People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University Of Kasdi Merbah - Ouargla

Department of Mathematics

In partial fulfillment of the requirements for the degree of master 2 of mathematical

Option: Algèbre

presented by:
Ouargli Moussa

Supervisor:
M.Guerboussa Yassine

Theme

Generation of the symmetric groups

Represented 26/06/2022 Limb from jury:

Mr.M.A.Behayou	MCB, Kasdi Merbah - Ouargla	President
Mr.M.Guedri	MCA, Constantine 1 - Constantine	Examiner
Mr.Y. Guerboussa	MCA, Kasdi Merbah - Ouargla	Supervisor

Dedicate

This work is dedicated to: My Mother
my Father
All my brothers
All frieds
All my family
My colleagues at the department of mathematics, University Kasdi Merbah Ouargla.

Remerciement

Firstly thanks go to Allah who enabled me to complete this work.I would like to express my deep gratitude to my advisor Dr. Y. Guerboussa, for his constructive criticisms, help and guidance. Also, I thank the jury members Dr. A. Bahayou and Dr. M. Guedri for their questions and comments that helped in improving the text.

Abstract

This thesis is devoted to proving Dixon's theorem:Almost all pairs of permutations in the symmetric group of degree n generates either the symmetric group or its alternating subgroup.

Résumé

Le but de cette thése est d'exposer le théoréme de Dixon: Un couple aléatoire de permutations dans le groupe symétrique de dégré n engendre soit le groupe symétrique ou bien le groupe alterné de degré n, avec un probabilité qui tend vers 1 lorsque n crois.

Contents

Introduction

The aim of this thesis is to give an (almost) self contained proof of Dixon's theorem: *Almost every pair of permutations in the alternating group A_n generate A_n.*

To make the last statement precise, let us define for an arbitrary finite group G the ingredient:

$$P_2(G) = \frac{|\{(x,y) \in G^2 \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Of course the latter represents the probability (the uniform one) that a randomly chosen pair of elements of G generates it. Observe that $P_2(G) > 0$ if and only if G can be generated by two elements. The latter fact is well-known for $G = A_n$ since the beginning of the theory of substitutions. Dixon's theorem can be restated now as: $P_2(A_n) \to 1$ as $n \to \infty$. We shall prove in fact that $P_2(A_n) \geq 1 - 2/(\log\log n)^2$.

A noteworthy is that the A_n, for $n \geq 5$, form an infinite family of finite simple groups. It was natural then that Dixon conjectures the following:

Conjecture. [J. Dixon, 1969] *For every simple group G,*

$$P_2(G) \to 1, \quad \text{as } |G| \to \infty.$$

At that time, this was a bold conjecture since we didn't know even all the finite simple groups. The situation changed after the announcement by D. Gorenstein that the classification of finite simple groups (CFSG) is complete ($\sim$ 1980). Roughly speaking, the latter asserts that every (non-abelian) simple group belongs to one of the following families:

- The alternating groups A_n for $n \geq 5$.
- The groups of Lie type. These are divided into two classes: the classical ($\mathrm{PSL}_n(q)$, $\mathrm{PSp}_{2n}(q)$, etc), and exceptional (e.g. $G_2(q)$, $F_4(q)$, and their twisted forms).
- 26 sporadic groups (the largest among them is called the Monster).

Dixon's conjecture was confirmed later (1990) by Kantor and Lubotzky for the classical groups, and by Liebeck and Shalev for the remaining cases (the exceptional groups) in 1995. About the proof, note that in any finite group G, a pair (x,y) does not generate G if, and only if, there exists a maximal subgroup M of G which contains x and y. It follows that

$$1 - P_2(G) \leq \sum_{M} \frac{|M|^2}{|G|^2},$$

where M runs over the maximal subgroups of G. Now, if one defines

$$\zeta_G(s) = \sum_M |G : M|^{-s} \quad (\text{ for } s \in \mathbb{R})$$

then it is enough to show that $\zeta_G(2) \to 0$ as $|G| \to \infty$ (G simple) to settle Dixon's conjecture. The CFSG gives enormous information about the maximal subgroups of G, and so about the behavior of $\zeta_G(2)$, which allows us to complete the proof (although, checking these needs clever ideas to deal with each family).

