Combinatorics, Probability and Computing (2002) 11, 447–464. © 2002 Cambridge University Press
DOI: 10.1017/S0963548302005217 Printed in the United Kingdom

Permutations with Restricted Cycle Structure and an Algorithmic Application

ROBERT BEALS,[1] CHARLES R. LEEDHAM-GREEN,[2]
ALICE C. NIEMEYER,[3]† CHERYL E. PRAEGER[3]†
and ÁKOS SERESS[4]‡

[1] IDA Center for Communications Research,
Princeton, NJ 08540, USA
(e-mail: beals@idaccr.org)

[2] School of Mathematical Sciences,
Queen Mary, University of London, London E1 4NS, England
(e-mail: crlg@maths.qmw.ac.uk)

[3] Department of Mathematics and Statistics,
The University of Western Australia, Crawley, WA 6009, Australia
(e-mail: alice@maths.uwa.edu.au)

[4] Department of Mathematics,
The Ohio State University, Columbus OH 43210, USA
(e-mail: akos@math.ohio-state.edu)

Received 13 July 2000; revised 14 August 2001

Let q be an integer with $q \geqslant 2$. We give a new proof of a result of Erdős and Turán determining the proportion of elements of the finite symmetric group S_n having no cycle of length a multiple of q. We then extend our methods to the more difficult case of obtaining the proportion of such elements in the finite alternating group A_n. In both cases, we derive an asymptotic formula with error term for the above mentioned proportion, which contains an unexpected occurrence of the Gamma-function.

We apply these results to estimate the proportion of elements of order $2f$ in S_n, and of order $3f$ in A_n and S_n, where $\gcd(2, f) = 1$, and $\gcd(3, f) = 1$, respectively, and $\log f$ is polylogarithmic in n. We also give estimates for the probability that the fth power of such elements is a transposition or a 3-cycle, respectively. An algorithmic application of these results to computing in A_n or S_n, given as a black-box group with an order oracle, is discussed.

† Research partially supported by an Australian Research Council large grant.
‡ Research partially supported by the NSF.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

1. Introduction

The main results of this paper belong to the area of statistical group theory, a discipline initiated by a series of papers of Erdős and Turán [11]–[17]. Erdős and Turán were mainly interested in properties satisfied by almost all elements of symmetric groups; two typical examples are bounds for the orders of permutations and for the number of cycles in permutations. In later work, the distribution of element orders received the most attention. The Erdős–Turán results were extended and improved by Best [7], Bovey [8], Nicolas [21], Goh and Schmutz [19], and Barbour and Tavaré [3]. A related theory about the distribution of partitions, which is relevant for representations of the symmetric groups, was established by Szalay and Turán [24]–[25].

Our results are also related to the Erdős–Turán investigation of element orders but, as we are primarily motivated by algorithmic applications, we are interested in certain properties which are *not* satisfied by almost all elements of S_n and A_n. In Section 2, we derive a formula for the proportion of elements in S_n which have no cycles of length divisible by q for some fixed q. For prime powers q, this result was already obtained in a paper of Erdős and Turán [12], and their method extends easily to all q. Here we give a new derivation, and determine the exact asymptotic behaviour of this proportion for fixed q and increasing n. In Section 3, we extend these results to the alternating groups.

In Section 4, we present a modification of a result of Barbour and Tavaré [3] on the upper bound for the order of most elements of S_n. This modification weakens the upper bound on the order while sharpening the error term significantly. We are grateful to A. Barbour for the elegant proof of this result.

Combining the results of the previous sections, in Section 5 we estimate the proportion of elements of order $2f$ in S_n and order $3f$ in A_n or S_n, where f is polylogarithmic in n and odd in the first case, and not divisible by 3 in the second. We also give estimates for the probability that the fth power of such elements is a transposition or a 3-cycle, respectively.

Finally, in Section 6, we describe randomized algorithms which are based on the probability estimates of Section 5. If a group G is isomorphic to S_n or A_n, we often need elements of G which act as transpositions or 3-cycles in the natural permutation representation of G on n points (although we may not have this natural action explicitly). The proportion of transpositions and 3-cycles is negligible in the symmetric and alternating groups, so a random search will find one of them only with very low probability. However, the estimates in Section 5 show that searching for random elements of order $2f$ or $3f$ as described above has a reasonable chance of success, and the probability that the fth power is a transposition or a 3-cycle is still large enough for fast algorithmic applications. The significance of this result is that in some important algorithmic situations, there are efficient procedures to determine the order of an element of G (see [10] and [6]) and to decide whether an element of G is a transposition or a 3-cycle in the natural representation (see [5] and [6]).

The algorithm for finding transpositions and 3-cycles indicated in the previous paragraph works in the quite general setting of black-box groups [2], provided that we are able to compute the order of any given group element, and to test whether a given element is

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

a transposition or a 3-cycle. Such black-box groups are said to be equipped with an *order oracle*, a *transposition oracle*, or a 3-*cycle oracle*, respectively. For details about black-box groups isomorphic to finite alternating or symmetric groups, and how transpositions and 3-cycles are used in algorithms, we refer to [4]–[6] and [9].

2. Elements of S_n with no cycle length divisible by q

Let n and q be positive integers with $q \geqslant 2$, and let $s_{\neg q}(n)$ denote the proportion of elements g of S_n such that, in the disjoint cycle representation for g, no cycle has length a multiple of q. In particular, if q is a prime power, then $s_{\neg q}(n)$ is the proportion of elements of S_n with order not divisible by q. We define $s_{\neg q}(0) := 1$.

Our basic tool is the following recursive formula.

Lemma 2.1. *For $n \geqslant q$,*

$$n\ s_{\neg q}(n) = \sum_{k=1}^{q-1} s_{\neg q}(n-k) + (n-q)s_{\neg q}(n-q).$$

Proof. For a positive integer m, let $S_{\neg q}(m)$ denote the subset of S_m consisting of permutations with no cycles of length divisible by q and let

$$N_q(m) := \{k \in \mathbb{Z} \mid 1 \leqslant k \leqslant m \text{ and } k \not\equiv 0 (\mathrm{mod}\ q)\}. \tag{2.1}$$

Then

$$|S_{\neg q}(n)| = \sum_{k \in N_q(n)} \binom{n-1}{k-1} (k-1)!\ |S_{\neg q}(n-k)|, \tag{2.2}$$

since the elements $x \in S_{\neg q}(n)$ can be enumerated according to the length k of the cycle of x containing the point 1. Note that $k \in N_q(n)$, and the permutation induced by x on the $n-k$ points outside of the x-cycle containing 1 lies in $S_{\neg q}(n-k)$. Noting that $|S_{\neg q}(m)| = m!\ s_{\neg q}(m)$, equation (2.2) is equivalent to

$$n\ s_{\neg q}(n) = \sum_{k \in N_q(n)} s_{\neg q}(n-k). \tag{2.3}$$

Applying this formula for $n-q$, we obtain

$$(n-q)s_{\neg q}(n-q) = \sum_{k' \in N_q(n-q)} s_{\neg q}(n-q-k'). \tag{2.4}$$

Finally, using the fact that, for $k > q$, $k \in N_q(n)$ if and only if $k' = k - q \in N_q(n-q)$, equations (2.3) and (2.4) yield the statement of the lemma. □

Lemma 2.2. *For all $m \geqslant 0$,*

$$s_{\neg q}(mq) = s_{\neg q}(mq+1) = \cdots = s_{\neg q}(mq+q-1).$$

Proof. We prove that $s_{\neg q}(n) = s_{\neg q}(q\lfloor n/q \rfloor)$ by induction on n. We have $1 = s_{\neg q}(0) = s_{\neg q}(1) = \cdots = s_{\neg q}(q-1)$, so we may suppose that $n \geqslant q$.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

