BOUNDS FOR THE PROBABILITY OF GENERATING THE SYMMETRIC AND ALTERNATING GROUPS

ATTILA MARÓTI AND M. CHIARA TAMBURINI

ABSTRACT. We give explicit, asymptotically sharp bounds for the probability that a pair of random permutations of degree n generates either S_n or A_n and also for the probability that a pair of random even permutations of degree n generates A_n. As an application we answer a question of Wiegold in the case of alternating groups.

1. INTRODUCTION

In [5] 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 [2] 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 [3]. Then, proving a conjecture of Dixon, Babai [1] showed that $p(S_n) = 1 - (1/n) + O(1/n^2)$. Finally, Dixon [6] 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 see [4]. 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.

One of the purposes of this short paper is to give explicit, asymptotically sharp lower and upper bounds for $p(A_n)$ and $p(S_n)$.

Theorem 1.1. *Let n be an integer at least 4 and let X be S_n or A_n. Then*

$$1 - \frac{1}{n} - \frac{13}{n^2} < p(X) \leq 1 - \frac{1}{n} + \frac{2}{3n^2}.$$

Theorem 1.1 depends on the Classification of Finite Simple Groups.

Date: September 20, 2010.

2000 *Mathematics Subject Classification.* Primary 20B30; Secondary 20P05.

Key words and phrases. symmetric group, alternating group, probability, generation.

The research of the first author was supported by a Marie Curie International Reintegration Grant within the 7th European Community Framework Programme, by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences, and by OTKA NK72523.

For a non-abelian finite simple group G let $h(G)$ be the largest non-negative integer k such that the k-th direct power of G can be generated by 2 elements. Erfanian and Wiegold [11] showed that $h(G)$ tends to infinity as $|G|$ tends to infinity whenever G is a non-abelian finite simple group of spread one. A year later Liebeck and Shalev [16] proved that there exists universal constants a and b such that $1-(a/m(G)) < p(G) < 1-(b/m(G))$ holds for any non-abelian finite simple group G where $p(G)$ denotes the probability of a random pair of elements of G (with respect to the uniform distribution) that generates G and $m(G)$ denotes the minimal index of a proper subgroup of G. This together with the observation of Hall [13] that $h(G) = (p(G)|G|^2)/|\mathrm{Aut}(G)|$ provides an asymptotic formula for $h(G)$. In fact we see that $h(G)$ tends to infinity as $|G|$ tends to infinity.

Problem 17.116 of [14] of Wiegold asks for an explicit lower bound for $h(G)$, namely $\sqrt{|G|}$. This lower bound has been established by Erfanian [9] for projective special linear groups and by Erfanian and Rezaee [10] for symplectic groups. A paper on an asymptotic result concerning the alternating groups has also been published [8] (but a stronger result follows from the previous paragraph). Here we prove the conjecture of Wiegold in the case of alternating groups. In fact, Theorem 1.1 gives more.

Corollary 1.2. *Let n be an integer at least 7. Then*
$$\Big(1-\frac{1}{n}-\frac{13}{n^2}\Big)\Big(\frac{n!}{4}\Big) < h(A_n) \leq \Big(1-\frac{1}{n}+\frac{2}{3n^2}\Big)\Big(\frac{n!}{4}\Big).$$

2. Transitive groups

In [5, Lemma 1] it was proved that the probability $p_1(S_n)$ that a random pair of permutations of degree n generates a transitive group is $1-(1/n)+O(1/n^2)$. Here we follow an alternative proof of this fact [1, Section 3] from which explicit upper and lower bounds can be derived. Let us denote the probability that a random pair of even permutations of degree n generates a transitive group by $p_1(A_n)$.