For the proof of Dixon's theorem, one just needs elementary results (avoiding the CFSG), although they are complicated and difficult to follow in general. A key ingredient here is the classic result of C. Jordan on primitive permutation groups, namely, if a primitive (permutation) group contain a p-cycle, for some prime $p \leq n-3$, then this group is A_n or S_n. The basic results on permutation groups, and a proof of Jordan's theorem will be given in the first chapter. The second chapter is of combinatorial nature. Statistical results on permutations, mainly due to Erdos and Turan, are needed to complete the proof.

Chapter 1

Permutation groups

Throughout, Ω denotes a finite set, the cardinality of which will be denoted by n.

1.1 The symmetric group

Definition 1.1.1. *A permutation of Ω is a bijective map from Ω to itself. The set S_Ω of these permutations form a group under the usual composition of maps which we call the symmetric group on Ω. A* permutation group *on Ω means a subgroup of S_Ω.*

The symmetric group on $\Omega = \{1, \ldots, n\}$ will be denoted by S_n.

For $u \in S_\Omega$, and $\alpha \in \Omega$, we write α^u for the image of α under u. Sometimes, it is convenient to use the notation

$$u = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^u & \alpha_2^u & \ldots & \alpha_n^u \end{pmatrix}.$$

For instance, $u = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ denotes the permutation in S_4 such that $1^u = 2$, $2^u = 4$, $3^u = 1$, and $4^u = 3$. If one considers moreover $v = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$, then

$$uv = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Note here that we are using the opposite law of the usual composition '$\circ$', which is more convenient to the exponential notation α^u.

The notation $(\alpha_1\, \alpha_2 \ldots \alpha_r)$ refers to the permutation that sends α_i to α_{i+1} for $i < t$, sends α_r to α_1, and fixes the remaining elements of Ω. A permutation of this form is called a *cycle* of length r, or an r*-cycle*. A 2-cycle is also called a *transposition*.

Recall that the order of a permutation $u \in S_\Omega$ is the smallest positive integer d such that $u^d = 1$, that is to say $\alpha^{u^d} = \alpha$ for all $\alpha \in \Omega$. It is readily seen that the order of r-cycle is equal to r.

For $u \in S_\Omega$, we write $\mathrm{fix}(\sigma)$ for the set of elements of Ω fixed by u, that is

$$\mathrm{fix}(u) = \{\alpha \in \Omega \mid \alpha^u = \alpha\}.$$

We write $\mathrm{supp}(u)$ for $\Omega \setminus \mathrm{fix}(u)$, and call it the support of u. Two permutations u and v in S_Ω are said to be *disjoint* if their supports are, that is to say $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\sigma') = \emptyset$.

The following result is straightforward.

Lemma 1.1.1. *Let $u, u' \in S_\Omega$ with supports S and S' respectively. If u and u' are disjoint, then*

(i) $\alpha^{uu'} = \alpha^{u'u} = \alpha^u$, *for* $\alpha \in S$;

(ii) $\alpha^{uu'} = \alpha^{u'u} = \alpha^{u'}$, *for* $\alpha \in S'$;

(iii) $\alpha^{uu'} = \alpha^{u'u} = \alpha \ \alpha \notin S \cup S'$.

In particular, u and u' commute.

More generally, if $(u_i)_{i \in I}$ is a finite family of disjoint permutations in S_Ω, then one can form the permutation $u = \prod_{i \in I} u_i$ (u is well defined since the σ_i 's commute, that is the order in which the u's are taken is unimportant). If we denote by S_i the support of σ_i, the preceding lemma shows at once that $\alpha^u = \alpha^{u_i}$ for $\alpha \in S_i$, and $\alpha^u = \alpha$ for $\alpha \notin \bigcup_{i \in I} S_i$.