If $n = mq + r$, where $1 \leqslant r \leqslant q-1$, then by Lemma 2.1 and by the induction hypothesis,

$$\begin{aligned} n\ s_{\neg q}(n) &= \sum_{k=1}^{q-1} s_{\neg q}(n-k) + (n-q)s_{\neg q}(n-q) \\ &= r\ s_{\neg q}(mq) + (n-1-r)s_{\neg q}(mq-q). \end{aligned} \tag{2.5}$$

Similarly,

$$(n-1)s_{\neg q}(n-1) = (r-1)s_{\neg q}(mq) + (n-1-r)s_{\neg q}(mq-q). \tag{2.6}$$

Taking the difference of (2.5) and (2.6), we obtain $n\ s_{\neg q}(n) - (n-1)s_{\neg q}(n-1) = s_{\neg q}(mq)$. By the induction hypothesis, $s_{\neg q}(n-1) = s_{\neg q}(mq)$ and so $s_{\neg q}(n) = s_{\neg q}(mq)$. □

Let γ denote Euler's constant, let $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ denote the Gamma-function and let $\log x$ denote the natural logarithm of x. We need the following information (for (2.8), see for example [1, p. 455]):

$$\begin{aligned} x - \frac{3x^2}{4} < \log(1+x) \qquad &\text{for } -\frac{1}{4} < x < 0 \quad \text{and} \\ \log(1+x) < x \ \text{ for } -1 < x, & \end{aligned} \tag{2.7}$$

$$\sum_{\ell=1}^{m} \frac{1}{\ell} = \gamma + \log m + \frac{1}{2m} - \frac{E(m)}{m^2}, \text{ where } 0 \leqslant E(m) \leqslant \frac{1}{8}. \tag{2.8}$$

Theorem 2.3. *Let $q \geqslant 2$ and $n \geqslant 1$. Set $c(q) = q^{1/q}\Gamma(1-\frac{1}{q})^{-1}$, so that, in particular, $c(2) = (\pi/2)^{-1/2} \cong 0.798$, $c(3) \cong 1.065$, $c(4) \cong 1.154$, and $c(9) \cong 1.184$. Then:*

(a) $s_{\neg q}(n) = \prod_{\ell=1}^{\lfloor n/q \rfloor} \left(1 - \frac{1}{\ell q}\right)$;

(b) *if $n \geqslant q$, then $c(q)n^{-1/q}(1-n^{-1}) \leqslant s_{\neg q}(n) \leqslant c(q)n^{-1/q}(1+2n^{-1})$, and hence $|s_{\neg q}(n) - c(q)n^{-1/q}| \leqslant 2c(q)n^{-1-1/q}$;*

(c) *if $n \geqslant q$, then $s_{\neg q}(n) = c(q)n^{-1/q} + O(n^{-1-1/q}) = (1+o(1))c(q)n^{-1/q}$.*

Proof. **(a)** Let $n = qm + r$, with $0 \leqslant r \leqslant q-1$. By Lemmas 2.1 and 2.2, $qm \cdot s_{\neg q}(mq) = (mq-1)s_{\neg q}(mq-q)$. Iterating, we obtain

$$s_{\neg q}(qm) = \prod_{\ell=1}^{m} \frac{\ell q - 1}{\ell q}.$$

For $1 \leqslant r \leqslant q-1$ the stated formula follows from this and from Lemma 2.2.

(b) We derive an interesting connection between the numbers $s_{\neg q}(mq)$ and the Gamma-function. Let $\mathbb{C}$ denote the complex plane and let $\mathrm{Log}(z)$ denote the main branch of the log-function in $\mathbb{C}\backslash\{0\}$. It is well known (see, for example, [22, Theorem 7.71]) that the functions $L_m(z)$ defined as follows,

$$L_m(z) := -\gamma z - \mathrm{Log}\ z - \sum_{\ell=1}^{m} \left(\mathrm{Log}\left(1 + \frac{z}{\ell}\right) - \frac{z}{\ell} \right), \tag{2.9}$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

converge uniformly on every compact subset of $\mathbb{C}\setminus\{0,-1,-2,\dots\}$ to an analytic function $L(z)$ and $e^{L(z)}=\Gamma(z)$. Note that, if we define $f_m(z)$ as

$$f_m(z) := e^{\sum_{\ell=1}^{m}\operatorname{Log}(1+z/\ell)} = \prod_{\ell=1}^{m}\left(1+\frac{z}{\ell}\right),$$

then $f_m\left(-\frac{1}{q}\right)=s_{\neg q}(mq)$. Applying the exp-function to (2.9) we obtain

$$e^{L_m(z)} = z^{-1}\cdot f_m(z)^{-1}\cdot e^{z(-\gamma+\sum_{\ell=1}^{m}\frac{1}{\ell})},$$

which for $z=-1/q$ yields, after rearranging,

$$s_{\neg q}(mq) = -q\cdot e^{-L_m(-1/q)}\cdot e^{q^{-1}(\gamma-\sum_{\ell=1}^{m}1/\ell)}. \tag{2.10}$$

We now derive upper and lower bounds for $e^{-L_m(-1/q)}$ and $e^{(\gamma-\sum_{\ell=1}^{m}1/\ell)}$. Let us first consider the term $e^{-L_m(-\frac{1}{q})}$. As $L(z)=\lim_{m\to\infty}L_m(z)$ it follows that

$$\begin{aligned} L(z) = \lim_{m\to\infty}L_m(z) &= -\gamma z - \operatorname{Log} z - \sum_{\ell=1}^{\infty}\left(\operatorname{Log}\left(1+\frac{z}{\ell}\right)-\frac{z}{\ell}\right)\\ &= L_m(z) - \sum_{\ell=m+1}^{\infty}\left(\operatorname{Log}\left(1+\frac{z}{\ell}\right)-\frac{z}{\ell}\right)\end{aligned}$$

Inserting $z=-1/q$ and rearranging, we obtain

$$L_m\left(-\frac{1}{q}\right) = L\left(-\frac{1}{q}\right) + \sum_{\ell=m+1}^{\infty}\left(\operatorname{Log}\left(1-\frac{1}{q\ell}\right)+\frac{1}{q\ell}\right).$$

By (2.7) and using the fact that $\int_{\ell=m+1}^{\infty}\frac{1}{\ell^2}dl\leqslant\frac{1}{m}$, we can see that

$$L\left(-\frac{1}{q}\right) - \frac{3}{4q^2m} \leqslant L_m\left(-\frac{1}{q}\right) \leqslant L\left(-\frac{1}{q}\right). \tag{2.11}$$

For the term $e^{(\gamma-\sum_{\ell=1}^{m}1/\ell)}$ we obtain from (2.8) that

$$-\log m - \frac{1}{2m} \leqslant \gamma - \sum_{\ell=1}^{m}\frac{1}{\ell} \leqslant -\log m - \frac{1}{2m} + \frac{1}{8m^2}. \tag{2.12}$$

Inserting (2.11) and (2.12) into (2.10), we get as an upper bound

$$\begin{aligned} s_{\neg q}(mq) &\leqslant -qe^{-(L(-1/q)-3/(4q^2m))}e^{(1/q)(-\log m-\frac{1}{2m}+\frac{1}{8m^2})}\\ &= \left(-\frac{1}{q}\Gamma\left(-\frac{1}{q}\right)\right)^{-1}\frac{1}{m^{1/q}}e^{\left(\frac{3}{4q^2m}-\frac{1}{2qm}+\frac{1}{8qm^2}\right)}.\end{aligned}$$

As $z\Gamma(z)=\Gamma(z+1)$ and as $\frac{3}{4q^2m}+\frac{1}{8qm^2}\leqslant\frac{1}{2qm}$ for all $q\geqslant 2$, this finally yields the upper bound

$$s_{\neg q}(mq) \leqslant \frac{1}{\Gamma\left(1-\frac{1}{q}\right)}\frac{1}{m^{1/q}} = \frac{c(q)}{(mq)^{1/q}}. \tag{2.13}$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

