subgroups of G, we have

$$C_G(g) \cong C_{G_1}(g_{\Omega_1}) \times C_{G_2}(g_{\Omega_2}),$$

where g_{Ω_i} is as in Definition 3.5.1. Note that g_{Ω_1} is the identity permutation on Ω_1 and so $|C_{G_1}(g_{\Omega_1})| = f!$. Note also that g_{Ω_2} is fixed-point-free on Ω_2, and so by Lemma 3.6.1, we have $|C_{G_2}(g_{\Omega_2})| \leq 2^{\lfloor (n-f)/2 \rfloor} \cdot \lfloor (n-f)/2 \rfloor !$. Thus it follows that

$$|C_G(g)| = |C_{G_1}(g_{\Omega_1})| \cdot |C_{G_2}(g_{\Omega_2})| \leq f! \cdot 2^{\lfloor (n-f)/2 \rfloor} \cdot \lfloor (n-f)/2 \rfloor !.$$

Set $c_r = r! \cdot 2^{\lfloor (n-r)/2 \rfloor} \cdot \lfloor (n-r)/2 \rfloor !$. We claim that $c_r \geq c_{r+2}$ for any non-negative $r \leq \sqrt{n} - 2$. By cancelling common factors we see that this holds if and only if $2\lfloor (n-r)/2 \rfloor \geq (r+2)(r+1)$. Clearly, $\lfloor (n-r)/2 \rfloor \geq (n-r-1)/2$, and hence it is enough to show that $n - r - 1 \geq (r+2)(r+1)$. This is true for $\sqrt{n} - 2 \geq r$. Therefore the claim is established. Also, it is trivial to see that $c_0 \geq c_1$, and so it follows that $c_0 \geq c_r$ for any non-negative integer $r \leq \sqrt{n}$. Lemma 3.6.1 completes the proof of the lemma. □

The following result provides upper bounds on the numbers of conjugacy classes of primitive maximal subgroups of S_n and of A_n, and appears in a paper of Maróti and Tamburini [49, Lemma 4.1], the proof of which depends on work of Stringer [55].

Theorem 3.6.3 ([49, Lemma 4.1])**.** *Let G be one of S_n or A_n and let $r(G)$ be the number of conjugacy classes of primitive maximal subgroups of G other than A_n. Then the following hold.*

(i) $r(G) \leq n^{3(\log_2 n)^2}$ *for* $n \geq 1000$.

(ii) $r(G) \leq 36$ *for* $23 \leq n < 1000$.

We next state a result of Maróti that gives an upper bound on the orders of primitive permutation groups.

Theorem 3.6.4 ([48, Corollary 1.1])**.** *Let $G < S_n$ be a primitive permutation group not containing A_n. Then $|G| < 50n^{\sqrt{n}}$.*

We are now in a position to prove the main result of this section. We divide the proof into two parts, where in the first part the proof is purely group theoretic and in the second part GAP calculations are mainly used.

Theorem 3.6.5. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that a random permutation in S_n is contained in a primitive maximal subgroup of S_n that contains g and does not contain A_n. Then we have*

$$p \leq \frac{1}{n^2} \quad \textit{for } n \geq 27.$$

Proof. Put $G = S_n$. Let Σ be the set of primitive maximal subgroups of G other than A_n. Consider the conjugation action of G on Σ. Note that $H \in \mathrm{fix}_\Sigma(g)$ if and only if $g \in N_G(H) = H$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_k$ be the orbits of this action. Pick $H_i \in \mathcal{O}_i$ for each i. We have

$$\begin{aligned} p = \frac{|\bigcup_{g \in H \in \Sigma} H|}{|G|} = \frac{|\bigcup_{H \in \mathrm{fix}_\Sigma(g)} H|}{|G|} \leq \sum_{i=1}^{k} \frac{|\bigcup_{H \in \mathrm{fix}_{\mathcal{O}_i}(g)} H|}{|G|} &\leq \sum_{i=1}^{k} \frac{|\mathrm{fix}_{\mathcal{O}_i}(g)||H_i|}{|G|} \\ &= \sum_{i=1}^{k} \frac{|\mathrm{fix}_{\mathcal{O}_i}(g)|}{|\mathcal{O}_i|}, \end{aligned}$$

where the last equality follows from the orbit-stabilizer property (Theorem 2.2.2(v)) since $|\mathcal{O}_i| = |G : \mathrm{Stab}_G(H_i)| = |G : N_G(H_i)| = |G : H_i|$. Thus it is enough to show that

$$\frac{|\mathrm{fix}_{\mathcal{O}_i}(g)|}{|\mathcal{O}_i|} \leq \frac{1}{kn^2} \quad \text{for all } i = 1, \ldots, k.$$

Now fix an arbitrary orbit $\mathcal{O}$ and fix $H \in \mathcal{O}$. Note that the action of G is transitive on $\mathcal{O}$, and the subgroup H is a point stabilizer, namely $\mathrm{Stab}_G(H) = N_G(H) = H$. Thus by Lemma 3.3.1, we have

$$\frac{|\mathrm{fix}_{\mathcal{O}}(g)|}{|\mathcal{O}|} = \frac{|g^G \cap H|}{|g^G|}.$$

Note also that $|g^G| = |G : C_G(g)|$ by Corollary 2.2.3. Thus we have

$$\frac{|\operatorname{fix}_{\mathcal{O}}(g)|}{|\mathcal{O}|} = \frac{|g^G \cap H| \cdot |C_G(g)|}{|G|} \leq \frac{|H| \cdot |C_G(g)|}{|G|} \leq \frac{50n^{\sqrt{n}} \cdot 2^{\lfloor n/2 \rfloor} \cdot (\lfloor n/2 \rfloor)!}{n!},$$

where the last inequality follows from Lemma 3.6.2 and Theorem 3.6.4. Thus it suffices to show that

$$\frac{50n^{\sqrt{n}} \cdot 2^{\lfloor n/2 \rfloor} \cdot (\lfloor n/2 \rfloor)!}{n!} \leq \frac{1}{kn^2} \tag{3.6}$$

provided that $n \geq 27$. By Stirling's bound (Theorem 3.5.2), we have $\sqrt{2\pi n} \cdot (n/e)^n \leq n!$ and $(\lfloor n/2 \rfloor)! \leq e \cdot \sqrt{n/2} \cdot (n/(2e))^{n/2}$. Thus it is enough to show that

$$\frac{50n^{\sqrt{n}} \cdot 2^{n/2} \cdot e \cdot \sqrt{n/2} \cdot (n/(2e))^{n/2}}{\sqrt{2\pi n} \cdot (n/e)^n} \leq \frac{1}{kn^2},$$

or equivalently,

$$(e/\sqrt{\pi}) \cdot 25n^{\sqrt{n}+2} \cdot k \leq (n/e)^{n/2}. \tag{3.7}$$

Also, by Theorem 3.6.3 we have $k \leq 36$ for $n < 1000$, and $k \leq n^{3(\log_2 n)^2}$ for $n \geq 1000$. Using these we see that (3.7) holds for $n \geq 27$. This completes the proof. □

By the help of GAP we can improve the bound on n in Theorem 3.6.5.

Theorem 3.6.6. *Let G be one of S_n or A_n and let $g \in G$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that a random permutation in G is contained in a primitive maximal subgroup of G that contains g and is different from A_n. Then we have*

$$p \leq \frac{1}{n^2} \quad \textit{for } n \geq 15.$$

Proof. The result already holds for $n \geq 27$ by Theorem 3.6.5. We now show that the result also holds for $15 \leq n \leq 26$. In the proof of Theorem 3.6.5, the bounds on $|H|$ and k there were not strong enough to show that (3.6) holds for $15 \leq n \leq 26$. To this purpose, we show that (3.6) holds when the factor of $50n^{\sqrt{n}}$ is replaced by $|H|$ using the GAP program below. We first explain how the program works.

The function `nr()` calculates the exact number of conjugacy classes of primitive maximal subgroups of S_n other than A_n.