Let us define on Ω the relation:

$$\alpha \sim \beta \qquad \Longleftrightarrow \qquad \text{there exists } m \in \mathbb{N} \text{ such that } \alpha^{u^m} = \beta.$$

The latter is readily seen to be an equivalence relation on Ω. Clearly, the orbit of $\alpha \in \Omega$ under this relation is

$$\mathcal{O}_\alpha = \{\alpha, \alpha^u, \alpha^{u^2}, \ldots\}.$$

Plainly, the set of all such orbits $\mathcal{O}_{\alpha_1}, \ldots \mathcal{O}_{\alpha_s}$ form a partition of Ω. Moreover, if for every $i = 1, \ldots, s$, we denote by u_i the permutation defined by:

$$\alpha^{u_i} = \alpha^u \text{ for } \alpha \in \mathcal{O}_{\alpha_i}, \qquad \text{and } \alpha^{u_i} = \alpha \text{ otherwise,}$$

then it follows from the preceding paragraph that $u = \prod_{i \in I} u_i$; and obviously each u_i is a cycle of length $|\mathcal{O}_{\alpha_i}|$. This proves the following:

Theorem 1.1.1. *Every permutation can be uniquely written as a product of disjoint cycles.*

Using the fact that disjoint cycles commute, it follows that:

Corollary 1.1.1. *If $r_1, \ldots, r_s$ are the sizes of the orbits of a permutation $u \in \Omega$, then the order of u is the least common multiple of the r_i's.*

Next, note that every cycle $c = (\alpha_1\, \alpha_2 \ldots \alpha_r)$ can be expressed as:

$$c = (\alpha_1\, \alpha_2)(\alpha_2\, \alpha_3) \cdot (\alpha_{s-1}\, \alpha_s).$$

Combining that with the above theorem yields the following.

Corollary 1.1.2. *Every permutation can be written as a product of tranpositions (not necessarily disjoint).*

1.2 Even permutations

Definition 1.2.1. *Fix an order* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *on* Ω*. Let* $u \in S_\Omega$*, and for each index* i*, let* k_i *be the integer such that* $\alpha_i^u = \alpha_{k_i}$*. The signature* $\varepsilon(u)$ *of* u *is defined by:*

$$\varepsilon(u) = \prod_{i<j} \frac{k_j - k_i}{j - i}.$$

Plainly, $\varepsilon(u) = \pm 1$. It is readily seen that $\varepsilon : S_\Omega \to \{1, -1\}$ is a group homomorphism.

Definition 1.2.2. *The alternating group* A_Ω *is the kernel of the signature map* $\varepsilon : S_\Omega \to \{1, -1\}$.

Obviously, the signature of a transposition is equal to -1; therefore, if we write $u \in A_\Omega$ as a product of transpositions $u = t_1 \cdots t_s$, then $\varepsilon(u) = (-1)^s = 1$. Thus, for any expression of u as a product of transpositions, the number of the latter is even. For this reason, the elements of A_Ω are called the even permutations.

Note also that the signature of an r-cycle is equal to $(-1)^{r-1}$. In particular, all the 3-cycles are even.

Theorem 1.2.1. *The alternating group* A_Ω *is generated by* 3*-transpositions.*

To see that we need only to prove that the product of two transpositions lies in the group generated by 3-cycles. In fact, we have:

$$(\alpha\,\beta)(\beta\,\gamma) = (\alpha\,\beta\,\gamma) \quad (\text{for } \alpha \neq \gamma);$$

and for disjoint transpositions $(\alpha\,\beta)$ and $(\gamma\,\delta)$, we have:

$$(\alpha\,\beta)(\gamma\,\delta) = \text{ a product of two 3-cycles,}$$

which completes the proof.

1.3 Transitivity

Let G be a permutation group on Ω. We say that G is *transitive* if for all $\alpha, \beta \in \Omega$, there exists $g \in G$ such that $\alpha^g = \beta$.

