Periodica Mathematica Hungarica Vol. 18 (4), (1987), pp. 259–269

GENERATION OF ALTERNATING GROUPS BY PAIRS OF CONJUGATES

L. B. BEASLEY (Logan), J. L. BRENNER (Palo Alto), P. ERDŐS (Budapest), M. SZALAY (Budapest) and A. G. WILLIAMSON (Haywards Heath)

Abstract

Considering the conjugacy classes of the alternating group of degree n, those classes that contain a pair of generators are in the majority. In fact, the proportion of such classes is $1 - \varepsilon(n)$, and $\varepsilon(n) \to 0$ as $n \to \infty$.

1. Introduction

In this article, we obtain the following result for the alternating groups $\mathsf{Alt}(n)$:

The proportion of conjugacy classes in $\mathsf{Alt}(n)$ *that contain a pair of generators approaches* 1 *as* $n \to \infty$.

In Section 2 we give a quick proof of a weaker form of this asymptotic result. In the weaker form, "$n \to \infty$" is replaced by the condition "n increases through some set Σ_0 that has density 1 in the set $\mathbf{Z}$ of all integers". The argument uses results of Erdős, Lehner, Cameron, Neumann and Teague ([9], [5]) together with a combinatorial construction.

The strong form of the theorem is proved in Section 3.

Some results from number theory needed in the proofs are established in Sections 2 and 3.

The number of classes involved in the construction in Section 3 is large enough to constitute an overwhelming majority in the set of all classes (as we show). It is reasonable to suppose that many more classes contain a pair of generators. This is indeed true; the proof would be too intricate to include,

AMS (MOS) subject classifications (1980). Primary 20P05; Secondary 20F05, 20D06, 20D60.
Key words and phrases. Alternating groups, pairs of generators in almost all conjugacy classes.

Akadémiai Kiadó, Budapest
D. Reidel, Dordrecht

since no uniform arguments seem to be available. On the other hand, although the discussion in Section 3 is not limpid in its simplicity, the argument does use a single technique.

2. A preliminary result

We first recall a theorem, due to P. Erdős and J. Lehner, concerning the number of summands in a partition.

2.01. THEOREM [9]. *Denote by $p(n)$ the number of unrestricted partitions of a positive integer n and by $p_k(n)$ the number of partitions of n which have at most k summands. If*

$$k = C^{-1}n^{1/2} \log n + xn^{1/2} ,$$

then

$$\lim \frac{p_k(n)}{p(n)} = \exp \left[-2C^{-1} \exp - (1/2)Cx\right]$$

as $n \to \infty$. Here $C = \pi\ (2/3)^{1/2}$.

2.02. COROLLARY. *If $p^{(l)}(n)$ denotes the number of partitions of n such that the average size of a summand is at least l and $1 \leq l \leq n^{1/2}/\log n$, then*

$$\lim \frac{p^{(l)}(n)}{p(n)} = 1$$

as $n \to \infty$.

PROOF. 2.01 yields that, for almost all partitions of n (i.e. with the exception of $o(p(n))$ partitions of n, as $n \to \infty$), the number of summands is

$$\big(1 + o(1)\big)C^{-1}n^{1/2} \log n ,$$

consequently the average size of a summand is

$$\big(1 + o(1)\big) \frac{Cn^{1/2}}{\log n} > \frac{n^{1/2}}{\log n}$$

in almost all partitions of n.

We also recall a result of P. J. Cameron, P. M. Neumann, and D. N. Teague:

2.03. THEOREM [5]. *The number of integers n that can be the degree of a primitive group contained properly in* Alt (n) *is vanishingly small. More precisely*