The function `max()` calculates the maximal size of a primitive subgroup of S_n other than A_n.

The function `check()` checks (3.6) for the exact value of k and the largest value of $|H|$; and returns `TRUE` if (3.6) is satisfied and returns `FALSE` otherwise.

Finally, the program prints `TRUE` if `check()` returns `TRUE` for all $15 \leq n \leq 26$, and prints `FALSE` otherwise.

```
nr:=function(n)
local a, l, m, s;
s:=SymmetricGroup(n);
a:=AlternatingGroup(n);
l:=MaximalSubgroupClassReps(s);
m:=Number(l, x->IsPrimitive(x,[1..n]) and
not IsSubset(x,a));
return(m);
end;

max:= function(n)
local a,l;
a:=AlternatingGroup(n);
l:=AllPrimitiveGroups(DegreeOperation, n,
x->IsSubset(x,a), false);
if l=[] then
return(0);
else
return(Maximum(List(l, x->Size(x))));
fi;
end;

check:=function(n)
if Factorial(n) >=
nr(n)*max(n)*(n^2)*(2^(Int(n/2)))*Factorial(Int(n/2))
then
return(true);
else
return(false);
fi;
end;

Print(ForAll([15..26], check));
```

□

3.7 The intransitive case

Let $G = S_n$ and let $g \in G$ be a permutation with at most $\sqrt{n}$ fixed points. In this section we consider the probability that a random permutation in G is contained in an intransitive maximal subgroup of G containing g. More precisely, we consider the ratio in (3.4) in the case M is intransitive.

In fact, in this section, we consider the more general situation where g is replaced by an arbitrary subgroup H with at most $\sqrt{n}$ fixed points. We obtain our desired result by setting $H = \langle g \rangle$.

We first obtain a result in the case where H is fixed-point-free and then consider the more general case.

Lemma 3.7.1. *Let $H \leq S_n$ be a fixed-point-free permutation group. Let p be the probability that H and a random permutation generate an intransitive group. Then we have*

$$p \leq \frac{11.9}{n} \quad \textit{for } n \geq 83.$$

Proof. Put $G = S_n$ and let Ω be the permutation domain. If H is transitive then there is nothing to prove. Thus we may assume that H is intransitive. Let $\mathcal{A}$ be the set of H-invariant subsets of Ω of size at most $n/2$. Note that for $g \in G$,

$$\begin{gathered}
\langle g, H\rangle \text{ is intransitive } \iff \\
\text{there is a proper } \langle g, H\rangle\text{-invariant subset of } \Omega \iff \\
\text{there is a proper subset of } \Omega \text{ that is both } g\text{-invariant and } H\text{-invariant } \iff \\
\text{there is a proper subset of } \Omega \\
\text{that is both a union of } g\text{-orbits and a union of } H\text{-orbits } \iff \\
g \in \operatorname{Stab}_G(\{T\}) \text{ for some } T \in \mathcal{A}.
\end{gathered}$$

We may therefore assume that each H-orbit has size 2 or 3. Suppose then that there are k orbits of size 2 and l orbits of size 3 of H so that $n = 2k + 3l$. Now,

$$\begin{aligned}
p = \frac{|\bigcup_{T\in\mathcal{A}} \operatorname{Stab}_G(\{T\})|}{|G|} \le \sum_{T\in\mathcal{A}} \frac{|\operatorname{Stab}_G(\{T\})|}{|G|} &= \sum_{T\in\mathcal{A}} \frac{|T|! \cdot (n-|T|)!}{n!} \\
&= \sum_{T\in\mathcal{A}} \frac{1}{\binom{n}{|T|}} \\
&= \sum_{t=2}^{\lfloor n/2\rfloor} \sum_{\substack{0\le r\le k\\ 0\le s\le l\\ t=2r+3s}} \frac{\binom{k}{r}\binom{l}{s}}{\binom{n}{t}}. \qquad (3.8)
\end{aligned}$$

Note that $k + l \le n/2$, and we have $r + s \le t/2$ and $t \le n/2$ in (3.8). Thus, by Proposition 3.5.5, we have

$$\binom{k}{r}\binom{l}{s} \le \binom{k+l}{r+s} \le \binom{\lfloor n/2\rfloor}{\lfloor t/2\rfloor} = \sqrt{\binom{\lfloor n/2\rfloor}{\lfloor t/2\rfloor}^2} \le \sqrt{\binom{n}{t}}.$$

Also, it is easy to see that the number of pairs (r, s) of non-negative integers with $t = 2r + 3s$ is at most $t/6 + 1 \le n/12 + 1$. We now have

$$\begin{aligned}
p &\le \sum_{t=2}^{\lfloor n/2\rfloor} \sum_{\substack{0\le r\le k\\ 0\le s\le l\\ t=2r+3s}} \frac{1}{\sqrt{\binom{n}{t}}} \\
&\le \sum_{t=2}^{5} \frac{1}{\sqrt{\binom{n}{t}}} + \sum_{t=6}^{\lfloor n/2\rfloor} \left(\frac{n}{12}+1\right) \cdot \frac{1}{\sqrt{\binom{n}{t}}} \\
&\le \sum_{t=2}^{5} \frac{1}{\sqrt{(\frac{n}{t})^t}} + \left(\frac{n}{2}-5\right) \cdot \left(\frac{n}{12}+1\right) \cdot \frac{1}{\sqrt{(\frac{n}{6})^6}} \\
&= \frac{2}{n} + \left(\frac{3}{n}\right)^{3/2} + \left(\frac{4}{n}\right)^2 + \left(\frac{5}{n}\right)^{5/2} + \frac{9(n^2+2n-120)}{n^3} \\
&\le \frac{11.9}{n},
\end{aligned}$$

where the last inequality holds since $n \ge 83$. □

As in Section 3.6, we use projections on to subsets in order to deal with the general case. We require the following two observations from [4].

Lemma 3.7.2 ([4, Observation 11])**.** *Let* $T \subseteq \Omega$*. Then the projection map* $\mathrm{pr}_T : \mathrm{Sym}(\Omega) \to \mathrm{Sym}(T)$ *is uniform, that is,*

$$|\,\mathrm{pr}_T^{-1}(g)| = \frac{|\Omega|!}{|T|!}$$

for all $g \in \mathrm{Sym}(T)$*.*

Lemma 3.7.3 ([4, Observation 12])**.** *Let* $g \in \mathrm{Sym}(\Omega)$ *and let* $T \subseteq \Omega$*. Let* $G \leq \mathrm{Sym}(T)$ *where* $\mathrm{Sym}(T)$ *is considered as a subgroup of* $\mathrm{Sym}(\Omega)$*. Then the orbits of the subgroup of* $\mathrm{Sym}(T)$ *generated by G and* g_T *are exactly the intersection of T with those orbits of the subgroup of* $\mathrm{Sym}(\Omega)$ *generated by G and g which have non-empty intersection with T.*

We are now ready to prove the general case.

Lemma 3.7.4. *Let* $H \leq S_n$ *be a permutation group with at most* $\sqrt{n}$ *fixed points. Let p be the probability that H and a random permutation generate an intransitive group. Then we have*

$$p \leq \frac{1}{\sqrt{n}} + \frac{15.2}{n} \quad \text{for } n \geq 104.$$

Proof. Put $G = S_n$ and let Ω be the permutation domain. Also, set $F = \mathrm{fix}_\Omega(H)$ and $R = \Omega \setminus F$. Let $g \in G$. Note that the group $\langle g, H\rangle$ is intransitive if and only if not all elements of R are in the same $\langle g, H\rangle$-orbit or there is a g-invariant subset of F, i.e., $g \in \mathrm{Stab}_G(\{A\})$ for some $A \subseteq F$. Let p_1 be the probability that there is a g-invariant subset of F, and let p_2 be the probability that not all elements of R are in the same $\langle g, H\rangle$-orbit. By the union bound, we have $p \leq p_1 + p_2$. Let $f = |F|$ so that $f \leq \sqrt{n}$.