Recall that the stabilizer G_α of an element $\alpha \in \Omega$ in G is defined by:

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\}.$$

Note that there is a natural bijective map from the orbit $\mathcal{O}_\alpha$ of α onto the set G/G_α of right cosets of G_α given by:

$$\bar{g} \mapsto \alpha^g.$$

It follows in particular that $|\mathcal{O}_\alpha| = |G : G_\alpha|$.

If G is transitive, then $\mathcal{O}_\alpha = \Omega$. The map $G/G_\alpha \to \Omega$ defined above gives in fact an isomorphism of G-sets, where G acts on G/G_α in the obvious way: $\bar{x}^g = \overline{xg}$, for all $\bar{x} \in G/G_\alpha$ and $g \in G$.

More generally, we can speak about highly transitive groups

Definition 1.3.1. *Let G be a permutation group on Ω, and k a non-negative integer. We say that G is k-transitive if for all $\alpha_1, \ldots, \alpha_k$ and $\beta_1, \ldots, \beta_k$ in Ω, with $\alpha_i \neq \alpha_j$ and $\beta_i \neq \beta_j$ for $i \neq j$, there exists $g \in G$ such that $\alpha_i^g = \beta_i$ for all $i = 1, \ldots, k$.*

For instance, $G = S_\Omega$ is n-transitive, and $G = A_\Omega$ is $(n-2)$-transitive. Note that G is transitive if and only if it is 1-transitive.

Note that one has a natural action of G on the set

$$\Omega^{(k)} = \left\{(\alpha_1, ..., \alpha_k) \in \Omega^k \mid \alpha_i \neq \alpha_j \text{ for } i \neq j\right\},$$

with $(\alpha_1, ..., \alpha_k)^g = (\alpha_1^g, ..., \alpha_k^g)$, for $g \in G$ and $(\alpha_1, ..., \alpha_k) \in \Omega^{(k)}$.

Plainly, saying that G is k-transitive on Ω amounts to saying that the action of G on $\Omega^{(k)}$ is transitive.

As

$$|\Omega^{(k)}| = n(n-1)......(n-k+1) = \frac{n!}{(n-k)!},$$

it follows that if G is k-transitive, the order of G is divisible by $\frac{n!}{(n-k)!}$. Indeed, we have $|G : G_\alpha| = |\Omega^{(k)}|$, for $\alpha = (\alpha_0, ..., \alpha_k) \in \Omega^{(k)}$.

The following result is immediate from the definition.

Lemma 1.3.1. *Let G be a transitive group on Ω, and $\alpha \in \Omega$. For G to be k-transitive ($k \geq 2$), it is necessary and sufficient that the stabilizer G_α be $(k-1)$-transitive on $G \setminus \{\alpha\}$.*

1.4 Primitive permutation groups

For a subset $\Psi \subseteq \Omega$, we write Ψ^g for the set of the element of the form α^g, where α runs over Ψ.

Definition 1.4.1. *A subset $\Psi \subseteq \Omega$ is called a* block *of G if for every $g \in G$, we have either Ψ^g=Ψ or $\Psi^g \cap \Psi = \phi$.*

For instance, $\Psi = \Omega$ and $\Psi = \{\alpha\}$ are blocks of G (for every $\alpha \in \Omega$). The previous subsets are called the trivial blocks of G.

Definition 1.4.2. *We say that G is primitive, if it is transitive and all its blocks are trivial.*

Note that if Ψ is a block of G, then the set $\{\Psi, \Omega - \Psi\}$ is a partition of Ω. Conversely, if we have a partition $\{P_1, \ldots, P_s\}$ preserved by G, that is, $P_i^g = P_i$ for every index i and every $g \in G$, then every P_i is a block of G. It follows then that G (supposed transitive) is primitive if G preserves only the trivial partitions $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$.

The following is a criterion to recognize the primitivity of G internally.