Lemma 2.1. *Let n be an integer at least 4 and let X denote S_n or A_n. Then $p_1(X) \leq 1-(1/n)+(2/3n^2)$.*

Proof. Clearly, $p_1(X)$ is less or equal than the probability that a random ordered pair of elements of X generates a permutation group with no fixed point, which in turn, by Bonferroni inequalities (truncated Inclusion-Exclusion Principle), is at most
$$\frac{1}{(n!)^2}\Big((n!)^2-\binom{n}{1}((n-1)!)^2+\binom{n}{2}((n-2)!)^2\Big).$$
But this former expression is less or equal than $1-(1/n)+(2/3n^2)$. □

Lemma 2.2. *Let n be an integer at least 5 and let X denote S_n or A_n. Then $1-(1/n)-(8.2/n^2) < p_1(X)$.*

Proof. First let $X = S_n$. Then
$$1-p_1(S_n) \leq \frac{1}{(n!)^2}\Big(n((n-1)!)^2+\binom{n}{2}3((n-2)!)^2+\sum_{k=3}^{[n/2]}\binom{n}{k}((n-k)!k!)^2\Big) <$$

$$< \frac{1}{n} + \frac{1.5}{n(n-1)} + \frac{3}{(n-1)(n-2)} < \frac{1}{n} + \frac{8.2}{n^2}$$

where the first 3 in these inequalities comes from the fact that $p_1(S_2) = 3/4$. The same argument applies in case $X = A_n$. □

We remark that by Lemmas 2.1 and 2.2 and by [6, Remark 3] we may obtain explicit upper and lower bounds for the number of subgroups of index n of a free group of rank 2 and also for the number of indecomposable permutations in S_n (in this context $x \in S_n$ is called indecomposable if there is no positive integer $m < n$ such that x maps $\{1, 2, \dots, m\}$ into itself).

3. Imprimitive groups

Let X be S_n or A_n and let $p_2(X)$ be the probability that a random ordered pair of elements of X generates an imprimitive transitive group. A maximal imprimitive subgroup of X has the form $(S_a \wr S_b) \cap X$ where a and b are positive integers at least 2 with $ab = n$. For the proof of Theorem 1.1 we will use the following upper bounds for $p_2(X)$ in the various cases for n.

Lemma 3.1. *Let n be a composite integer at least 10. Then we have the following.*

(i) *If $43 \leq n$ then $p_2(X) \leq n/2^{[(n+3)/2]}$.*
(ii) *If $23 \leq n \leq 42$ then $p_2(X) \leq ((n/\ell)!^{\ell}\ell!)/(2(n-1)!)$ where ℓ is the smallest prime divisor of n.*
(iii) *If $10 \leq n \leq 22$ then $p_2(X) \leq \sum_{\substack{a,b>1 \\ ab=n}} (a!^b b!)/n!$.*

Proof. Clearly, for all composite n, we have

$$p_2(X) \leq \sum_{\substack{a,b>1 \\ ab=n}} \Big(\frac{n!}{a!^b b!}\Big)\frac{(a!^b b!)^2}{(n!)^2} = \sum_{\substack{a,b>1 \\ ab=n}} \frac{a!^b b!}{n!}.$$

This gives (iii). By the proof of [18, Lemma 2.1] we also have

$$\sum_{\substack{a,b>1 \\ ab=n}} \frac{a!^b b!}{n!} \leq \frac{(n/\ell)!^{\ell}\ell!}{2(n-1)!}$$

where ℓ is the smallest prime divisor of n. This gives (ii). Finally, again by the proof of [18, Lemma 2.1], we have $((n/\ell)!^{\ell}\ell!)/(2(n-1)!) \leq n/2^{[(n+3)/2]}$ for $n \geq 8$. This gives (i). □

4. Primitive groups

Let X be S_n or A_n and let $p_3(X)$ be the probability that a random ordered pair of elements of X generates a primitive group different from A_n or S_n. Before we bound this probability we need some preliminary results.

For an integer n at least 5 let $r(S_n)$ be the number of conjugacy classes of maximal primitive subgroups of S_n apart from A_n plus the number of conjugacy classes of maximal almost simple primitive subgroups of A_n (for a partial explanation of this definition see the second paragraph of the proof of Lemma 4.1), and let $r(A_n)$ be the number of conjugacy classes of maximal primitive subgroups of A_n. We say that two finite primitive permutation groups different from the full alternating group and the full symmetric group (of their degrees) lie in the same cohort if and only if they have the same degree and their respective socles are permutation isomorphic.