Now,

$$\begin{aligned}
p_1 = \frac{|\bigcup_{A\subseteq F}\mathrm{Stab}_G(\{A\})|}{|G|} \leq \sum_{A\subseteq F}\frac{|\mathrm{Stab}_G(\{A\})|}{|G|} &= \sum_{i=1}^{f}\sum_{\substack{A\subseteq F\\|A|=i}}\frac{|\mathrm{Stab}_G(\{A\})|}{|G|}\\
&= \sum_{i=1}^{f}\binom{f}{i}\cdot\frac{i!(n-i)!}{n!}\\
&= \sum_{i=1}^{f}\frac{f(f-1)\cdots(f-i+1)}{n(n-1)\cdots(n-i+1)}\\
&\leq \sum_{i=1}^{f}\left(\frac{f}{n}\right)^i\\
&\leq \frac{f}{n}+\left(\frac{f}{n}\right)^2+(f-2)\left(\frac{f}{n}\right)^3\\
&\leq \frac{1}{\sqrt{n}}+\frac{1}{n}+\frac{\sqrt{n}-2}{n^{3/2}}\\
&\leq \frac{1}{\sqrt{n}}+\frac{2}{n}.
\end{aligned}$$

Now set $H_R = \{h_R : h \in H\}$, where h_R is as in Definition 3.5.1. Then,

$$\begin{aligned}
p_2 &= \frac{|\{g\in G:\ \text{not all elements of } R \text{ are in the same } \langle g,H\rangle\text{-orbit}\}|}{|G|}\\
&= \frac{|\{g\in G : \langle g_R,H_R\rangle \text{ is intransitive on } R\ \}|}{|G|}\\
&= \frac{(|\Omega|!/|R|!)|\{g\in \mathrm{Sym}(R) : \langle g,H_R\rangle \text{ is intransitive on } R\ \}|}{|\Omega|!}\\
&= \frac{|\{g\in \mathrm{Sym}(R) : \langle g,H_R\rangle \text{ is not transitive on } R\ \}|}{|R|!}\\
&\leq \frac{11.9}{n-f}\\
&\leq \frac{11.9}{n-\sqrt{n}},
\end{aligned}$$

where the second equality follows from Lemma 3.7.3, the third equality follows from Lemma 3.7.2, and the first inequality follows from Lemma 3.7.1 since H_R is fixed-point-free on R and $|R| = n-f \geq n-\sqrt{n} \geq 83$. Thus we have

$$p \leq p_1+p_2 \leq \frac{1}{\sqrt{n}}+\frac{2}{n}+\frac{11.9}{n-\sqrt{n}} \leq \frac{1}{\sqrt{n}}+\frac{15.2}{n},$$

where the last inequality holds since $n \geq 104$. □

We need an elementary lemma to prove the main results of this section.

Lemma 3.7.5. *Let $H \leq S_n$ be a permutation group. Let p_1 be the probability that a random permutation is contained in an intransitive maximal subgroup of S_n containing H. Let p_2 be the probability that H and a random permutation in S_n generate an intransitive subgroup. Then we have $p_1 \leq p_2$.*

Proof. Let M be an intransitive maximal subgroup of S_n containing H. Then for any $g \in M$, $\langle H, g \rangle \leq M$. Since $\langle H, g \rangle$ is contained in the intransitive subgroup M, it must be intransitive. Conversely, let $g \in S_n$ be a permutation such that the group $\langle H, g \rangle$ is intransitive. Then this group is contained in an intransitive maximal subgroup of S_n by the first paragraph of Section 2.6, and clearly contains H and g. The result now follows. □

We now state and prove the main results of this section.

Theorem 3.7.6. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that a random permutation is contained in an intransitive maximal subgroup of S_n containing g. Then we have*

$$p \leq \frac{1}{\sqrt{n}} + \frac{26}{n} \quad \textit{for } n \geq 496.$$

Proof. The proof follows from Lemmas 3.7.4 and 3.7.5 by setting $H = \langle g \rangle$. □

3.8 The transitive imprimitive case

Let $G = S_n$ and let $g \in G$ be a permutation with at most $\sqrt{n}$ fixed points. In this section we consider the probability that a random permutation in G is contained in a transitive imprimitive maximal subgroup of G containing g. More precisely, we consider the ratio in (3.4) in the case M is transitive imprimitive.

First, we give an easy combinatorial fact.

Lemma 3.8.1. *Let Ω be a set with n elements. Let $n = ab$, where $a, b \in \mathbb{Z}^+$. Then the number of partitions of Ω into b subsets of size a is*

$$\frac{n!}{(a!)^b \cdot b!}.$$

Note that the transitive imprimitive maximal subgroups of S_n containing g correspond to g-invariant partitions of the permutation domain into subsets of equal size greater than 1. Thus we are really interested in bounding the proportion of such g-invariant partitions.

We first state and prove the result in the case where the blocks have size at least 3 and then consider the remaining cases in another lemma.

Lemma 3.8.2. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let $\mathcal{S}$ be the set of partitions of the permutation domain into b blocks of size a, where $a > 2$ and $b > 1$. Let p be the proportion of g-invariant partitions in $\mathcal{S}$. Then we have*

$$p \leq \frac{1}{2n^{3/2}} \quad \textit{for } n \geq 57.$$

Proof. Let Ω be the permutation domain and let $c_1, \ldots, c_r$ be a subset of Ω containing exactly one element from each cycle of g. Denote by f the number of fixed points of g so that $f \leq \sqrt{n}$. Consider an arbitrary but fixed partition in $\mathcal{S}$ and label its blocks from 1 to b. We call such a partition a labelled partition. It is easy to see that a g-invariant labelled partition is uniquely determined by the placement of elements $c_1, \ldots, c_r$ in its blocks and the induced action of g on the set of its blocks. The number of ways of distributing the elements $c_1, \ldots, c_r$ into the blocks is at most b^r. Therefore, the number of g-invariant labelled partitions is at most $b^r b!$. Since there are $b!$ ways of labelling the blocks of a given partition in $\mathcal{S}$, it follows that the number of g-invariant partitions in $\mathcal{S}$ is at most b^r. Note also that $|\mathcal{S}| = n!/(a!^b b!)$ by Lemma 3.8.1. Using Stirling's bound (Theorem 3.5.2), we have

$$\begin{aligned} p \leq \frac{b^r}{n!/((a!)^b \cdot b!)} = \frac{b^r \cdot (a!)^b \cdot b!}{n!} &\leq \frac{b^r \cdot (e\sqrt{a}(a/e)^a)^b \cdot e\sqrt{b}(b/e)^b}{\sqrt{2\pi n}(n/e)^n} \\ &= \frac{e \cdot a^{b/2}}{\sqrt{2\pi n} \cdot b^{n-r-b-1/2}}. \end{aligned}$$

Thus it suffices to show that

$$\frac{e \cdot a^{b/2}}{\sqrt{2\pi n} \cdot b^{n-r-b-1/2}} \leq \frac{1}{2n^{3/2}} \tag{3.9}$$

for $n \geq 57$. Note that $n = ab$ and so (3.9) holds if and only if

$$e\sqrt{2/\pi} \cdot n^{b/2+1} \leq b^{n-r-b/2-1/2}. \tag{3.10}$$

Taking logarithms of both sides of (3.10), we see that (3.9) holds if and only if

$$1 + \ln(\sqrt{2/\pi}) + (b/2 + 1)\ln(n) + (b/2)\ln(b) \leq (n - r - 1/2)\ln(b). \qquad (3.11)$$

Note that r, the number of cycles of g, is maximum when all cycles of g are of length 1 or 2. Thus it follows that $r \leq f + (n - f)/2 \leq (n + \sqrt{n})/2$. Therefore, it is enough to show that

$$\frac{1 + \ln(\sqrt{2/\pi})}{\ln(b)} + \left(\frac{b}{2} + 1\right) \cdot \frac{\ln(n)}{\ln(b)} + \frac{b}{2} \leq \frac{n - \sqrt{n} - 1}{2}. \qquad (3.12)$$

(3.12) trivially holds for $b = 2$, $n \geq 31$ and also for $b = 3$, $n \geq 26$. Also holding n fixed, the left-hand side of (3.12) is an increasing function of b on $[4, \infty]$. Note that $b \leq n/3$ by assumption, and hence for $b \geq 4$ the inequality (3.12) is implied by

$$\frac{1 + \ln(\sqrt{2/\pi})}{\ln(n/3)} + \left(\frac{n}{6} + 1\right) \cdot \frac{\ln(n)}{\ln(n/3)} + \frac{n}{6} \leq \frac{n - \sqrt{n} - 1}{2},$$

which holds if and only if $n \geq 57$. This completes the proof. This completes the proof. □

We need the following lemma.