For the lower bound we obtain

$$s_{\neg q}(mq) \geqslant -qe^{-L(-1/q)}e^{(1/q)(-\log m - 1/2m)}$$
$$= \left(\Gamma\left(1-\frac{1}{q}\right)\right)^{-1}\frac{1}{m^{1/q}}e^{-1/2qm} = \frac{c(q)}{(mq)^{1/q}}e^{-1/2qm}.$$

For the case $n = qm + r$, $1 \leqslant r \leqslant q-1$, we observe in addition that

$$(mq)^{-1/q} = (n-r)^{-1/q} = n^{-1/q}\left(1-\frac{r}{n}\right)^{-1/q}.$$

Hence

$$\frac{c(q)}{n^{1/q}}\left(1-\frac{r}{n}\right)^{-1/q}e^{-1/2qm} \leq s_{\neg q}(n) \leq \frac{c(q)}{n^{1/q}}\left(1-\frac{r}{n}\right)^{-1/q}. \tag{2.14}$$

It is possible to verify directly that $1 \leqslant \left(1-\frac{r}{n}\right)^{-1/q} \leqslant 1+\frac{2}{n}$ and that $e^{-1/2qm} \geqslant 1-\frac{1}{n}$. Thus we have the first inequality in (b). The second inequality is a trivial consequence of the first one.

Part (c) follows immediately from (b). □

3. Elements of A_n with no cycle length divisible by q

We now turn to the problem of estimating the proportion $a_{\neg q}(n)$ of elements in A_n with no cycle length divisible by q, where q is an integer greater than 1. We define $a_{\neg q}(0) := 1$ and use an argument similar to the symmetric group case.

Lemma 3.1. *For $n \geqslant q$,*

$$n\, a_{\neg q}(n) = \sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ odd}}} a_{\neg q}(n-k) + \sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ even}}} (2s_{\neg q}(n-k) - a_{\neg q}(n-k)) + (n-q)X_{n-q},$$

where $X_{n-q} = a_{\neg q}(n-q)$ if q is even and $X_{n-q} = 2s_{\neg q}(n-q) - a_{\neg q}(n-q)$ if q is odd.

Proof. For a positive integer m, let $A_{\neg q}(m)$ denote the subset of A_m consisting of permutations with no cycles of length divisible by q. Enumerating the elements $x \in A_{\neg q}(n)$ according to the length k of the cycle containing 1, we have

$$|A_{\neg q}(n)| = \sum_{\substack{k\in N_q(n)\\ k \text{ odd}}} \binom{n-1}{k-1}(k-1)!\ |A_{\neg q}(n-k)|$$
$$+ \sum_{\substack{k\in N_q(n)\\ k \text{ even}}} \binom{n-1}{k-1}(k-1)!\ (|S_{\neg q}(n-k)| - |A_{\neg q}(n-k)|),$$

where $N_q(n)$ is given by (2.1), since, if k is even, then x induces an odd permutation on the $n-k$ points not in the cycle containing 1, while if k is odd, then x induces an even

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

permutation on these $n-k$ points. Dividing both sides by $(n-1)!/2$, we obtain

$$n\ a_{\neg q}(n) = \sum_{\substack{k\in N_q(n)\\ k \text{ odd}}} a_{\neg q}(n-k) + \sum_{\substack{k\in N_q(n)\\ k \text{ even}}} (2s_{\neg q}(n-k) - a_{\neg q}(n-k)). \tag{3.1}$$

Writing (3.1) for $n-q$ yields

$$\begin{aligned}(n-q)\ a_{\neg q}(n-q) = &\sum_{\substack{k'\in N_q(n-q)\\ k' \text{ odd}}} a_{\neg q}(n-q-k')\\ &+ \sum_{\substack{k'\in N_q(n-q)\\ k' \text{ even}}} (2s_{\neg q}(n-q-k') - a_{\neg q}(n-q-k')).\end{aligned} \tag{3.2}$$

Obviously, for any $k > q$, we have $k \in N_q(n)$ if and only if $k' \in N_q(n-q)$, where $k' := k-q$. Also, if q is even then $n-k$ is odd if and only if $n-q-k'$ is odd. Hence the difference of (3.1) and (3.2) is

$$\begin{aligned}n\ a_{\neg q}(n) - (n-q)\ a_{\neg q}(n-q) = &\sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ odd}}} a_{\neg q}(n-k)\\ &+ \sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ even}}} (2s_{\neg q}(n-k) - a_{\neg q}(n-k)),\end{aligned}$$

which immediately yields the statement of the lemma. On the other hand, if q is odd, then $n-k$ is odd if and only if $n-q-k'$ is even. In this case, the sum of (3.1) and (3.2) is

$$\begin{aligned}n\ a_{\neg q}(n) + (n-q)\ a_{\neg q}(n-q) = &\sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ odd}}} a_{\neg q}(n-k) + \sum_{\substack{1\leqslant k\leqslant q-1\\ k \text{ even}}} (2s_{\neg q}(n-k) - a_{\neg q}(n-k))\\ &+ \sum_{k'\in N_q(n-q)} 2s_{\neg q}(n-q-k').\end{aligned}$$

By (2.4) in the proof of Lemma 2.1, $\sum_{k'\in N_q(n-q)} s_{\neg q}(n-q-k') = (n-q)s_{\neg q}(n-q)$ and so the lemma follows in this case as well. □

Lemma 3.2. *Let $n = mq + r$ for some $m \geqslant 0$ and $1 \leqslant r \leqslant q-1$.*

(a) *If $2 \leqslant r \leqslant q-1$, then $a_{\neg q}(n) = s_{\neg q}(n)$.*
(b) *If $r = 1$, then $a_{\neg q}(n) = a_{\neg q}(n-1)$.*

Proof. We prove both statements simultaneously, by induction on n. Since $a_{\neg q}(0) = a_{\neg q}(1) = \cdots = a_{\neg q}(q-1) = 1$, the statements hold for $n \leqslant q-1$ and we may suppose that $n \geqslant q$, and that the assertions hold for integers less than n.

Let us first suppose that $n = mq + r$ with $2 \leqslant r \leqslant q-1$. By the induction hypothesis, if $n-k \notin \{mq, mq+1\}$ for some $1 \leqslant k \leqslant q$ then $2s_{\neg q}(n-k) - a_{\neg q}(n-k) = a_{\neg q}(n-k) = s_{\neg q}(n-k)$. Also, by the induction hypothesis and Lemma 2.2,

$$2s_{\neg q}(mq+1) - a_{\neg q}(mq+1) + a_{\neg q}(mq) = 2s_{\neg q}(mq)$$

and

$$a_{\neg q}(mq+1) + 2s_{\neg q}(mq) - a_{\neg q}(mq) = 2s_{\neg q}(mq).$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

Therefore, independently of the parity of r and q, the recursion of Lemma 3.1 yields

$$n\ a_{\neg q}(n) = r\ s_{\neg q}(mq) + (n-r-1)s_{\neg q}(mq-q). \tag{3.3}$$

Comparing (3.3) with (2.5) in the proof of Lemma 2.2, we obtain $a_{\neg q}(n) = s_{\neg q}(n)$.

