Asymptotics of generating the symmetric and alternating groups

John D. Dixon
School of Mathematics and Statistics
Carleton University,
Ottawa, Ontario K2G 0E2
Canada
jdixon@math.carleton.ca

Submitted: Jul 18, 2005; Accepted: Oct 8, 2005; Published: Nov 7, 2005
MSC 2000: Primary 20B30; Secondary 20P05 05A16 20E05

Abstract

The probability that a random pair of elements from the alternating group A_n generates all of A_n is shown to have an asymptotic expansion of the form $1 - 1/n - 1/n^2 - 4/n^3 - 23/n^4 - 171/n^5 - \dots$. This same asymptotic expansion is valid for the probability that a random pair of elements from the symmetric group S_n generates either A_n or S_n. Similar results hold for the case of r generators ($r > 2$).

1 Introduction

In [5] I proved that the probability that a random pair of elements from the symmetric group S_n will generate either S_n or A_n is at least $1 - 2/(\log\log n)^2$ for large enough n. This estimate was improved by Bovey and Williamson [3] to $1 - \exp(-\sqrt{\log n})$. Finally Babai [1] showed that the probability has the asymptotic form $1 - 1/n + O(1/n^2)$. Unlike the earlier estimates, the proof of Babai's result uses the classification of finite simple groups.

Babai's result depends on two elementary results from [5], namely: the probability t_n that a pair of elements in S_n generates a transitive group is $1 - 1/n + O(1/n^2)$; and the probability that a pair of elements generates a transitive, imprimitive group of S_n is $\leq n2^{-n/4}$. Using the classification, he shows that the probability that a pair of elements generates a primitive subgroup of S_n different from A_n or S_n is $< n^{\sqrt{n}}/n!$ for all sufficiently large n. Thus the probability that a pair of elements of S_n generates a transitive group but does not generate either S_n or A_n is $O(n2^{-n/4} + n^{\sqrt{n}}/n!) = O(n^{-k})$ for all k.

The object of the present paper is to show that there is an asymptotic series of the form $t_n \sim 1 + \sum c_k/n^k$ so that

$$t_n = 1 + c_1/n + c_2/n^2 + ... + c_m/n^m + O(1/n^{m+1}) \text{ for } m = 1, 2, ... \ .$$

By what we have just said, the same asymptotic series is valid for the probability that a pair of elements of S_n generates either A_n or S_n. We shall also show that this asymptotic series is valid for the probability that a pair of elements in A_n generates A_n.

More precisely, we shall prove the following.

Theorem 1 *The probability t_n that a random pair of elements from S_n generates a transitive group has an asymptotic series of the form described above. The first few terms are*

$$t_n \sim 1 - \frac{1}{n} - \frac{1}{n^2} - \frac{4}{n^3} - \frac{23}{n^4} - \frac{171}{n^5} - \frac{1542}{n^6} - ... \ .$$

The same asymptotic series is valid for the probability that the subgroup generated by a random pair of elements from S_n is either A_n or S_n.

Theorem 2 *If a_n is the number of pairs $(x, y) \in A_n \times A_n$ which generate a transitive subgroup of A_n and s_n is the number of pairs $(x, y) \in S_n \times S_n$ which generate a transitive subgroup of S_n, then $s_n - 4a_n = (-1)^n 3 \cdot (n-1)!$ for all $n \geq 1$. Thus for $n \geq 2$ the probability $4a_n/(n!)^2$ that a random pair of elements from A_n generates a transitive subgroup is equal to $t_n \pm 3/(n \cdot n!)$. Hence the probability that a random pair of elements from A_n generates A_n has the same asymptotic expansion as given above for t_n.*

Remark 3 *The sequence $\{t_n\}$ also appears in other contexts. Peter Cameron has pointed out to me that a theorem of M. Hall shows that the number $N(n, 2)$ of subgroups of index n in a free group of rank 2 is equal to $n!nt_n$ (see (1) below and [6]). On the other hand, a result of Comtet [4] (quoted in [8, page 48] and [7, Example 7.4]) implies that $n!nt_n = c_{n+1}$ for all $n \geq 1$ where c_n is 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 $\{1, 2, ..., m\}$ into itself).*

We shall discuss a generalisation to more than two generators at the end of this paper.