Lemma 3.8.3. *Let $g \in \mathrm{Sym}(\Sigma)$ be a fixed-point-free permutation all of whose cycles are of the same size. Denote by $n(g, \Sigma)$ the number of g-invariant partitions of Σ into blocks of size 2. Then $n(g, \Sigma)$ is maximal when the cycles of g are of size 2.*

Proof. Let $x \in \mathrm{Sym}(\Sigma)$ be a fixed-point-free involution and let $h \in \mathrm{Sym}(\Sigma)$ be a fixed-point-free permutation all of whose cycles are of the same size. We need to show that $n(h, \Sigma) \leq n(x, \Sigma)$. We may assume by raising h to a suitable power that h is fixed-point-free of order a prime p. If $p = 2$, there is nothing to prove. If $p > 2$, then we have $|\Sigma| = 2pk$ for some integer k (note that we may assume Σ has even size since otherwise there is nothing to prove). This means that there are pk cycles of x, each of length 2. Suppose first that k is even. The number of x-invariant partitions of Σ into blocks of size 2 where no block is fixed is equal to

$$\frac{(pk)!}{(2!)^{pk/2} \cdot (pk/2)!} \cdot 2^{pk/2} = \frac{(pk)!}{(pk/2)!}.$$

This follows since each such partition can be obtained by breaking the pk cycles into groups each consisting of two cycles and for each group forming a partition that is left invariant by these cycles. In particular, we have $n(x,\Sigma) \geq (pk)!/(pk/2)!$. On the other hand, h is a permutation having $2k$ cycles, each of length $p > 2$, and so an h-invariant partition can have no block fixed. Arguing as above and noting that there are p distinct ways of forming a partition out of two cycles of length p that is also left invariant by these cycles (distribute the elements in one cycle into p empty blocks and then there are p distinct ways of distributing the elements in the other cycle into the blocks), we see that

$$n(h,\Sigma) = \frac{(2k)!}{(2!)^k \cdot k!} \cdot p^k.$$

Assuming $pk \geq 8$, that is, $(p,k) \neq (3,2)$, we have

$$n(x,\Sigma) \geq \frac{(pk)!}{(pk/2)!} \geq \left(\frac{pk}{2}\right)^{pk/2} \geq \left(\frac{pk}{2}\right)^{3k/2} \geq (pk)^k \geq n(h,\Sigma).$$

Also for $(p,k) = (3,2)$, we have $n(x,\Sigma) \geq 6!/3! = 120 \geq 27 = n(h,\Sigma)$. Thus, the result holds for even k. Suppose now that k is odd. Arguing similarly as before, the number of x-invariant partitions with exactly one block fixed is equal to

$$\binom{pk}{1} \cdot \frac{(pk-1)!}{(2!)^{(pk-1)/2} \cdot ((pk-1)/2)!} \cdot 2^{(pk-1)/2} = \frac{(pk)!}{((pk-1)/2)!}.$$

In particular, we have $n(x,\Sigma) \geq (pk)!/((pk-1)/2)!$. Also, as before, $n(h,\Sigma) = (2k)!/((2!)^k k!) \cdot p^k$. Assuming $pk \geq 8$, that is, $(p,k) \notin \{(3,1),(5,1),(7,1)\}$ we have

$$\begin{aligned} n(x,\Sigma) \geq \frac{(pk)!}{((pk-1)/2)!} \geq \left(\frac{pk+1}{2}\right)^{(pk+1)/2} \geq \left(\frac{pk}{2}\right)^{pk/2} &\geq \left(\frac{pk}{2}\right)^{3k/2} \\ &\geq (pk)^k \\ &\geq n(h,\Sigma). \end{aligned}$$

Note that $n(h,\Sigma) \leq n(x,\Sigma)$ trivially holds for $(p,k) \in \{(3,1),(5,1),(7,1)\}$. Thus, the result also holds for odd k. The proof is complete. □

We now state and prove our result in the general case.

Lemma 3.8.4. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let $\mathcal{S}$ be the set of partitions of the permutation domain into b blocks of size a, where $a > 1$ and $b > 1$. Let p be the proportion of g-invariant partitions in $\mathcal{S}$. Then we have*

$$p \leq \frac{1}{2n^{3/2}} \quad \textit{for } n \geq 106.$$

Proof. By Lemma 3.8.2 we may assume that $a = 2$. Note that, in this case, a set of blocks cyclically permuted by g is permuted either by one cycle of even length or by two cycles of equal length. Write $g = g_{i_1} g_{i_2} \cdots g_{i_k}$ where $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ and g_{i_j} is the product of cycles of length i_j in the cycle decomposition of g. Let Ω_j be the subset of Ω consisting of the elements in the cycles of g_{i_j} so that $\Omega = \bigsqcup_{j=1}^{k} \Omega_j$. Note that if g is to fix a partition, the number of cycles of length i_j must be even for i_j odd. Thus we may assume that $|\Omega_j|$ is even for all j. Now, viewing g_{i_j} as an element of $\mathrm{Sym}(\Omega_j)$, a g-invariant partition of Ω can be regarded as a union of g_{i_j}-invariant partitions of Ω_j, for $j = 1, \ldots, k$. We now set some notation. For a set Σ and a permutation $h \in \mathrm{Sym}(\Sigma)$, denote by $n(h, \Sigma)$ the number of h-invariant partitions of Σ into blocks of size 2. Thus we have

$$n(g, \Omega) = \prod_{j=1}^{k} n(g_{i_j}, \Omega_j).$$

Fix some $i_j \geq 2$, and set $h = g_{i_j}$, $\Sigma = \Omega_j$. Let $x \in \mathrm{Sym}(\Sigma)$ be a fixed-point-free involution. By Lemma 3.8.3 we have $n(h, \Sigma) \leq n(x, \Sigma)$. We may therefore assume that g is an involution. Let c be the number of 2-cycles of g so that $n = f + 2c$. Arguing as above, we have $n(g, \Omega) = n(g_1, \Omega_1) \cdot n(g_2, \Omega_2)$. Clearly,

$$n(g_1, \Omega_1) = \frac{f!}{(2!)^{f/2} \cdot (f/2)!} \leq \left(\frac{f}{2}\right)^{f/2}.$$

The number of g_2-invariant partitions of Ω_2 into blocks of size 2 with exactly i blocks fixed is

$$c_i = \begin{cases} \binom{c}{i} \cdot \dfrac{(c-i)!}{(2!)^{(c-i)/2} \cdot ((c-i)/2)!} \cdot 2^{(c-i)/2} & \text{if } i - c \equiv 0 \pmod 2, \\ 0 & \text{if } i - c \equiv 1 \pmod 2. \end{cases}$$

$$= \begin{cases} \dfrac{c!}{i! \cdot ((c-i)/2)!} & \text{if } i - c \equiv 0 \pmod 2, \\ 0 & \text{if } i - c \equiv 1 \pmod 2. \end{cases}$$

Note that $c_i \leq c!$ for each i. Thus,

$$n(g_2, \Omega_2) = \sum_{i=0}^{c} c_i \leq c \cdot c!.$$

Note also that $|\mathcal{S}| = n!/((2!)^{n/2} \cdot (n/2)!) \geq (n/4)^{n/2}$. Using Stirling's bound (Theorem 3.5.2), we have

$$p = \frac{n(g,\Omega)}{|\mathcal{S}|} = \frac{n(g_1,\Omega_1)\cdot n(g_2,\Omega_2)}{|\mathcal{S}|} \le \frac{(f/2)^{f/2}\cdot c\cdot c!}{(n/4)^{n/2}}$$
$$= c\cdot c!\cdot\left(\frac{2f}{n}\right)^{f/2}\cdot\left(\frac{4}{n}\right)^{c}$$
$$\le c\cdot e\sqrt{c}\cdot\left(\frac{2f}{n}\right)^{f/2}\cdot\left(\frac{4c}{en}\right)^{c}.$$

Note that $f \le \sqrt{n}$ and $(n-\sqrt{n})/2 \le c \le n/2$. Thus we have

$$p \le e\cdot\left(\frac{n}{2}\right)^{3/2}\cdot\left(\frac{2}{e}\right)^{\frac{n-\sqrt{n}}{2}} \le \frac{1}{2n^{3/2}},$$

where the last inequality holds for $n \ge 106$. The proof is complete. □

We now state and prove the main results of this section.