If $n = mq+1$ then the recursion of Lemma 3.1 yields

$$\begin{aligned}(mq+1)a_{\neg q}(mq+1) = a_{\neg q}(mq) + (q-2)s_{\neg q}(mq-q)\\ + (mq-q+1)X_{mq-q+1},\end{aligned} \tag{3.4}$$

with the expression X_{mq-q+1} defined in the statement of Lemma 3.1. The same recursion for the value mq yields

$$mq\ a_{\neg q}(mq) = (q-2)s_{\neg q}(mq-q) + Y_{mq-q+1} + (mq-q)X_{mq-q}, \tag{3.5}$$

where $Y_{mq-q+1} = a_{\neg q}(mq-q+1)$ if q is even and $Y_{mq-q+1} = 2s_{\neg q}(mq-q+1) - a_{\neg q}(mq-q+1)$ if q is odd. In any case, since $a_{\neg q}(mq-q+1) = a_{\neg q}(mq-q)$ by the induction hypothesis and $s_{\neg q}(mq-q+1) = s_{\neg q}(mq-q)$ by Lemma 2.2, we have $Y_{mq-q+1} = X_{mq-q}$. Therefore, taking the difference of (3.4) and (3.5) yields $(mq+1)a_{\neg q}(mq+1) - mq\ a_{\neg q}(mq) = a_{\neg q}(mq)$, which implies $a_{\neg q}(mq+1) = a_{\neg q}(mq)$. □

Theorem 3.3. *For all $q \geqslant 2$ and $n = qm + r \geqslant 2$, where $0 \leqslant r \leqslant q-1$,*

(a) $a_{\neg q}(n) = s_{\neg q}(n) + \delta_{\neg q}(n) = \prod_{\ell=1}^{\lfloor n/q \rfloor}\left(1 - \frac{1}{\ell q}\right) + \delta_{\neg q}(n)$, *where*

$$\delta_{\neg q}(n) = \begin{cases} (-1)^{q\lfloor n/q \rfloor} \prod_{\ell=1}^{\lfloor n/q \rfloor}\left(1 - \frac{q-1}{\ell q}\right) & \text{if } 0 \leqslant r \leqslant 1, \\ 0 & \text{if } 2 \leqslant r \leqslant q-1, \end{cases}$$

(b) $1 - \dfrac{1}{q-1} \leqslant \dfrac{a_{\neg q}(n)}{s_{\neg q}(n)} \leqslant 1 + \dfrac{1}{q-1}$;

(c) $|\delta_{\neg q}(n)| < (n/q)^{-1+1/q}$, *whence, for $n \geqslant q$,*

$$\begin{aligned}|a_{\neg q}(n) - c(q)n^{-1/q}| &< (n/q)^{-1+1/q} + 2c(q)n^{-1-1/q} \\ &\leqslant n^{-1+1/q}\left(q^{1-1/q} + 2c(q)q^{-2/q}\right).\end{aligned}$$

Thus, for $q \geqslant 3$, $a_{\neg q}(n) = s_{\neg q}(n) + O(n^{-1+1/q}) = (1+o(1))s_{\neg q}(n)$.

Proof. **(a)** For $2 \leqslant r \leqslant q-1$, the formula for $a_{\neg q}(n)$ follows immediately from Lemma 3.2(a) and Theorem 2.3(a). We also have $a_{\neg q}(mq+1) = a_{\neg q}(mq)$, so it is enough to find an expression for $a_{\neg q}(mq)$, for $m \geqslant 1$.

We define the numbers $d_q(m)$ as the solution of $a_{\neg q}(mq) = (1 + d_q(m))s_{\neg q}(mq)$. Since there are $(q-1)!$ cycles of length q in S_q, we have $s_{\neg q}(q) = (q! - (q-1)!)/q! = (q-1)/q$. If q is even then these q-cycles are odd permutations and so $a_{\neg q}(q) = 1$ and $a_{\neg q}(q)/s_{\neg q}(q) = 1 + 1/(q-1)$. If q is odd then these q-cycles are in A_q and so $a_{\neg q}(q) = (q!/2 - (q-1)!)/(q!/2) = (q-2)/q$ and $a_{\neg q}(q)/s_{\neg q}(q) = 1 - 1/(q-1)$. Therefore, for all q,

$$d_q(1) = (-1)^q \frac{1}{q-1}. \tag{3.6}$$

Our goal is to give a recursion for $d_q(m)$.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

Suppose first that q is even. Lemma 3.1 gives a recursive form for $a_{\neg q}(mq)$ which, using Lemmas 2.2 and 3.2 as in the proof of Lemma 3.2, can be written as

$$mq\, a_{\neg q}(mq) = (q-2)s_{\neg q}(mq-q) + a_{\neg q}(mq-q) + (mq-q)a_{\neg q}(mq-q). \tag{3.7}$$

Using

$$a_{\neg q}(mq) = (1+d_q(m))s_{\neg q}(mq) = (1+d_q(m))s_{\neg q}(mq-q)(1-1/qm)$$

and

$$a_{\neg q}(mq-q) = (1+d_q(m-1))s_{\neg q}(mq-q),$$

(3.7) simplifies to

$$d_q(m) = \frac{mq-q+1}{mq-1}d_q(m-1). \tag{3.8}$$

If q is odd then similarly

$$\begin{aligned} mq\, a_{\neg q}(mq) = (q-2)s_{\neg q}(mq-q) &+ \big(2s_{\neg q}(mq-q) - a_{\neg q}(mq-q)\big) \\ &+ (mq-q)\big(2s_{\neg q}(mq-q) - a_{\neg q}(mq-q)\big), \end{aligned} \tag{3.9}$$

which simplifies to

$$d_q(m) = -\frac{mq-q+1}{mq-1}d_q(m-1). \tag{3.10}$$

Hence, for all q,

$$d_q(m) = (-1)^q \frac{mq-q+1}{mq-1}d_q(m-1).$$

Combining with (3.6), we obtain

$$d_q(m) = (-1)^{qm}\prod_{\ell=1}^{m}\left(\frac{\ell q-q+1}{\ell q-1}\right), \tag{3.11}$$

which implies immediately the formula for $a_{\neg q}(n)$ stated in (a).

(b) If $2 \leqslant r \leqslant q-1$ then $a_{\neg q}(n)/s_{\neg q}(n) = 1$ by Lemma 3.2. If $0 \leqslant r \leqslant 1$ then, by (3.11),

$$\left|-1+\frac{a_{\neg q}(n)}{s_{\neg q}(n)}\right| = \prod_{\ell=1}^{m}\left(\frac{\ell q-q+1}{\ell q-1}\right) \leqslant \prod_{\ell=1}^{1}\left(\frac{\ell q-q+1}{\ell q-1}\right) = \frac{1}{q-1}.$$

(c) Now $\log|\delta_{\neg q}(n)| = \sum_{\ell=1}^{m}\log(1-(q-1)/\ell q)$, and each of these 'log' terms is negative. By (2.7),

$$\left|\log\left(1-\frac{q-1}{\ell q}\right)\right| > \frac{q-1}{\ell q},$$

for each $\ell = 1,\ldots,m$. Thus

$$\begin{aligned} |(\log|\delta_{\neg q}(n)|)| &> \frac{q-1}{q}\sum_{\ell=1}^{m}\frac{1}{\ell} \\ &> \frac{q-1}{q}\int_1^{m+1}\frac{dt}{t} = \frac{q-1}{q}\log(m+1). \end{aligned}$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

We therefore have $\log|\delta_{\neg q}(n)| < -(1-1/q)\log(m+1) = \log((m+1)^{-1+1/q})$, which implies the bound $|\delta_{\neg q}(n)| < (m+1)^{-1+1/q} < (n/q)^{-1+1/q}$ (since $n < (m+1)q$). Thus we have, for $n \geqslant q$, $|a_{\neg q}(n) - c(q)n^{-1/q}| \leqslant |\delta_{\neg q}(n)| + |s_{\neg q}(n) - c(q)n^{-1/q}|$ whence, by part (a), the bound just obtained on $|\delta_{\neg q}(n)|$, and Theorem 2.3, is less than $(n/q)^{-1+1/q} + 2c(q)n^{-1-1/q} \leqslant n^{-1+1/q}(q^{1-1/q} + 2c(q)q^{-2/q})$. Thus $a_{\neg q}(n) = c(q)n^{-1/q} + O(n^{-1+1/q})$, and the other forms for $a_{\neg q}(n)$ follow from Theorem 2.3. □

4. Bounds on the order of a permutation

Landau [20, p. 222] proved that the maximal order of an element of S_n is $e^{(1+o(1))(n\log n)^{1/2}}$. Erdős and Turán [11, 13] showed that most elements of S_n have a much smaller order, namely $n^{(1/2+o(1))\log n}$. Barbour and Tavaré in [3, Theorem 1.2] improved the error term in the Erdős–Turán result.