Lemma 4.1. *Let n be an integer at least 10 and let X be S_n or A_n. Then we have the following.*

(i) $r(X) \leq n^{3(\log_2 n)^2}$ *for* $n \geq 1000$.
(ii) $r(S_n)$ *is at most* 2 *times the number of cohorts of primitive groups of degree* n.
(iii) $r(A_n)$ *is at most* 3 *times the number of cohorts of primitive groups of degree* n.
(iv) $r(X) \leq 36$ *for* $23 \leq n < 1000$.
(v) $r(X) \leq 12$ *for* $12 \leq n \leq 22$.
(vi) $r(X) \leq 9$ *for* $n = 10$ *or* $n = 11$.

Proof. (i) By [19, Table 7.1] we see that there are at most $n^2 + 12n^3n^{2(\log_2 n)^2} + 2n^{4(1+5\log_2 n)}$ conjugacy classes of maximal almost simple primitive subgroups in S_n. Similarly, as it is proved in [19, Section 9.4], the same upper bound holds for the number of conjugacy classes of maximal almost simple primitive subgroups in A_n which are different from M_{23} (in case $n = 23$) and different from M_{24} (in case $n = 24$). But we only consider the case $n \geq 1000$.

Let X be A_n or S_n. By [15], a maximal subgroup G of X which is different from an almost simple primitive group is either wreath product primitive, affine primitive, or diagonal primitive, and has the form $G = H \cap X$ where H is a maximal subgroup of S_n of the same type as G.

By [19, Table 7.1.], the number of conjugacy classes of maximal primitive subgroups of S_n of wreath product type or affine type is at most $1 + \log_2 n$. By the remark above on maximal subgroups of A_n, we see that the number of conjugacy classes of maximal primitive subgroups of A_n of wreath product type or affine type is at most $1 + \log_2 n$.

By [17, Page 350], there are at most 2 conjugacy classes of maximal primitive subgroups of S_n of diagonal type. Hence there are at most 2 conjugacy classes of maximal primitive subgroups of A_n of diagonal type.

Putting the above together, we only need to see the validity of the following inequality for $n \geq 1000$.

$$2n^2 + 24n^3n^{2(\log_2 n)^2} + 4n^{4(1+5\log_2 n)} + 1 + \log_2 n + 2 \leq n^{3(\log_2 n)^2}.$$

(ii) This follows from [19, Lemma 8.2.6] and [19, Lemma 9.5.5].

(iii) This follows from [19, Lemma 8.2.6], [19, Lemma 2.1.4] and [19, Lemma 9.5.5] together with the observation that if S_n acts transitively on a given set, then A_n has at most two orbits on the same set.

Statements (iv), (v), and (vi) follow from (iii) and [7, Table 4]. □

For a positive integer n at least 10 let $h(n)$ be the maximum order of a proper primitive subgroup of S_n apart from A_n.

Lemma 4.2. *Let n be a positive integer at least 10. Then we have the following.*

(i) *If $n \geq 12$ then $h(n) \leq 50n^{\sqrt{n}}$.*
(ii) *$h(10) = 1440$ and $h(11) = 7920$.*

Proof. Part (i) (for all n) is [18, Corollary 1.1]. Part (ii) is established by [12]. □

Finally, we obtain bounds for $p_3(X)$.