Proposition 1.4.1. *Let $\alpha \in \Omega$, and assume that G is transitive on Ω. For G to be primitive, it is necessary and sufficient that the stabilizer G_α be a maximal subgroup of G.*

Proof. Suppose G is primitive. If G_α is not maximal in G, then there exists $H \leq G$ such that $G_\alpha < H < G$. Set

$$\Psi = \{\alpha^h \mid h \in H\}.$$

Let $g \in G$ so that $\Psi \cap \Psi^g \neq \phi$; then there exist $h, h^{'} \in H$ such that $\alpha^h = \alpha^{h'g}$. It follows that $h^{'}gh^{-1} \in G_\alpha \leq H$, so $g \in H$, in particular $\Psi^g = \Psi$, which proves that Ψ is a block of G.

Now, as $G_\alpha < H$, every element $H \setminus G_\alpha$ satisfies $\alpha^h \neq \alpha$, so $\Psi \neq \{\alpha\}$ (as $\alpha^h \in \Psi$). Also, for $g \in G \setminus H$, we have $\Psi^g \neq \Psi$ (otherwise g would lie in H as we have shown above); therefore $\Psi \neq \Omega$. This shows that Ψ is a non-trivial block of G, a contradiction (G is primitive).

Conversely, assume G_α is maximal in G. If G has a non-trivial block Ψ, define

$$H = \{g \in G \mid \Psi^g = \Psi\},$$

so, $H < G$, and H is proper in G since $\Psi \neq \Omega$ (here we are using the fact that G is transitive on Ω). Pick an element $\alpha \in \Psi$. Obviously, $G_\alpha \leq H$, and if $G_\alpha = H$ then $\Psi = \{\alpha\}$ which contradicts the fact that Ψ is not trivial. It follows that $G_\alpha < H$, contradicting the assumption G_α is maximal in G. The result follows. □

The following result will be useful later. Below, for $\Pi \subseteq \Omega$, G_Π denotes the intersection $\bigcap_{\alpha\in\Pi} G_\alpha$.

Lemma 1.4.1. *Assume G is k-transitive on Ω, and let $\Pi \subseteq \Omega$ with $|\Pi| = k$. Suppose $U \leq G_\Pi$ is conjugate in G_Π to every $V \leq G_\Pi$ which is conjugate to U in G (that is if $U = V^g$ for some $g \in G$, then $U = V^h$ for some $h \in G_\Pi$). Then $N_G(U)$ is k-transitive on the set*

$$\Omega' = \{\alpha \in \Omega \mid \alpha^u = \alpha \text{ for all } u \in U\}.$$

Proof. Set $N = N_G(U)$. For $g \in N$, $\alpha \in \Omega$ and $u \in U$, we have $(\alpha^g)^u = \alpha^{(gu)} = \alpha^{gug^{-1}g} = \alpha^g$ (hence Notics on $\Omega^{'}$, Now let $\alpha_1, ..., \alpha_k \in \Omega^{'}$ with $\alpha_i \neq \alpha_j$ for $i \neq j$.

□

Assume G is a permutation group on Ω and $\Delta \subseteq \Omega$, with $|\Delta| > 1$. We say that Δ is a *Jordan set* if there exists a subgroup of G which fixes $\Omega \diagup \Delta$ element-wise and acts transitively on Δ.

For instance, if G is k-transitive, then every Δ which $\dfrac{|G|}{|\Delta|} < k$ is a Jordan set.

Theorem 1.4.1. *If G is primitive and has a Jordan set, then G is 2-transitive.*

Proof. First, observe that for every $\Delta \subsetneq \Omega$ such that $1 < |\Delta| < |\Omega|$, and for all $\alpha, \beta \in \Omega$ with $\alpha \neq \beta$, there exists $g \in G$ such that $\alpha \in \Delta^g$ and $\beta \notin \Delta^g$. Indeed, the relation:

$$\alpha \sim \beta \iff \alpha, \beta \in \Delta^g \text{ for all } g \in G,$$

is an equivalence relation for hich every class form a block of G. As G is primitive, it follows that each class contains exactly one element, and our claim follows.

Now, set $|\Omega| = n$, and choose a maximal Jordan set $\Delta \subsetneq G$, and write $k = |\Delta|$. By the preceding observation we have $\Omega \setminus \{\alpha\} = \cup\Delta^g, more\ over\ as$ Δ ho turce of these sets. Cover Ω, so they form a partition of $\Omega/\{\alpha\}$. Thus k divides $n - 1(n - 1 = |\Omega/\{\alpha\}|)$.