Theorem 3.8.5. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that a random permutation is contained in a transitive imprimitive maximal subgroup of S_n containing g.*

$$p \le \frac{1}{n} \quad \textit{for } n \ge 106.$$

Proof. Let Σ be the collection of transitive imprimitive maximal subgroups of S_n containing g. For $a, b > 1$ with $ab = n$, let $\Sigma_{a,b} \subseteq \Sigma$ be the set of members of Σ that leave invariant a (unique) partition of the permutation domain into b blocks of size a so that $\Sigma = \bigsqcup_{\substack{a,b>1\\ n=ab}} \Sigma_{a,b}$. By Theorem 3.8.4, we have

$$|\Sigma_{a,b}| \le \frac{1}{2n^{3/2}}\cdot\frac{n!}{a!^b b!}.$$

Also, for $M \in \Sigma_{a,b}$, we have $|M| = a!^b b!$. Thus,

$$p = \frac{|\bigcup_{M\in\Sigma} M|}{|S_n|} \le \sum_{M\in\Sigma}\frac{|M|}{|S_n|} = \sum_{\substack{a,b>1\\ n=ab}}\sum_{M\in\Sigma_{a,b}}\frac{|M|}{|S_n|} = \sum_{\substack{a,b>1\\ n=ab}}|\Sigma_{a,b}|\cdot\frac{a!^b b!}{|S_n|} \le \sum_{\substack{a,b>1\\ n=ab}}\frac{1}{2n^{3/2}}$$
$$\le \frac{1}{n},$$

where the last inequality holds because the number of positive divisors of n is clearly at most $2\sqrt{n}$. □

3.9 Main results

We put together the results we have obtained so far to state and prove the main results of this chapter that will be used in Chapter 4 to prove the main theorem of the thesis (Theorem 1.9.1).

Theorem 3.9.1. *Let $g \in S_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that g and a random permutation generate S_n. Then for $n \geq 106$, we have*

$$p \geq \begin{cases} \frac{1}{2} - \left(\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}\right) & \text{if } g \in A_n, \\ 1 - \left(\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}\right) & \text{if } g \in S_n \setminus A_n. \end{cases}$$

Proof. Note that

$$p = \frac{|\{x \in S_n : \langle g, x\rangle = S_n\}|}{|S_n|}.$$

If $g \in S_n \setminus A_n$ then we have

$$p = \frac{|\{x \in S_n : \langle g, x\rangle \geq A_n\}|}{|S_n|}.$$

If $g \in A_n$ then we have

$$p \geq \frac{|\{x \in S_n : \langle g, x\rangle \geq A_n\}| - n!/2}{|S_n|} = \frac{|\{x \in S_n : \langle g, x\rangle \geq A_n\}|}{|S_n|} - \frac{1}{2}.$$

The result now follows from Theorem 3.4.3. □

Theorem 3.9.2. *Let $g \in A_n$ be a permutation with at most $\sqrt{n}$ fixed points. Let p be the probability that g and a random permutation generate A_n. Then we have*

$$p \geq 1 - 2 \cdot \left(\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}\right) \quad \text{for } n \geq 106.$$

Proof. Note that

$$\begin{aligned} p = \frac{|\{x \in A_n : \langle g, x\rangle = A_n\}|}{|A_n|} &\geq \frac{|\{x \in S_n : \langle g, x\rangle \geq A_n\}| - n!/2}{|A_n|} \\ &= 2 \cdot \frac{|\{x \in S_n : \langle g, x\rangle \geq A_n\}|}{|S_n|} - 1. \end{aligned}$$

The result now follows from Theorem 3.4.3. □

CHAPTER 4

HAMILTONIAN CYCLES IN GENERATING GRAPHS

In this chapter we use the results obtained in Chapter 3 to prove that the generating graphs of S_n and A_n are Hamiltonian provided that $n \geq 107$.

4.1 Graphs

In this section we introduce some basic terminology in graph theory.

A **graph** Γ is a finite, non-empty set $V = V(\Gamma)$ together with a set $E = E(\Gamma)$ of 2-element subsets of distinct elements of V. The set V is called the **vertex set** and the set E is called the **edge set**. Elements of V are called **vertices** and the members of E are called **edges**.

If $e = \{u, v\}$ is an edge in Γ, then u and v are said to be **adjacent**, and u (or v) and e are said to be **incident**. We denote the edge $\{u, v\}$ simply by uv or vu.

The **degree** $d(\Gamma, v)$ of a vertex v in Γ is the number of edges of Γ incident with v.

A graph Δ is a **subgraph** of the graph Γ if $V(\Delta) \subseteq V(\Gamma)$ and $E(\Delta) \subseteq E(\Gamma)$.

Let $U \subseteq V(\Gamma)$. Then the subgraph of Γ **induced** by U is the graph having U as its vertex set and whose edge set consists of those edges of Γ that are incident with two elements of U.

The graph Γ is called **bipartite** if the vertex set $V(\Gamma)$ can be partitioned into two subsets V_1 and V_2 such that every edge of Γ is incident with a vertex from V_1 and a vertex from V_2.

The graph Γ is called **complete** if every pair of its vertices are adjacent.

A **cycle** in Γ is a finite sequence $v_1, v_2, \ldots, v_n, v_1$ ($n \geq 3$) of adjacent vertices with $v_i \neq v_j$ for $i \neq j$.

The graph Γ is said to be **Hamiltonian** if it has a cycle that contains each of its vertices. Such a cycle is called a **Hamiltonian cycle**.

4.2 Hamiltonian cycles in graphs

We note that a Hamiltonian cycle is named after Sir William Rowan Hamilton, who devised a puzzle in which such a path along the polyhedron edges of a dodecahedron was sought (this is the Icosian game). The problem of establishing the existence of a Hamiltonian cycle in a graph has been investigated in the literature with respect to several parameters. For the purposes of this thesis we need results that depend on the vertex degrees. Roughly speaking, a graph contains a Hamiltonian cycle if it has "enough" edges.

Theorem 4.2.1 (Dirac, 1952 [24]). *A simple graph with $n \geq 3$ vertices is Hamiltonian if the degree of each vertex is at least $n/2$.*

The next result is due to Ore and can be viewed as a generalization of Dirac's result.

Theorem 4.2.2 (Ore, 1960 [52]). *A simple graph with $n \geq 3$ vertices is Hamiltonian if the sum of vertex degrees of every pair of distinct non-adjacent vertices is at least n.*

In 1962 Pósa gave a more general result.

Definition 4.2.3. Let Γ be a graph with n vertices and vertex degrees $d_1 \leq d_2 \leq \ldots \leq d_n$. Then Γ satisfies **Pósa's criterion** if $d_k \geq k+1$ for all positive integers k with $k < n/2$.