Lemma 4.3. *Let n be an integer at least 10 and let X denote S_n or A_n. Then we have the following.*

(i) *If $n \geq 1000$ then $p_3(X) \leq (100n^{\sqrt{n}}n^{3(\log_2 n)^2})/n!$.*
(ii) *If $23 \leq n < 1000$ then $p_3(X) \leq (3600n^{\sqrt{n}})/n!$.*
(iii) *If $12 \leq n \leq 22$ then $p_3(X) \leq (1200n^{\sqrt{n}})/n!$.*
(iv) *If $n = 10$ or 11 then $p_3(X) \leq (18h(n))/n!$.*

Proof. The statements follow from Lemma 4.1, Lemma 4.2, and from the inequality $p_3(X) \leq (h(n)r(X))/|X|$. □

5. Proof of Theorem 1.1

The upper bound of Theorem 1.1 follows from Lemma 2.1.

By [12] (see function `EulerianFunction`) it is easy to check that the lower bound of Theorem 1.1 holds for $n \leq 9$. Indeed, $p(A_4) = 96/144$, $p(S_4) = 312/576$, $p(A_5) = p(S_5) = 19/30$, $p(A_6) = p(S_6) = 53/90$, $p(A_7) = 229/315$, $p(S_7) = 2003/2520$, $p(A_8) = 133/180$, $p(S_8) = 16057/20160$, $p(A_9) = 15403/18144$, and $p(S_9) = 155947/181440$.

To see the lower bound of Theorem 1.1 for $n \geq 10$ one can use Lemma 2.2 and the above statements of Lemma 3.1 and Lemma 4.3 to verify the inequality

$$1 - p(X) \leq (1 - p_1(X)) + p_2(X) + p_3(X) < (1/n) + (13/n^2).$$

References

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

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

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

[4] R. Cori, Indecomposable permutations, hypermaps and labeled Dyck paths. *J. Combin. Theory Ser. A* **116** (2009), no. 8, 1326-1343.

[5] J. D. Dixon, The probability of generating the symmetric group. *Math. Z.* **110** (1969) 199-205.

[6] J. D. Dixon, Asymptotics of generating the symmetric and alternating groups. *Electron. J. Combin.* **12** (2005) Research paper 56, 5 pp.

[7] J. D. Dixon and B. Mortimer, The primitive permutation groups of degree less than 1000. *Math. Proc. Camb. Phil. Soc.* **103**, (1988), 213-237.

[8] A. Erfanian, A note on growth sequences of alternating groups. *Arch. Math. (Basel)* **78** (2002), no. 4, 257-262.

[9] A. Erfanian, A note on growth sequences of $\mathrm{PSL}(m, q)$. *Southeast Asian Bull. Math.* **29** (2005), no. 4, 697-713.

[10] A. Erfanian and R. Rezaee, On the growth sequences of $\mathrm{PSp}(2m, q)$. *Int. J. Algebra* **1** (2007), no. 1-4, 51-62.

[11] A. Erfanian and J. Wiegold, A note on growth sequences of finite simple groups. *Bull. Austral. Math. Soc.* **51** (1995), no. 3, 495-499.

[12] The GAP Group, GAP – *Groups, Algorithms, and Programming, Version 4.4*; 2005, (http://www.gap-system.org).

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

[14] The Kourovka Notebook. Unsolved problems in group theory. Seventeenth augmented edition, 2010. Edited by V. D. Mazurov and E. I. Khukhro.

[15] M. W. Liebeck; C. E. Praeger and J. Saxl, A classification of maximal subgroups of the finite alternating and symmetric groups. *J. Algebra* **111** (1987) no 2, 365-383.

[16] M. W. Liebeck and A. Shalev, Simple groups, probabilistic methods, and a conjecture of Kantor and Lubotzky. *J. Algebra* **184** (1996), no. 1, 31–57.

[17] M. W. Liebeck and A. Shalev, Maximal subgroups of symmetric groups. *J. Combin. Theory Ser. A* **75** (1996), no. 2, 341-352.

[18] A. Maróti, On the orders of primitive groups. *J. Algebra* **258** (2002), no. 2, 631-640.

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

MTA Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

E-mail address: maroti@renyi.hu

Dipartimento di Matematica e Fisica, Università Cattolica del Sacro Cuore, Via dei Musei 41, 25121 Brescia, Italy

E-mail address: c.tamburini@dmf.unicatt.it