In this section we present a modification of the above mentioned theorem of Barbour and Tavaré [3, Theorem 1.2]. This new result gives a slightly weaker upper bound for the orders of 'most' permutations in A_n or S_n. However, the proportion of elements which have order larger than this upper bound is significantly smaller.

We are grateful to Andrew Barbour for providing the elegant proof below for Theorem 4.1 based on the arguments in [3]. In the next section we use Theorem 4.1 (with the parameters $c = 7$ and $k = 18$) to estimate the proportion of elements in A_n or S_n which have order at most $n^{18\log n}$ and have no cycle of length divisible by q for $q = 2$ and $q = 3$.

For a permutation in S_n let $C_i^{(n)}$ denote the number of its cycles of length i, for $i = 1, \ldots, n$ and set $C^{(n)} := (C_1^{(n)}, \ldots, C_n^{(n)})$. Also let $o_n := o_n(C^{(n)})$ denote the order of the permutation (so $o_n(C^{(n)}) = \operatorname{lcm}\{i \mid C_i^{(n)} \neq 0\}$).

Theorem 4.1. *For all constants $c > 0$ and positive integers n, there exists a constant $k = k(c) > 0$ such that the probability that a random permutation in S_n has order greater than $n^{k\log n}$ is less than n^{-c}. In particular, if $c \geqslant e^2 - 1$ then we may take $k = 2(c+2)$.*

Proof. The statement is equivalent to proving

$$P[\log o_n(C^{(n)}) \geqslant k\log^2 n] \leqslant n^{-c}.$$

The cases $n = 1, 2$ are evident. For $n \geq 3$, let $(Z_j,\ 1 \leqslant j \leqslant n)$ be independent Poisson random variables with expected value $E(Z_j) = 1/j$. Then the coupling inequality [3, Equation (2.1)] derived by Barbour and Tavaré [3, pp. 169–170] implies in particular that the distribution of $\log o_n(C^{(n)})$ is stochastically smaller than that of

$$\log n + \sum_{j=1}^{n} Z_j \log j,$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

from which it follows immediately that, for any $x > 0$,

$$P[\log o_n(C^{(n)}) \geqslant x] \leqslant P\left[\sum_{j=1}^{n} Z_j \log j \geqslant x - \log n\right] \leqslant P\left[\sum_{j=1}^{n} Z_j \geqslant \frac{x}{\log n} - 1\right]. \tag{4.1}$$

Since the Z_j are independent Poisson random variables, the following equation holds for any t,

$$E((e^t)^{\sum_{j=1}^{n} Z_j}) = \prod_{j=1}^{n} E(e^{tZ_j}),$$

and since Z_j is a Poisson random variable with mean $1/j$, for any $s > 0$ we have $E(s^{Z_j}) = e^{(s-1)/j}$ for each j. Thus, setting $h_n = \sum_{j=1}^{n} 1/j$, we have

$$E\left(\exp\left\{t\sum_{j=1}^{n} Z_j\right\}\right) = \prod_{j=1}^{n} e^{(e^t-1)/j} = e^{h_n(e^t-1)}$$

for each t. Note that $\log n < h_n < 1 + \log n$ and therefore, using the Bienaymé–Markov inequality, we have

$$P\left[\sum_{j=1}^{n} Z_j \geqslant y\right] \leqslant e^{-ty} E(e^{t\sum_{j=1}^{n} Z_j}) = e^{-ty} e^{h_n(e^t-1)}$$

for all $y, t > 0$. Taking $y = (s+1)h_n$ and $e^t = s + 1$ this gives

$$P\left[\sum_{j=1}^{n} Z_j \geqslant (s+1)(1+\log n)\right] \leqslant P\left[\sum_{j=1}^{n} Z_j \geqslant (s+1)h_n\right] \leqslant (s+1)^{-(s+1)h_n} e^{h_n s} \leqslant e^{-((s+1)\log(s+1)-s)h_n}$$

and since $h_n > \log n$ this is less than $n^{-((s+1)\log(s+1)-s)}$. Combining this with (4.1) and setting $c(s) := (s+1)\log(s+1) - s$ and $x = (1 + (s+1)(1+\log n))\log n$ then gives

$$P\left[\log o_n(C^{(n)}) \geqslant (1 + (s+1)(1+\log n))\log n\right] \leqslant P\left[\sum_{j=1}^{n} Z_j \geqslant (s+1)(1+\log n)\right] \leqslant n^{-c(s)}.$$

Since, for $n \geqslant 3$, we have $1+(s+1)(1+\log n) \leqslant 2(s+2)\log n$, it follows that $P[\log o_n(C^{(n)}) \geqslant 2(s+2)\log^2 n] \leqslant n^{-c(s)}$ for all $s > 0$. But since $c(s)$ can be made arbitrarily large by choice of s, the result is proved.

If $c \geqslant e^2 - 1$ then $(c+1)\log(c+1) - c > c$. Hence, for the value of s for which $c(s) = c$, we have $s < c$, since the function $f(x) = (x+1)\log(x+1) - x$ is strictly increasing for positive x. Thus $s + 2 < 2(c+2)$, and we can choose $k(c) = 2(c+2)$. □

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

5. Pre-transpositions and pre-3-cycles

A *pre-transposition* in S_n is an element $\sigma \in S_n$ of order $2f$, for some odd positive integer f, such that σ^f is a transposition. Similarly a *pre-3-cycle* is an element $\sigma \in S_n$ of order $3f$, where f is not divisible by 3, such that σ^f is a 3-cycle. In Section 6 we will describe some randomized algorithms for constructing transpositions and 3-cycles in finite symmetric and alternating groups, using pre-transpositions and pre-3-cycles, respectively. In this section we derive probabilistic results concerning the proportions of pre-transpositions and pre-3-cycles, and related classes of permutations, in S_n and A_n. These will be used to analyse the performance of the algorithms presented in Section 6.

First we consider the classes of permutations needed for constructing transpositions. The values of the constants $c(q)$, $q = 2, 4$, mentioned in Theorem 5.1 below, are given in Theorem 2.3. For $\sigma \in S_n$, $\operatorname{supp}\sigma$ denotes the subset of $\{1, \ldots, n\}$ of points i such that $i^\sigma \neq i$, and is called the *support* of σ.

Theorem 5.1.

(a) *The proportion* $p_{\mathrm{pre}}(n)$ *of pre-transpositions in* S_n *for* $n \geqslant 2$ *is*

$$p_{\mathrm{pre}}(n) = \frac{c(2)}{2} n^{-1/2} + O(n^{-3/2}) = (2\pi)^{-1/2} \cdot n^{-1/2} + O(n^{-3/2}),$$

and, for $n \geqslant 5$, *the proportion* $p_{\mathrm{pre}}^{\mathrm{small}}(n)$ *of pre-transpositions in* S_n *of order at most* $n^{18 \log n}$ *satisfies* $p_{\mathrm{pre}}^{\mathrm{small}}(n) > 0.318 n^{-1/2}$.