Theorem 4.2.4 (Pósa, 1962 [53]). *A graph is Hamiltonian if it satisfies Pósa's criterion.*

We note that Theorems 4.2.1 and 4.2.2 can be derived from Theorem 4.2.4.

Yet another result in this direction was given by Chvátal.

Definition 4.2.5. Let Γ be a graph with $n \geq 3$ vertices and vertex degrees $d_1 \leq d_2 \leq \ldots \leq d_n$. Then Γ satisfies **Chvátal's criterion** if $d_{n-i} \geq n - i$ whenever $d_i \leq i < n/2$.

Theorem 4.2.6 (Chvátal, 1972 [18])**.** *A graph is Hamiltonian if it satisfies Chvátal's criterion.*

The best vertex degree characterization of Hamiltonian graphs is due to Bondy and Chvátal.

Definition 4.2.7. Let Γ be a graph with n vertices. The **closure** $\mathrm{cl}(\Gamma)$ of Γ is the graph (with the same vertex set) constructed from Γ by adding for all non-adjacent pairs of vertices u and v with $d(\Gamma, u) + d(\Gamma, v) \geq n$ the new edge uv.

Theorem 4.2.8 (Bondy, Chvátal, 1972 [6])**.** *A graph is Hamiltonian if and only if its closure is Hamiltonian.*

4.3 Proof of the main theorem

In this section we prove the main theorem of the thesis (Theorem 1.9.1).

We first prove our result in the case of symmetric groups and then turn our attention to alternating groups.

Before we consider the two cases, we introduce some notation and make an observation that will be used in both cases.

Notation 4.3.1. Let $A_1(n)$ and $A_2(n)$ be the sets of permutations in $S_n \setminus A_n$ and A_n, respectively, with less than $\sqrt{n}$ fixed points. Set $B_1(n) = (S_n \setminus A_n) \setminus A_1(n)$ and $B_2(n) = A_n \setminus (A_2(n) \cup \{1\})$.

Lemma 4.3.2. *For $i = 1, 2$, we have*

$$|B_i(n)| \leq \frac{n!}{2(\lceil\sqrt{n}\rceil)!}.$$

Proof. $B_i(n)$ is the set of permutations in $S_n \setminus A_n$ and A_n, respectively, with at least $\lceil\sqrt{n}\rceil$ fixed points. Note that the number of $\lceil\sqrt{n}\rceil$-element subsets of the permutation domain is $\binom{n}{\lceil\sqrt{n}\rceil}$, and the number of permutations in $S_n \setminus A_n$ and in A_n fixing all elements in each such subset is $(n - \lceil\sqrt{n}\rceil)!/2$. Therefore, by union bound, we have

$$|B_i(n)| \leq \binom{n}{\lceil\sqrt{n}\rceil} \cdot \frac{(n - \lceil\sqrt{n}\rceil)!}{2} = \frac{n!}{2(\lceil\sqrt{n}\rceil)!}$$

for $i = 1, 2$. □

4.3.1 Symmetric groups

In this subsection we show that the generating graphs of symmetric groups of degree at least 107 satisfies Chvátal's criterion and hence are Hamiltonian.

We need a result of Breuer, Guralnick, Lucchini, Maróti and Nagy concerning minimal vertex degrees in a certain subgraph of $\Gamma(S_n)$.

Theorem 4.3.3 ([11, Theorem 6.1]). *Let $\Gamma_b(S_n)$ be the bipartite subgraph of $\Gamma(S_n)$ obtained by throwing away edges between elements in $S_n \setminus A_n$. Then for $n > 15$, the degree of every vertex in $\Gamma_b(S_n)$ is at least $n!/n^3$.*

We also set some notation.

Notation 4.3.4. For a graph Γ, we set $\mathrm{cl}^{(1)}(\Gamma) = \mathrm{cl}(\Gamma)$ and inductively set $\mathrm{cl}^{(i)}(\Gamma) = \mathrm{cl}(\mathrm{cl}^{(i-1)}(\Gamma))$ for every positive integer $i \geq 2$. The graph $\mathrm{cl}^{(i)}(\Gamma)$ is called the **i-th closure** of the graph Γ.

In the next lemma we investigate adjacency in the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$.

Lemma 4.3.5. *Let $n \geq 107$ be an integer. The set $S_n \setminus A_n$ induces a complete subgraph in the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$. Furthermore, every vertex in $A_1(n)$ is adjacent to every other vertex and every vertex in $B_1(n)$ is adjacent to at least $(n!/2)-1+(n!/n^3)$ other vertices in the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$.*

Proof. Set $\Gamma_0 = \Gamma(S_n)$. Since $1/\sqrt{n} + 16.2/n + 1/n^2 \leq 1/4$ for $n \geq 107$, by Theorem 3.9.1, for $u \in A_1(n)$ we have

$$d(\Gamma_0, u) \geq \left(1 - \left(\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}\right)\right) \cdot n! \geq \frac{3}{4}n!,$$

and for $v \in A_2(n)$ we have

$$d(\Gamma_0, v) \geq \frac{1}{4} n!.$$

We now show that in the graph $\Gamma_1 = \mathrm{cl}(\Gamma(S_n))$ the set $A_1(n)$ induces a complete subgraph and every vertex in $A_1(n)$ is adjacent to every vertex in $A_2(n)$.

The first claim holds since for any $u, v \in A_1(n)$ we have

$$d(\Gamma_0, u) + d(\Gamma_0, v) \geq (3/2)n! > n! - 1.$$

Also, the latter claim holds since for $u \in A_1(n)$ and $v \in A_2(n)$, we have

$$d(\Gamma_0, u) + d(\Gamma_0, v) \geq n! > n! - 1.$$

Now we show that in the graph $\Gamma_2 = \mathrm{cl}^{(2)}(\Gamma(S_n))$ every vertex in $A_1(n)$ is adjacent to every other vertex in the graph. Let $u \in A_1(n)$ and $v \in B_1(n) \cup B_2(n)$. Then by what we have shown above, in the graph Γ_1, u is adjacent to every other vertex in $A_1(n) \cup A_2(n)$. Also, by Theorem 4.3.3, $d(\Gamma_1, v) \geq n!/n^3$. Thus, by Lemma 4.3.2, we have

$$\begin{aligned} d(\Gamma_1, u) + d(\Gamma_1, v) &\geq (n! - 2 - |B_1(n) \cup B_2(n)|) + \frac{n!}{n^3} \\ &\geq \left(n! - 2 - \frac{n!}{(\lceil \sqrt{n} \rceil)!}\right) + \frac{n!}{n^3} \\ &\geq n! - 1. \end{aligned}$$

We next show that in the graph $\Gamma_3 = \mathrm{cl}^{(3)}(\Gamma(S_n))$ every vertex in $B_1(n)$ is adjacent to every other vertex in $B_1(n)$. Let $u, v \in B_1(n)$. By Theorem 4.3.3 and Lemma 4.3.2, we have

$$\begin{aligned} d(\Gamma_2, u) + d(\Gamma_2, v) \geq 2\left(|A_1(n)| + \frac{n!}{n^3}\right) &= 2\left(\frac{n!}{2} - |B_1(n)| + \frac{n!}{n^3}\right) \\ &\geq 2\left(\frac{n!}{2} - \frac{n!}{(\lceil \sqrt{n} \rceil)!} + \frac{n!}{n^3}\right) \\ &\geq n! - 1. \end{aligned}$$

It follows from what we have shown above and from Theorem 4.3.3 that every vertex in $B_1(n)$ is adjacent to at least $(n!/2) - 1 + (n!/n^3)$ other vertices in the graph Γ_3. The proof is complete. □

We are now ready to prove the main theorem of the thesis (Theorem 1.9.1) in the case of symmetric groups.

Theorem 4.3.6. *The graph* $\mathrm{cl}^{(3)}(\Gamma(S_n))$ *satisfies Chvátal's criterion for* $n \geq 107$.