As G is transitive,every α is outside exactly $n/k - 1$ translates of Δ ($n/_{k-1}$ is the number of orbits in $\Omega/\{\alpha\}$). It fellows that the number of the translates Δ^g of Δ is equal to $\frac{n(n-1)}{k(n-k)}$.

Now, since k divides $n - 1$, k as well as $n - k$ are coprime to n.
So $k(n - k)divides$ $n - 1$ (Euclide-Gauss). then $k = 1$ or $k = n - 1$ The case $k = 1$ contradicts the definition of Jordan set. Hence, $k = n - 1$. So G is 2- transitive. ☐

The following result is crucial in proving Dixon's theorem.

Theorem 1.4.2 (Jordan)**.** *If a primitive subgroup $G \leq S_\Omega$ contains a p-cycle, with p prime and $p \leq n - 3$, then G contains A_Ω (in other words, G is either A_Ω or S_Ω).*

Chapter 2

Generation of the symmetric and the alternating groups

2.1 The main result

Netto conjectured and Dixon (1969) proved that *Almost every pair of permutations in the symmetric group S_n generate either S_n or the alternating group A_n.*

To make the last statement precise, let us define for an arbitrary finite group G the ingredient:

$$P_2(G) = \frac{|\{(x,y) \in G^2 \mid \langle x,y \rangle = G\}|}{|G|^2}.$$

Of course, the latter represents the probability (the uniform one) that a randomly chosen pair of elements of G generates G.

Observe that $P_2(G) > 0$ if, and only if, G can be generated by two elements. The latter fact is well-known for $G = A_n$ since the beginning of the theory of substitutions. Dixon's theorem can be restated now as:

Theorem 2.1.1. *We have $P_2(A_n) \to 1$ and $P_2(S_n) \to \frac{3}{4}$, as $n \to \infty$.*

The group generated by a pair (x,y) is in A_n if and only if both x and y are even permutations. Since half of the permutation in S_n are odd (as A_n has index 2 in S_n), the above theorem follows from the more refined result:

Theorem 2.1.2. *The proportion of ordered pairs (x,y), with $x, y \in S_n$, which generate either A_n or S_n is greater than $1 - 2/(\log\log n)^2$ for all sufficiently large n.*

2.2 Some remarks

Let G be a finite group, and n a positive integer. Define

$$P_n(G) = \frac{|\{(x_1,\ldots,x_n) \in G^n \mid \langle x_1,\ldots,x_n \rangle = G\}|}{|G|^n}.$$

Lemma 2.2.1. *For any finite group G, we have:*

$$P_n(G) \le \sum_M |G:M|^{-n},$$

where M runs over the set of maximal subgroups of G.

Proof. First observe that some elements $g_1 g_2, ..., g_n \in G$ don't generate G if, and only if, one has

$$\langle g_1, g_2, ..., g_n \rangle < G,$$

or equivalently, if (and only if) there exists a maximal subgroup M of G such that that

$$\langle g_1, g_2, ..., g_n \rangle \leq M,$$

that is $(g_1, g_2, ..., g_n) \in M^n$.

It follows that $\{(g_1, g_2, ..., g_n) \in G^n \mid < g_1, g_2, ..., g_n > \neq G\}$ is contained in $\cup_M M^n$. Hence

$$1 - P_2(G) \leq \frac{|\cup_M M^n|}{|G^n|} \leq \sum_M \frac{|M^n|}{|G^n|} = \sum_M |G : M|^{-n},$$

as claimed. □

It is useful to define the function

$$\zeta_G(s) = \sum_M |G : M|^{-s},$$

with M runs over the maximal subgroups of G. The latter is known as the *Witten Zeta function* (in honor of the physician Edouard Witten who introduced similar functions when dealing with Lie groups)

To prove Dixon's theorem, we have to show that $\zeta_{A_n}(2) \to 0 \ \ as \ \ |G| \to \infty$.