(b) *The proportion* $p_{2\,\mathrm{odd}}(n)$ *of elements of* S_n *of twice odd order is*

$$p_{2\,\mathrm{odd}}(n) = c(4) n^{-1/4} - c(2) n^{-1/2} + O(n^{-5/4}),$$

and, for $n \geqslant 5$, *the proportion* $p_{2\,\mathrm{odd}}^{\mathrm{small}}(n)$ *of elements of* S_n *of twice odd order and order at most* $n^{18 \log n}$ *satisfies* $0.175\, n^{-1/4} < p_{2\,\mathrm{odd}}^{\mathrm{small}}(n) < 1.616\, n^{-1/4}$.

(c) *For* $n \geqslant 5$ *the conditional probability* $p_{\mathrm{pre}/2\,\mathrm{odd}}^{\mathrm{small}}(n)$ *that an element of* S_n *is a pre-transposition, given that it has twice odd order at most* $n^{18 \log n}$, *is at least* $0.196\, n^{-1/4}$.

Proof. **(a)** A pre-transposition $\sigma \in S_n$ is of the form $\sigma = (i, j)\tau$, where $\{i, j\} \cap \operatorname{supp}\tau = \emptyset$, and τ has odd order. There are $\binom{n}{2}$ possibilities for choosing two points to form a 2-cycle, and for a given choice there are $(n-2)!\, s_{\neg 2}(n-2)$ elements τ of odd order on the remaining points. Hence $p_{\mathrm{pre}}(n) = s_{\neg 2}(n-2)/2$, and so by Theorem 2.3(c), $p_{\mathrm{pre}}(n) = c(2)(n-2)^{-1/2}/2 + O(n^{-3/2}) = c(2) n^{-1/2}/2 + O(n^{-3/2})$, as claimed. If $n \geqslant 5$, then by Theorem 2.3(a) and (b),

$$\begin{aligned} s_{\neg 2}(n-2)/2 &\geqslant s_{\neg 2}(n)/2 \geqslant c(2) n^{-1/2}(1 - n^{-1})/2 \\ &\geqslant c(2) n^{-1/2}(1 - 1/5)/2 > 0.319\, n^{-1/2}. \end{aligned}$$

Let 'pre' denote the event that a random permutation of S_n is a pre-transposition. For $n \geqslant 5$ the proportion of pre-transpositions in S_n of order at most $n^{18 \log n}$ can be estimated using this result and Theorem 4.1 with $c = 7$ as follows:

$$\begin{aligned} P\left[o(g) \leqslant n^{18 \log n} \text{ and } g \in \mathrm{pre}\right] &\geqslant p_{\mathrm{pre}}(n) - P\left[o(g) > n^{18 \log n}\right] \\ &\geqslant 0.319 n^{-1/2} - n^{-7} \geqslant 0.319 n^{-1/2} - 5^{-13/2} n^{-1/2} > 0.318 n^{-1/2}. \end{aligned}$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

(b) The subset of S_n of elements with no cycles of length divisible by 4 is the disjoint union of the subset of permutations of twice odd order, and the subset of elements of odd order. So $p_{2\,\mathrm{odd}}(n) = s_{\neg 4}(n) - s_{\neg 2}(n)$ and the asymptotic formula then follows from Theorem 2.3(c). If $n \geqslant 5$ then $p^{\mathrm{small}}_{2\,\mathrm{odd}}(n) \leqslant p_{2\,\mathrm{odd}}(n) < s_{\neg 4}(n) \leqslant c(4)n^{-1/4}(1 + 2/n) \leqslant c(4)n^{-1/4}(1 + 2/5) < 1.616\, n^{-1/4}$. For the lower bound, we have

$$\begin{aligned} p_{2\,\mathrm{odd}}(n) &\geqslant c(4)n^{-1/4}(1 - 1/n) - c(2)n^{-1/2}(1 + 2/n) \\ &\geqslant c(4)n^{-1/4}(1 - 1/5) - c(2)n^{-1/4}5^{-1/4}(1 + 2/5) > 0.176\, n^{-1/4}, \end{aligned}$$

and $p^{\mathrm{small}}_{2\,\mathrm{odd}}(n) \geqslant p_{2\,\mathrm{odd}}(n) - P\left[o(g) > n^{18\log n}\right] \geqslant 0.176\, n^{-1/4} - n^{-7} > 0.175\, n^{-1/4}$.

(c) By parts (a) and (b), $p^{\mathrm{small}}_{\mathrm{pre}/2\,\mathrm{odd}}(n) > 0.318\, n^{-1/2}/(1.616\, n^{-1/4}) > 0.196\, n^{-1/4}$. □

Now we derive analogous results for the proportions in A_n and S_n of pre-3-cycles, and elements of order $3f$, with f not divisible by 3. Recall that the values of the constants $c(3), c(9)$ are given in Theorem 2.3.

Theorem 5.2.

(a) *The proportions $p^A_{\mathrm{pre}\,3}(n)$, $p^S_{\mathrm{pre}\,3}(n)$ of pre-3-cycles in A_n and S_n, respectively, are*

$$p^A_{\mathrm{pre}\,3}(n) = \frac{c(3)}{3}n^{-1/3} + O(n^{-2/3}), \qquad p^S_{\mathrm{pre}\,3}(n) = \frac{c(3)}{3}n^{-1/3} + O(n^{-4/3}),$$

and, for $n \geqslant 5$, the proportion $p^{\mathrm{small}A}_{\mathrm{pre}\,3}(n)$, $p^{\mathrm{small}S}_{\mathrm{pre}\,3}(n)$ of pre-3-cycles of order at most $n^{18\log n}$ in A_n and S_n, respectively, satisfy

$$p^{\mathrm{small}A}_{\mathrm{pre}\,3}(n) > 0.140\, n^{-1/3} \quad \textit{and} \quad p^{\mathrm{small}S}_{\mathrm{pre}\,3}(n) > 0.282\, n^{-1/3}.$$

(b) *The proportions $p^A_{3f}(n)$, $p^S_{3f}(n)$ of elements of order $3f$, for some f not divisible by 3, in A_n and S_n, respectively, are given by $p^A_{3f}(n) = c(9)n^{-1/9} - c(3)n^{-1/3} + O(n^{-2/3})$, and $p^S_{3f}(n) = c(9)n^{-1/9} - c(3)n^{-1/3} + O(n^{-10/9})$. Moreover, for $n \geqslant 9$, the proportions $p^{\mathrm{small}A}_{3f}(n)$ and $p^{\mathrm{small}S}_{3f}(n)$ of elements of A_n and S_n, respectively, of order at most $n^{18\log n}$ and of the form $3f$ with f not divisible by 3, satisfy*

$$0.24\, n^{-1/9} < p^{\mathrm{small}S}_{3f}(n) < 1.45\, n^{-1/9} \quad \textit{and} \quad 0.19\, n^{-1/9} < p^{\mathrm{small}A}_{3f}(n) < 1.63\, n^{-1/9}.$$

(c) *For $n \geqslant 9$, the conditional probabilities $p^{\mathrm{small}A}_{\mathrm{pre}\,3/3f}(n), p^{\mathrm{small}S}_{\mathrm{pre}\,3/3f}(n)$ that an element of A_n or S_n, respectively, is a pre-3-cycle, given that it has order $3f \leqslant n^{18\log n}$ for some f not divisible by 3, satisfy*

$$p^{\mathrm{small}S}_{\mathrm{pre}\,3/3f}(n) > 0.194n^{-2/9} \quad \textit{and} \quad p^{\mathrm{small}A}_{\mathrm{pre}\,3/3f}(n) > 0.085n^{-2/9}.$$