Proof. Set $\Gamma = \mathrm{cl}^{(3)}(\Gamma(S_n))$. Let $d_1 \leq d_2 \leq \ldots \leq d_{n!-1}$ be the vertex degrees of the graph Γ. Let k be a positive integer with $k < (n!-1)/2$. It is sufficient to show that

$$d_{n!-1-k} \geq n! - 1 - k. \tag{4.1}$$

By Lemma 4.3.5, every vertex in $A_1(n)$ has largest possible degree, namely, $n! - 2$. Therefore, (4.1) holds for $k < |A_1(n)|$. Thus we may assume that $k \geq |A_1(n)|$. By Lemma 4.3.2, we have

$$k \geq |A_1(n)| = |S_n \setminus A_n| - |B_1(n)| \geq \frac{n!}{2} - \frac{n!}{2(\lceil\sqrt{n}\rceil)!}.$$

But then by Lemma 4.3.5, we have

$$d_{n!-1-k} \geq \frac{n!}{2} - 1 + \frac{n!}{n^3} \geq \frac{n!}{2} - 1 + \frac{n!}{2(\lceil\sqrt{n}\rceil)!} \geq n! - 1 - k.$$

The proof is complete. □

Proof of Theorem 1.9.1 in the case of symmetric groups. By Theorem 4.3.6 the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$ satisfies Chvátal's criterion. Thus by Theorem 4.2.6 the graph $\mathrm{cl}^{(3)}(\Gamma(S_n))$ is Hamiltonian. Then by three applications of Theorem 4.2.8 we have that $\Gamma(S_n)$ is Hamiltonian for $n \geq 107$. □

4.3.2 Alternating groups

In this subsection we show that the generating graphs of alternating groups of degree at least 107 satisfy Pósa's criterion and hence are Hamiltonian.

We need a result of Breuer, Guralnick, Lucchini, Maróti, Nagy on the minimal vertex degrees in $\Gamma(A_n)$.

Theorem 4.3.7 ([11, Theorem 5.3]). *Let* $n \geq 8$. *Then the degree of every vertex in* $\Gamma(A_n)$ *is at least* $n!/(10n^3)$.

Theorem 4.3.8. *The graph* $\Gamma(A_n)$ *satisfies Pósa's criterion for* $n \geq 107$.

Proof. Let $A(n)$ be the set of permutations in A_n with less than $\sqrt{n}$ fixed points and let $B(n) = A_n \setminus A(n)$. Then by Lemma 4.3.2,

$$|B(n)| \leq \frac{n!}{2(\lceil \sqrt{n} \rceil)!}.$$

Let $d_1 \leq d_2 \leq \ldots \leq d_{n!/2-1}$ be the vertex degrees in the graph $\Gamma(A_n)$. Let $k < (n!/2 - 1)/2$. We need to show $d_k \geq k + 1$. If there exists $i \leq k$ such that d_i is equal to the vertex degree of a permutation in $A(n)$, then by Theorem 3.9.2 we have

$$d_k \geq d_i \geq \left(1 - 2 \cdot \left(\frac{1}{\sqrt{n}} + \frac{16.2}{n} + \frac{1}{n^2}\right)\right) \cdot \frac{n!}{2} \geq \frac{n!}{4} \geq k + 1,$$

where the third inequality holds since $1/\sqrt{n} + 16.2/n + 1/n^2 \leq 1/4$. Thus we may assume that d_i is the vertex degree of a permutation in $B(n)$ for each $i \leq k$. But then $k \leq |B(n)|$ and hence by Theorem 4.3.7 we have

$$d_k \geq \frac{n!}{10n^3} \geq \frac{n!}{2(\lceil \sqrt{n} \rceil)!} + 1 \geq |B(n)| + 1 \geq k + 1,$$

where the second inequality holds since $n \geq 101$. This completes the proof. □

We are now ready to prove the main theorem of the thesis (Theorem 1.9.1) in the case of alternating groups.

Proof of Theorem 1.9.1 in the case of alternating groups. The graph $\Gamma(A_n)$ satisfies Pósa's criterion by Theorem 4.3.8 and hence $\Gamma(A_n)$ is Hamiltonian for $n \geq 107$ by Theorem 4.2.4. □

REFERENCES

[1] M. Aschbacher and R. Guralnick. Some applications of the first cohomology group. *J. Algebra*, 90(2):446–460, 1984.

[2] L. Babai. The probability of generating the symmetric group. *J. Combin. Theory Ser. A*, 52(1):148–153, 1989.

[3] L. Babai. Automorphism groups, isomorphism, reconstruction. In *Handbook of combinatorics, Vol. 1, 2*, pages 1447–1540. Elsevier Sci. B. V., Amsterdam, 1995.

[4] L. Babai and T. P. Hayes. The probability of generating the symmetric group when one of the generators is random. *Publ. Math. Debrecen*, 69(3):271–280, 2006.

[5] B. Bollobás. *Modern graph theory*, volume 184 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[6] J. A. Bondy and V. Chvátal. A method in graph theory. *Discrete Math.*, 15(2):111–135, 1976.

[7] J. Bovey and A. Williamson. The probability of generating the symmetric group. *Bull. London Math. Soc.*, 10(1):91–96, 1978.

[8] J. D. Bovey. The probability that some power of a permutation has small degree. *Bull. London Math. Soc.*, 12(1):47–51, 1980.

[9] T. Breuer. GAP computations concerning Hamiltonian cycles in the generating graphs of finite groups. *ArXiv e-prints*, Nov. 2009.

[10] T. Breuer, R. M. Guralnick, and W. M. Kantor. Probabilistic generation of finite simple groups. II. *J. Algebra*, 320(2):443–494, 2008.

[11] T. Breuer, R. M. Guralnick, A. Lucchini, A. Maróti, and G. P. Nagy. Hamiltonian cycles in the generating graphs of finite groups. *Bull. Lond. Math. Soc.*, 42(4):621–633, 2010.

[12] R. Brown. Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. *J. Combin. Theory Ser. A*, 49(2):294–307, 1988.

[13] R. Brown. Minimal covers of S_n by abelian subgroups and maximal subsets of pairwise noncommuting elements. II. *J. Combin. Theory Ser. A*, 56(2):285–289, 1991.

[14] T. C. Burness. Fixed point spaces in actions of classical algebraic groups. *J. Group Theory*, 7(3):311–346, 2004.

[15] T. C. Burness and E. Crestani. On the generating graph of direct powers of a simple group. *J. Algebraic Combin.*, 38(2):329–350, 2013.

[16] T. C. Burness and S. Guest. On the uniform spread of almost simple linear groups. *Nagoya Math. J.*, 209:35–109, 2013.

[17] P. J. Cameron, A. Lucchini, and C. M. Roney-Dougal. Generating sets of finite groups. *ArXiv e-prints*, Sept. 2016.

[18] V. Chvátal. On Hamilton's ideals. *J. Combinatorial Theory Ser. B*, 12:163–168, 1972.

[19] L. Comtet. Sur les coefficients de l'inverse de la série formelle $\sum n!t^n$. *C. R. Acad. Sci. Paris Sér. A-B*, 275:A569–A572, 1972.

[20] R. Cori. Indecomposable permutations, hypermaps and labeled Dyck paths. *J. Combin. Theory Ser. A*, 116(8):1326–1343, 2009.

[21] E. Crestani and A. Lucchini. The generating graph of finite soluble groups. *Israel J. Math.*, 198(1):63–74, 2013.

[22] E. Crestani and A. Lucchini. The non-isolated vertices in the generating graph of a direct powers of simple groups. *J. Algebraic Combin.*, 37(2):249–263, 2013.

[23] P. Diaconis, J. Fulman, and R. Guralnick. On fixed points of permutations. *Journal of Algebraic Combinatorics*, 28(1):189, 2008.

[24] G. A. Dirac. Some theorems on abstract graphs. *Proc. London Math. Soc. (3)*, 2:69–81, 1952.

[25] J. D. Dixon. The probability of generating the symmetric group. *Math. Z.*, 110:199–205, 1969.