Let $X_n = \{(x, y) \in S_n^2 \mid A_n \leq \langle x, y \rangle\}$; in other words, $X_n = \{(x, y) \in S_n^2/$<x,y>$= A_n \ \ ou \ \ $<x,y>$= S_n\}$

that is $X_n = X_n^{'} \bigcup X_n^{''}$

where $X_n^{'} = \{(x, y) \in S_n^2/$<x,y>$= A_n\}$

and $X_n^{''} = \{(x, y) \in S_n^2/$<x,y>$= S_n\}$

2.3 Generating transitive and primitive groups

Let t_n be the proportion of the $(n!)^2$ pairs (x, y), $x, y \in S_n$ which generate a transitive subgroup of S_n, and let p_n be the corresponding proportion which generate a primitive subgoup of S_n. Obviously, t_n and p_n represent the probability that a random pair of elements in S_n will generate a transitive subgroup and a primitive subgroup, respectively.

Theorem 2.3.1. *We have*

$$t_n = 1 - \frac{1}{n} + O(n^{-2})$$

as $n \to \infty$.

The same asymptotic estimate holds for the proportion of pairs which generate a primitive subgroup roughly $n - 1$ times out of n.

Proof. Put $\Omega = \{1, 2, ..., n\}$ for each partition $\Omega = \Omega_1 \cup \Omega_2 ... \cup \Omega_k \ \ of \ \ \Omega$ into nutually disjoint subsets ,the number of pairs $(x, y)(x, y \in S_n)$ such that the group $< x, y >$ generated has precisely $\Omega_1, \Omega_2 ... \Omega_k$ as its orbits is equal to $\pi_{i=1}^{k} (n_i!)^2 t_{n_i}$; where $n_i = |\Omega_i| (i = 1, 2, ...k)$
Indeed we can choose the paire of restrictions $(x/\Omega_i, y/\Omega_i)$ independently for different i and subject only to the cendition that $(x/\Omega_i, y/\Omega_i)$ should generate a transitive group Ω_i.
Now it is well known that the number of ways of partitioning Ω such that there are k_i classes of order $i(so \sum_{i=1} nik_i = n)$ equals $V_{k_1,k_2,...,k_n}$=$n!/\{\pi_{i=1}^{n} (i!)^2 t_i\}^{k^i} = n! \sum \pi_{i=1}^{n} (i!t_i)_i^k / k_i!$
where both sums are over all n-tuples$(k_1, k_2, ..., k_n)$ for which each k_i is in an integer $\geq$ 0and $\sum ik_i = n$
we get a formal power series identity:
$\sum_{n=0}^{\infty} n!X^n = \pi_{i=0}^{\infty} exp(i!t_i X^i) = exp(\sum_{n=0}^{\infty} i!t_i X^i)$
Formal differentiation then gives $\sum_{n=0}^{\infty} n!nX^{n-1} = \sum_{n=1}^{\infty} i!it_i X^{i-1} \sum_{n=0}^{\infty} n!X^n$
Hence by equating coefficients of X^{n-1} we get $n = \frac{1}{n!} \sum_{n=1}^{\infty} i!(n-1)!it_i = \sum_{n=1}^{n} \binom{n}{i} it_i$
$(i = 1, 2, ...)$
Where$\binom{n}{i} = \frac{n!}{i!(n-i)!}$,we can use (1) to calculate the values of t_n recursively.The first few values are:$t_1 = 1, t_2 = \frac{3}{4}, t_3 = \frac{13}{18} = 0.722..., t_4 = \frac{71}{96} = 0.738...$
We shall now use Eq(1) to prove the following lemma which gives the first half of the main theorem ☐

Lemma 2.3.1. $t_n = 1 - \frac{1}{n} + O(n^{-2}) as \ \ n \to \infty$

Proof. Put $r_n = n(1 - tn), and \ \ not \ \ that \ \ r_n \geq 0$
because $t_n \leq 1$.We have to show that $r_n - 1 = 0(\frac{1}{n})$;from (1) we have $r_n = c_n - \sum_{i=1}^{n-1} \binom{n}{i} r_i$ ...(2)
Where $C_n = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} i. Because \binom{n}{i}^{-1} = \binom{n}{n-i}^{-i}$
for all i