Proof. **(a)** A pre-3-cycle $\sigma \in S_n$ is of the form $\sigma = (i, j, k)\tau$, where τ has order coprime to 3 and $\{i, j, k\} \cap \mathrm{supp}\,\tau = \emptyset$. There are $\binom{n}{3}$ choices for the three points i, j, k, and there are two 3-cycles with support $\{i, j, k\}$. For a given choice, there are then $(n-3)!s_{\neg 3}(n-3)$ permutations, and $(n-3)!a_{\neg 3}(n-3)/2$ even permutations τ of order coprime to 3 on the remaining points. Thus $p^S_{\mathrm{pre}\,3}(n) = s_{\neg 3}(n-3)/3$, and $p^A_{\mathrm{pre}\,3}(n) = a_{\neg 3}(n-3)/3$, and the asymptotic formulas now follow from Theorems 2.3 and 3.3.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

If $n \geqslant 5$, then

$$p^S_{\mathrm{pre}\,3}(n) = s_{\neg 3}(n-3)/3 \geqslant s_{\neg 3}(n)/3 \geqslant c(3)n^{-1/3}(1-1/n)/3$$
$$\geqslant (4c(3)/15)n^{-1/3} > 0.283\, n^{-1/3}.$$

Also, using Theorem 3.3(b), $p^A_{\mathrm{pre}\,3}(n) = a_{\neg 3}(n-3)/3 \geqslant (1/2)s_{\neg 3}(n-3)/3$, which for $n \geqslant 5$ yields $p^A_{\mathrm{pre}\,3}(n) > 0.141\, n^{-1/3}$. Moreover, applying Theorem 4.1 with $c = 7$ yields

$$p^{\mathrm{small}A}_{\mathrm{pre}\,3}(n) \geqslant p^A_{\mathrm{pre}\,3}(n) - n^{-7} > 0.140\, n^{-1/3}$$

and

$$p^{\mathrm{small}S}_{\mathrm{pre}\,3}(n) \geqslant p^S_{\mathrm{pre}\,3}(n) - n^{-7} > 0.282\, n^{-1/3}.$$

(b) Let $G = S_n$ or A_n. Then the subset of G of elements with no cycles of length divisible by 9 is the disjoint union of the subset of G consisting of permutations with order $3f$, f not divisible by 3, and the subset of G of permutations with order coprime to 3. So $p^S_{3f}(n) = s_{\neg 9}(n) - s_{\neg 3}(n)$ and $p^A_{3f}(n) = a_{\neg 9}(n) - a_{\neg 3}(n)$. The asymptotic formulas now follow from Theorems 2.3 and 3.3. If $n \geqslant 9$, then

$$p^S_{3f}(n) < s_{\neg 9}(n) \leqslant c(9)n^{-1/9}\left(1+\frac{2}{n}\right) \leqslant \frac{11}{9}c(9)n^{-1/9} < 1.45\, n^{-1/9}$$

and

$$p^S_{3f}(n) > c(9)n^{-1/9}\left(1-\frac{1}{n}\right) - c(3)n^{-1/3}\left(1+\frac{2}{n}\right)$$
$$\geqslant c(9)n^{-1/9}\left(1-\frac{1}{9}\right) - c(3)n^{-1/9}\,9^{-2/9}\left(1+\frac{2}{9}\right) > 0.25\, n^{-1/9}.$$

For $n \geqslant 9$ we also have

$$p^A_{3f}(n) = a_{\neg 9}(n) - a_{\neg 3}(n) < a_{\neg 9}(n) \leqslant s_{\neg 9}(n)\left(1+\frac{1}{8}\right)$$
$$\leqslant c(9)\left(1+\frac{2}{9}\right)\left(1+\frac{1}{8}\right)n^{-1/9} < 1.63\, n^{-1/9}.$$

For the lower bound we get for $n \geqslant 30$

$$p^A_{3f}(n) = a_{\neg 9}(n) - a_{\neg 3}(n) > s_{\neg 9}(n)\left(1-\frac{1}{8}\right) - s_{\neg 3}(n)\left(1+\frac{1}{2}\right)$$
$$\geqslant n^{-1/9}\left(c(9)\left(1-\frac{1}{n}\right)\frac{7}{8} - c(3)\left(1+\frac{2}{n}\right)\frac{3}{2}\,n^{-2/9}\right) > 0.2\, n^{-1/9},$$

while we find that this is also true for $9 \leqslant n < 30$ by exact computation using the formula for $a_{\neg q}(n)$ given in Theorem 3.3(a). Finally, by Theorem 4.1,

$$p^{\mathrm{small}A}_{3f}(n) \geqslant p^A_{3f}(n) - n^{-7} > 0.19\, n^{-1/9} \quad \text{and} \quad p^{\mathrm{small}S}_{3f}(n) \geqslant p^S_{3f}(n) - n^{-7} > 0.24\, n^{-1/9}.$$

(c) By parts (a) and (b),

$$p^{\mathrm{small}S}_{\mathrm{pre}\,3/3f}(n) > 0.282\, n^{-1/3}/(1.45\, n^{-1/9}) > 0.194 n^{-2/9}$$

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

and

$$p^{\text{small}A}_{\text{pre } 3/3f}(n) > 0.14\, n^{-1/3}/(1.63\, n^{-1/9}) > 0.085 n^{-2/9}. \qquad \square$$

6. Constructing transpositions and 3-cycles

A *black-box group* G is a group whose elements are encoded as 0–1 strings of uniform length N, and the group operations are performed by an oracle (the 'black box'). Given strings representing $g, h \in G$, the black box can compute strings representing gh and g^{-1}, and decide whether $g = h$. Standard examples of black-box groups are permutation and matrix groups.

In [4] procedures were given for constructing transpositions and 3-cycles in black-box groups $G \cong S_n$ or A_n. These algorithms and the procedures given in this section inspired the design in [6] of recognition algorithms for matrix groups isomorphic to A_n or S_n in their natural actions on deleted permutation modules (of dimension $n-1$ or $n-2$) over finite fields. These are the smallest-dimensional faithful absolutely irreducible matrix representations of such groups.

In this section, we describe algorithms to construct transpositions and 3-cycles in groups G isomorphic to S_n or A_n, supposing that G is given as a black-box group equipped with oracles for determining element orders, and for testing for transpositions and 3-cycles. Efficient oracles are available for these tasks, for example in the deleted permutation module setting mentioned above [6, 10].

First we consider the problem of constructing a transposition. A brief description of the procedure is given below. The procedure succeeds with probability at least $1 - \varepsilon$, where the probability ε of failure may be specified ahead of time.

The time required for the algorithm is given in terms of parameters $\mu, \xi, \rho, \tau, \varepsilon$, and n, where μ is an upper bound on the time required for each group operation in G; ξ is an upper bound on the time requirement per element for the construction of independent, (nearly) uniformly distributed random elements of G; ρ is the time requirement for a call to the order oracle; τ is the time requirement for testing whether an element of G is a transposition, that is, for a call to the transposition oracle; ε is the desired error probability; and n is the degree of the permutation group S_n which is isomorphic to G. The parameters ξ, ρ and τ can be expressed as functions of μ and n; the actual expressions depend on the representation of the black box-group. For details, we refer to [5] and [6].

For the analysis of the algorithm, we need *Chernoff's bound* [23, Theorem 1.3.13]. Let $Y_1, \ldots, Y_t$ be not necessarily independent, 0–1 valued random variables with the property that, for some r and each i, the conditional probability $P[Y_i = 1 \mid Y_1 = x_1, \ldots, Y_{i-1} = x_{i-1}] \geqslant r$ for all 0–1 sequences $(x_1, \ldots, x_{i-1})$. Then, whenever $0 < \delta < 1$,

$$P\left[\sum_{i=1}^{t} Y_i \leqslant (1-\delta)rt\right] \leqslant e^{-\delta^2 rt/2}. \tag{6.1}$$

Procedure 6.1. (FINDTRANSPOSITION) *Given a black-box group $G \cong S_n$ which is equipped with an order oracle and a transposition oracle, and given a positive number ε, this procedure*

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

constructs a transposition with probability at least $1-\varepsilon$ *at a cost* $O\big(\log(\varepsilon^{-1})(n^{1/2}(\xi+\rho)+n^{1/4}\log^2 n\mu+n^{1/4}\tau)\big)$.