[26] J. D. Dixon. Asymptotics of generating the symmetric and alternating groups. *Electron. J. Combin.*, 12:Research Paper 56, 5, 2005.

[27] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[28] S. Eberhard, K. Ford, and B. Green. Permutations fixing a k-set. *Int. Math. Res. Not. IMRN*, (21):6713–6731, 2016.

[29] S. Eberhard, K. Ford, and D. Koukoulopoulos. Permutations contained in transitive subgroups. *ArXiv e-prints*, May 2016.

[30] D. Frohardt and K. Magaard. Grassmannian fixed point ratios. *Geom. Dedicata*, 82(1-3):21–104, 2000.

[31] D. Frohardt and K. Magaard. Composition factors of monodromy groups. *Ann. of Math. (2)*, 154(2):327–345, 2001.

[32] D. Gluck and K. Magaard. Character and fixed point ratios in finite classical groups. *Proc. London Math. Soc. (3)*, 71(3):547–584, 1995.

[33] R. Guralnick and G. Malle. Products of conjugacy classes and fixed point spaces. *J. Amer. Math. Soc.*, 25(1):77–121, 2012.

[34] R. M. Guralnick. The spread of finite groups. *In preparation*.

[35] R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000. Special issue in honor of Helmut Wielandt.

[36] R. M. Guralnick and A. Maróti. Average dimension of fixed point spaces with applications. *Adv. Math.*, 226(1):298–308, 2011.

[37] W. M. Kantor and A. Lubotzky. The probability of generating a finite classical group. *Geom. Dedicata*, 36(1):67–87, 1990.

[38] M. W. Liebeck, C. E. Praeger, and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *J. Algebra*, 111(2):365–383, 1987.

[39] M. W. Liebeck and J. Saxl. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc. (3)*, 63(2):266–314, 1991.

[40] M. W. Liebeck and A. Shalev. The probability of generating a finite simple group. *Geom. Dedicata*, 56(1):103–113, 1995.

[41] M. W. Liebeck and A. Shalev. Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra*, 184(1):31–57, 1996.

[42] A. Lucchini. The diameter of the generating graph of a finite soluble group. *ArXiv e-prints*, Jan. 2017.

[43] A. Lucchini and A. Maróti. On finite simple groups and Kneser graphs. *J. Algebraic Combin.*, 30(4):549–566, 2009.

[44] A. Lucchini and A. Maróti. On the clique number of the generating graph of a finite group. *Proc. Amer. Math. Soc.*, 137(10):3207–3217, 2009.

[45] A. Lucchini and A. Maróti. Some results and questions related to the generating graph of a finite group. In *Ischia group theory 2008*, pages 183–208. World Sci. Publ., Hackensack, NJ, 2009.

[46] A. Lucchini, A. Maróti, and C. M. Roney-Dougal. On the generating graph of a simple group. *Journal of the Australian Mathematical Society*, page 1–13, 2016.

[47] T. Łuczak and L. Pyber. On random generation of the symmetric group. *Combin. Probab. Comput.*, 2(4):505–512, 1993.

[48] A. Maróti. On the orders of primitive groups. *J. Algebra*, 258(2):631–640, 2002.

[49] A. Maróti and M. C. Tamburini. Bounds for the probability of generating the symmetric and alternating groups. *Arch. Math. (Basel)*, 96(2):115–121, 2011.

[50] L. Morgan and C. M. Roney-Dougal. A note on the probability of generating alternating or symmetric groups. *Arch. Math. (Basel)*, 105(3):201–204, 2015.

[51] P. M. Neumann. *A study of some finite permutation groups*. PhD thesis, University of Oxford, 1966.

[52] O. Ore. Note on Hamilton circuits. *Amer. Math. Monthly*, 67:55, 1960.

[53] L. Pósa. A theorem concerning Hamilton lines. *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, 7:225–226, 1962.

[54] R. Steinberg. Generators for simple groups. *Canad. J. Math.*, 14:277–283, 1962.

[55] L. Stringer. *Pairwise generating sets for the symmetric and alternating groups*. PhD thesis, Royal Holloway, University of London, 2008.

[56] M. J. Tomkinson. Groups as the union of proper subgroups. *Math. Scand.*, 81(2):191–198, 1997.

[57] P. Turán. Eine Extremalaufgabe aus der Graphentheorie. *Mat. Fiz. Lapok*, 48:436–452, 1941.

[58] S.-C. Virchow. The Probability of Generating the Symmetric Group. *ArXiv e-prints*, Nov. 2016.

[59] R. A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer-Verlag London, Ltd., London, 2009.

CURRICULUM VITAE

PERSONAL INFORMATION

Name, Surname:	Fuat Erdem
Nationality:	Turkish
E-mail:	erdemfuat@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
B.S.	METU, Department of Mathematics	2010
High School	Atatürk Anatolian High School	2006

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2010–2018	METU, Department of Mathematics	Research Assistant

AWARDS AND SCHOLARSHIPS

- TÜBİTAK 2214/A International Research Fellowship for Doctorate Students
  2013–2014
- TÜBİTAK 2211/A Domestic Doctorate Fellowship
  2011–2016

PUBLICATIONS

- F. Erdem, On the generating graphs of symmetric groups, *J. Group Theory*, Ahead of print (published online: 2018), DOI: 10.1515/jgth-2018-0004.

ACADEMIC VISITS

- Alfréd Rényi Institute of Mathematics, Budapest, Hungary
  April 2017
- Technische Universität Kaiserslautern, Kaiserslautern, Germany
  September 2013–September 2014
- Alfréd Rényi Institute of Mathematics, Budapest, Hungary
  August 2012

CONFERENCE TALKS

- Hamiltonian cycles in the generating graphs of the alternating and symmetric groups
  Groups St Andrews 2017 in Birmingham
  August 5–13, 2017
  University of Birmingham, Birmingham, UK
- Hamiltonian cycles in the generating graphs of the alternating and symmetric groups
  Finite Groups and Their Automorphisms 2017
  May 3–6, 2017
  Abant İzzet Baysal University, Bolu, Turkey
- Hamiltonian cycles in the generating graph of the symmetric group
  2015 Zassenhaus Group Theory Conference
  May 22–24, 2015
  Binghamton University, Binghamton, USA

CONFERENCES ATTENDED

- Groups St Andrews 2017 in Birmingham
  August 5–13, 2017
  University of Birmingham, Birmingham, UK

- Finite Groups and Their Automorphisms 2017
  May 3–6, 2017
  Abant İzzet Baysal University, Bolu, Turkey

- The International Mini-Workshop on Finite Groups and Their Automorphisms
  August 7–12, 2015
  Doğuş University, Istanbul, Turkey

- 2015 Zassenhaus Group Theory Conference
  May 22–24, 2015
  Binghamton University, Binghamton, USA

- Young Algebraists' Conference 2014
  June 9–13, 2014
  Swiss Federal Institute of Technology in Lausanne, Lausanne, Switzerland

- The International Conference on Group Theory in Honor of the 70th Birthday of Professor Victor D. Mazurov
  July 16–20, 2013
  Sobolev Institute of Mathematics, Novosibirsk, Russia

- 2nd Biennial International Group Theory Conference
  February 4–8, 2013
  Doğuş University, Istanbul, Turkey

- International Conference on Group Theory and Lie Theory
  March 19–21, 2012
  Harish-Chandra Research Institute, Allahabad, India

- The International Workshop on Finite Groups and Their Automorphisms
  June 7–11, 2011
  Boğaziçi University, Istanbul, Turkey

COURSES ASSISTED AT METU

- Math 111 - Fundamentals of Mathematics

- Math 112 - Discrete Mathematics
- Math 115 - Analytic Geometry
- Math 116 - Basic Algebraic Structures
- Math 117 - Calculus I
- Math 118 - Calculus II
- Math 119 - Calculus With Analytic Geometry
- Math 120 - Calculus of Functions of Several Variables
- Math 261 - Linear Algebra I
- Math 262 - Linear Algebra II
- Math 367 - Abstract Algebra