2 Lattice of Young subgroups

In the present section we shall prove Theorem 2. Consider the set $\mathcal{P}$ of all (set) partitions of $\{1, 2, ..., n\}$. If $\Pi = \{\Sigma_1, ...\Sigma_k\}$ is a partition with k parts then, as usual, we define the *Young subgroup* $Y(\Pi)$ as the subgroup of S_n consisting of all elements which map each of the parts Σ_i into itself. The set of Young subgroups of S_n is a lattice, and we define an ordering on $\mathcal{P}$ by writing $\Pi \geq \Pi'$ when $Y(\Pi) \leq Y(\Pi')$. Under this ordering the greatest element of $\mathcal{P}$ is $\Pi_1 := \{\{1\},\{2\},...,\{n\}\}$ and the least element is $\Pi_0 := \{\{1,2,...,n\}\}$. Consider the Möbius function μ on $\mathcal{P}$ (see, for example, [8, Section 3.7]), and write $\mu(\Pi)$ in place of $\mu(\Pi_0,\Pi)$. By definition, $\mu(\Pi_0) = 1$ and $\sum_{\Pi' \leq \Pi} \mu(\Pi') = 0$ for all $\Pi > \Pi_0$. Example 3.10.4 of [8] shows that $\mu(\Pi) = (-1)^{k+1}(k-1)!$ whenever Π has k parts.

Now let $f_A(\Pi)$ (respectively $f_S(\Pi)$) be the number of pairs (x,y) of elements from A_n (respectively, S_n) such that the parts of Π are the orbits of the group $\langle x,y\rangle$ generated by x and y. Similarly let $g_A(\Pi)$ and $g_S(\Pi)$, respectively, be the number of pairs for which the parts of Π are invariant under $\langle x,y\rangle$; that is, for which $x,y \in Y(\Pi)$. Every Young subgroup $Y(\Pi)$ except for the trivial group $Y(\Pi_1)$ contains an odd permutation and so we have

$$g_A(\Pi) = \frac{1}{4}\left|Y(\Pi)\right|^2 = \frac{1}{4}g_S(\Pi) \text{ for } \Pi \neq \Pi_1 \text{ and } g_A(\Pi_1) = g_S(\Pi_1) = 1.$$

We also have

$$g_A(\Pi) = \sum_{\Pi' \geq \Pi} f_A(\Pi') \text{ and } g_S(\Pi) = \sum_{\Pi' \geq \Pi} f_S(\Pi').$$

Since $\mu(\Pi_1) = (-1)^{n+1}(n-1)!$, the Möbius inversion formula [8, Propositon 3.7.1] now shows that

$$\begin{aligned} s_n = f_S(\Pi_0) &= \sum_{\Pi} \mu(\Pi) g_S(\Pi) = 4\sum_{\Pi} \mu(\Pi) g_A(\Pi) - 3\mu(\Pi_1)\cdot 1 \\ &= 4f_A(\Pi_0) - 3\mu(\Pi_1) = 4a_n + (-1)^n 3(n-1)! \end{aligned}$$

as claimed.

3 Asymptotic expansion

It remains to prove Theorem 1 and obtain an asymptotic expansion for $t_n = s_n/(n!)^2$. It is possible that this can be done with a careful analysis of the series $f_S(\Pi_0) = \sum_{\Pi} \mu(\Pi) g_S(\Pi)$ since the size of the terms decreases rapidly: the largest are those when Π has the shapes $[1, n-1]$, $[2, n-2]$, $[1^2, n-2]$, ...; but the argument seems to require considerable care. We therefore approach the problem from a different direction using a generating function for t_n which was derived in [5]. Consider the formal power series

$$E(X) := \sum_{n=0}^{\infty} n! X^n \text{ and } T(X) := \sum_{n=1}^{\infty} n! t_n X^n.$$

Then Section 2 of [5] shows that $E(X) = \exp T(X)$ and so

$$T(X) = \log E(X). \tag{1}$$

We shall apply a theorem of Bender [2, Theorem 2] (quoted in [7, Theorem 7.3]):

Theorem 4 *(E.A. Bender) Consider formal power series* $A(X) := \sum_{n=1}^{\infty} a_n X^n$ *and* $F(X,Y)$ *where* $F(X,Y)$ *is analytic in some neighbourhood of* $(0,0)$*. Define* $B(X) := F(X, A(X)) = \sum_{n=0}^{\infty} b_n X^n$*, say. Let* $D(X) := F_Y(X, A(X)) = \sum_{n=0}^{\infty} d_n X^n$*, say, where* $F_Y(X,Y)$ *is the partial derivative of* F *with respect to* Y*.*

Now, suppose that all $a_n \neq 0$ *and that for some integer* $r \geq 1$ *we have: (i)* $a_{n-1}/a_n \to 0$ *as* $n \to \infty$*; and (ii)* $\sum_{k=r}^{n-r} |a_k a_{n-k}| = O(a_{n-r})$ *as* $n \to \infty$*. Then*

$$b_n = \sum_{k=0}^{r-1} d_k a_{n-k} + O(a_{n-r}).$$

Using the identity (1) we take $A(X) = E(X) - 1$, $F(X,Y) = \log(1+Y)$, $D(X) = 1/E(X)$ and $B(X) = T(X)$ in Bender's theorem. Then condition (i) is clearly satisfied and (ii) holds for every integer $r \geq 1$ since for $n > 2r$

$$\sum_{k=r}^{n-r} k!(n-k)! \leq 2r!(n-r)! + (n-2r-1)(r+1)!(n-r-1)! < \{2r! + (r+1)!\}\,(n-r)!.$$