☐

$$\text{where } C_n = \sum_{i=1}^{n-1} \tbinom{n}{i}^{-1} . Because \tbinom{n}{i}^{-1} = \tbinom{n}{n-i}^{-1}$$

for all is
$C_n = \frac{1}{2} n \sum_{i=1}^{n-1} \tbinom{n}{i}^{-1} = 1 + \dfrac{2}{n-1} + \dfrac{1}{2} n \sum_{i=3}^{n-3} \tbinom{n}{i}^{-1} \ , \ forall \ n \geq 6.$
By the well known monotonicity property of the binomial cafficients,
$\binom{n}{3} \leq \binom{n}{i} \ for \ 3 \leq i \leq n - 3$
There fore the last sum in this expression for C_n is at most
$\frac{1}{2} n \binom{n}{3}^{-1} (n - 4) = 0(\frac{1}{4})$
Thus we conclude that
$C_n = 1 + 0(\frac{1}{n}) as \ n \longrightarrow \infty$
Finally, since $r_i \geq 0$ for all i, (2) shows that $r_n \leq C_n$.Therefore applying (2) again we get
$r_n = C_n - \sum_{i=1}^{n-1} \tbinom{i}{n}^{-1} 0(1) = C_n + \dfrac{2C_n}{n} 0(1) = 1 + 0(\dfrac{1}{n}).$
as required.

Lemma 2.3.2. *Let* $T_n = \bigcup_q C_{qn}$, *where the union is over all primes* q *with* $(\log \ n)^2 \leq q \leq n-3$. *Then the proportion* U_n *of elements of* S_n *which lie in* T_n *is at least*
$1 - \frac{4}{(3 \log \log n)}$ *for all sufficiently large* n.

Proof. we need two results from the paper [1]of Erdos and Turan. Theorem VI of that paper shows that for any integers a_i ; $with$ $1 \leq a_1 \leq a_2 \leq ... \leq a_k \leq n$, the proportion of permutation in S_n whose cycle de compositions contain no cycles of lengths $a_1, a_2, ..or\ a_k$ is at most
$\sum_{i=1}^{k}(\dfrac{1}{a_i})^{-1}$
Lemma 2.1.5 of that paper shows that the proportion of elements in S_{n-q} with order relatively prime to q (for a given prime q) is $\Pi_i \frac{qi-1}{qi}$ where the product is over all i, $1 \leq i \leq \frac{n-q}{q}$.
Now elementary estimtes show that

$\Pi \frac{qi-1}{qi} = \exp(\frac{\log n - \log q + 0(1)}{q})$

Therefore in our case the product is greater then $\exp(\frac{\log n}{q}) \geq \exp(-\frac{1}{\log n})$ for all Sufficiently large n.
A permutation is of order relatively prime to g if and only if all cycles in its cycle de composition have lengths relatively prime to q Thus form the two results just- quoted and the definition of C_{n_q} we conclude that
$U_n \geq (1 - (\sum_q \frac{1}{q})^{-1}) \exp(-\frac{1}{\log n})$
for all sufficiently large n.
Here q rums over all primes,$(\log n)^2 \leq q \leq n-3$
on
$\sum_q \frac{1}{q} = \log\log n + 0(1) as\ n \longrightarrow \infty$
where p runs over all primes, $1 \leq p \leq n$. Thus $\sum_q \frac{1}{q} = \log\log(n-3) - \log\log(\log n)^2 + 0(1) > \frac{4}{5}\log\log\ n$.

□

Bibliography

[1] L.Babai. *The probability of generating the symmetric group*.J.Combin.Theorp ser.A52(1989),148 -153

[2] J.D.Dixon. *The probability of generating the symmetric group,Math-Z-110(1969).*

[3] Wielandt,H. *Finite permutation groups*.New York ,Acodemic Press 1964.