Thus we get

$$n!t_n = \sum_{k=0}^{r-1} d_k (n-k)! + O((n-r)!)$$

and hence

$$t_n = 1 + \sum_{k=1}^{r-1} \frac{d_k}{[n]_k} + O(n^{-r})$$

where $[n]_k = n(n-1)...(n-k+1)$. The Stirling numbers $S(m,k)$ of the second kind satisfy the identity

$$\sum_{m=k}^{\infty} S(m,k) X^m = \frac{X^k}{(1-X)(1-2X)...(1-kX)}$$

where the series converges for $|X| < 1$ (see [8, page 34]). Thus for $n \geq k > 0$ we have

$$\frac{1}{[n]_k} = \frac{1}{n^k(1-1/n)(1-2/n)...(1-(k-1)/n)} = \sum_{m=k-1}^{\infty} S(m,k-1)\frac{1}{n^{m+1}}.$$

This shows that t_n has an asymptotic expansion of the form $1 + \sum_{k=1}^{\infty} c_k n^{-k}$ where $c_k = \sum_{i=1}^{k-1} S(k-1,i) d_{i+1}$ since $S(m,0) = 0$ for $m = 0$. To compute the numerical values of the coefficients we can use a computer algebra system such as Maple to obtain

$$D(X) = 1/E(X) = 1 - X - X^2 - 3X^3 - 13X^4 - 71X^5 - 461X^6 - 3447X^7 - ...$$

and then

$$\begin{aligned} t_n &\sim 1 - \frac{1}{[n]_1} - \frac{1}{[n]_2} - \frac{3}{[n]_3} - \frac{13}{[n]_4} - \frac{71}{[n]_5} - \frac{461}{[n]_6} - ... \\ &\sim 1 - \frac{1}{n} - \frac{1}{n^2} - \frac{4}{n^3} - \frac{23}{n^4} - \frac{171}{n^5} - \frac{1542}{n^6} - ... . \end{aligned}$$

4 Generalization to more than two generators

In view of the theorem of M. Hall mentioned in Remark 3 there is some interest in extending the analysis for t_n to the case of r generators where $r \geq 2$. Let $t_n(r)$ be the probability that r elements of S_n generate a transitive group (so $t_n = t_n(2)$). A simple argument similar to that in Section 2 of [5] shows that the generating function $T_r(X) := \sum_{n=1}^{\infty}(n!)^{r-1}t_n(r)X^n$ satisfies the equation

$$T_r(X) = \log E_r(X)$$

where $E_r(X) := \sum_{n=0}^{\infty}(n!)^{r-1}X^n$. Now, following the same path as we did in the previous section, an application of Bender's theorem leads to

$$t_n(r) \sim 1 + \sum_{k=1}^{\infty} \frac{d_k(r)}{([n]_k)^{r-1}}$$

where the coefficients $d_k(r)$ are given by $1/E_r(X) = \sum_{k=0}^{\infty} d_k(r)X^k$. For example, we find that

$$1/E_3(X) = 1 - X - 3X^2 - 29X^3 - 499X^4 - 13101X^5 - ...$$

so

$$\begin{aligned} t_n(3) &\sim 1 - \frac{1}{[n]_1^2} - \frac{3}{[n]_2^2} - \frac{29}{[n]_3^2} - \frac{499}{[n]_4^2} - \frac{13101}{[n]_5^2} ... \\ &\sim 1 - \frac{1}{n^2} - \frac{3}{n^4} - \frac{6}{n^5} - ... \,. \end{aligned}$$

References

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

[2] E.A. Bender, An asymptotic expansion for some coefficients of some formal power series, J. London Math. Soc. **9** (1975) 451–458.

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

[4] L. Comtet, "Advanced Combinatorics", Reidel, 1974.

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

[6] M. Hall, Jr., Subgroups of finite index in free groups, Canad. J. Math. **1** (1949) 187–190.

[7] A.M. Odlyzko, Asymptotic enumeration methods, *in* "Handbook of Combinatorics (Vol. II)" (eds.: R.L. Graham, M. Grötschel and L. Lovász), M.I.T. Press and North-Holland, 1995 (pp. 1063–1229).

[8] R.P. Stanley, "Enumerative Combinatorics (Vol. 1)", Wadsworth & Brooks/Cole, 1986 (reprinted Cambridge Univ. Press, 1997).