Set $i := 0$ *and* $j := 0$.
Set $i_M := \lceil 4\cdot 196^{-1}\cdot 0.175^{-1}\cdot n^{1/2}\log((\varepsilon/2)^{-1})\rceil$;
Set $j_M := \lceil 0.196^{-1}\cdot n^{1/4}\log((\varepsilon/2)^{-1})\rceil$;
Set $o_M := n^{18\log n}$;
while $i < i_M$ **and** $j < j_M$ **do**
    select an independent random element $g \in G$;
    set $i := i+1$;
    if $o(g) = 2f$ *with* f *odd and* $o(g) \leqslant o_M$ **then**
        compute $h := g^f$;
        if h *is a transposition* **then**
            return h;
        else
            set $j := j+1$;
        fi;
    fi;
done;
if *no transposition has been found* **then**
    return *failure*;
fi;

Proof. Let the Y_i be 0–1 valued random variables with $Y_i = 1$ if and only if the ith random element has order $2f$ with f odd and $2f < n^{18\log n}$. By Theorem 5.1(b), $P[Y_i = 1] > 0.175\, n^{-1/4}$. Choose $r = 0.175\, n^{-1/4}$, $\delta = 3/4$, and $t = \lceil 4\cdot 0.175^{-1}\cdot 0.196^{-1}n^{1/2}\log(\varepsilon/2)^{-1}\rceil$. Then, by Chernoff's bound (6.1), we obtain

$$P\left[\sum_{i=1}^{t} Y_i \leqslant 0.196^{-1}n^{1/4}\log(\varepsilon/2)^{-1}\right] < e^{-(9/8)\cdot 0.196^{-1}n^{1/4}\log(\varepsilon/2)^{-1}} < \varepsilon/2,$$

which means that, with probability greater than $1-\varepsilon/2$, among t independent random elements of G we find at least $0.196^{-1}n^{1/4}\log((\varepsilon/2)^{-1})$ which have twice odd order at most $n^{18\log n}$. By Theorem 5.1(c), the probability that among $\lceil 0.196^{-1}n^{1/4}\log(\varepsilon/2)^{-1}\rceil$ elements of order $2f$ we do not find a pre-transposition is less than $\varepsilon/2$. Hence the procedure succeeds with probability at least $1-\varepsilon$.

Computing an element h costs at most $O(\mu\log f) = O(\mu\log^2 n)$. It follows that the cost is as stated. □

The procedure for constructing a 3-cycle is analogous to this. We state the result but omit the proof. We assume that G possesses an oracle which tests whether an element of G is a 3-cycle, and denote by τ_3 the time requirement for a call to this 3-cycle oracle.

Procedure 6.2. (FIND3CYCLE) *Given a black-box group* $G \cong S_n$ *or* A_n *which is equipped with an order oracle and a 3-cycle oracle, and given a positive number* ε, *the procedure*

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

constructs a 3*-cycle with probability at least* $1 - \varepsilon$ *at a cost of* $O\big(\log(\varepsilon^{-1})(n^{1/3}(\xi + \rho) + n^{2/9}\log^2 n\mu + n^{2/9}\tau_3)\big)$. □

Acknowledgements

We thank Peter Neumann, Horst Niemeyer, Akshay Venkatesh, Adrian Baddeley, and Keith Conrad for helpful discussions at various stages of our work. We also thank an anonymous referee for bringing to our attention the result of Barbour and Tavaré discussed in Section 4 and Andrew Barbour for the proof of Theorem 4.1.

References

[1] Apostol, T. M. (1962) *Calculus* II. Blaisdell Publishing Company, New York/London.
[2] Babai, L. and Szemerédi, E. (1984) On the complexity of matrix group problems, I. In *Proc. 25th IEEE Sympos. Foundations Comp. Sci.*, pp. 229–240.
[3] Barbour, A. D. and Tavaré, S. (1994) A rate for the Erdős–Turán law. *Combin. Probab. Comput.* **3** 167–176.
[4] Beals, R., Leedham-Green, C. R., Niemeyer, A. C., Praeger, C. E. and Seress, Á. A black-box algorithm for recognizing finite symmetric and alternating groups, I. *Trans. Amer. Math. Soc.* To appear.
[5] Beals, R., Leedham-Green, C. R., Niemeyer, A. C., Praeger, C. E. and Seress, Á. (2002) A black-box algorithm for recognizing finite symmetric and alternating groups, II. Preprint.
[6] Beals, R., Leedham-Green, C. R., Niemeyer, A. C., Praeger, C. E. and Seress, Á. (2002) Constructive recognition of finite alternating and symmetric groups acting as matrix groups on their natural permutation modules. Preprint.
[7] Best, M. R. (1970) The distribution of some variables on symmetric groups. *Nederl. Akad. Wetensch. Proc. Ser. A* **73** = *Indag. Math.* **32** 385–402.
[8] Bovey, J. D. (1980) An approximate probability distribution for the order of elements of the symmetric group. *Bull. London Math. Soc.* **12** 41–46.
[9] Bratus, S. and Pak, I. (2000) Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's Conjecture. *J. Symbolic Comput.* **29** 33–57.
[10] Celler, F. and Leedham-Green, C. R. (1997) Calculating the order of an invertible matrix. In *DIMACS 1995*, Vol. 28 of *Amer. Math. Soc. DIMACS Series*, pp. 55–60.
[11] Erdős, P. and Turán, P. (1965) On some problems of a statistical group-theory, I. *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **4** 175–186.
[12] Erdős, P. and Turán, P. (1967) On some problems of a statistical group-theory, II. *Acta Math. Acad. Sci. Hungar.* **18** 151–163.
[13] Erdős, P. and Turán, P. (1967) On some problems of a statistical group-theory, III. *Acta Math. Acad. Sci. Hungar.* **18** 309–320.
[14] Erdős, P. and Turán, P. (1968) On some problems of a statistical group-theory, IV. *Acta Math. Acad. Sci. Hungar.* **19** 413–435.
[15] Erdős, P. and Turán, P. (1971) On some problems of a statistical group-theory, V. *Period Math. Hungar.* **1** 5–13.
[16] Erdős, P. and Turán, P. (1970) On some problems of a statistical group-theory, VI. *J. Indian Math. Soc.* **34** 175–192.
[17] Erdős, P. and Turán, P. (1972) On some problems of a statistical group-theory, VII. *Period Math. Hungar.* **2** 149–163.
[18] Feller, W. (1968) *An Introduction to Probability Theory and its Applications*, Vol. 1. Wiley, New York, 3rd edn.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press

[19] Goh, W. M. Y. and Schmutz, E. (1991) The expected order of a random permutation. *Bull. London Math. Soc.* **23** 34–42.
[20] Landau, E. (1909) *Handbuch der Lehre vor der Verteilung der Primzahlen*, Teubner, Leipzig.
[21] Nicolas, J.-L. (1985) Distribution statistique de l'ordre d'un élément du groupe symmétrique. *Acta Math. Hungar.* **45** 69–84.
[22] Stromberg, K. R. (1981) *An Introduction to Classical Real Analysis*, Wadsworth, Belmont, CA.
[23] Stroock, D. W. (1993) *Probability Theory: An Analytic View*, Cambridge University Press.
[24] Szalay, M. and Turán, P. (1977) On some problems of the statistical theory of partitions with application to characters of the symmetric group, I. *Acta Math. Acad. Sci. Hungar.* **29** 361–379.
[25] Szalay, M. and Turán, P. (1978) On some problems of the statistical theory of partitions with application to characters of the symmetric group, III. *Acta Math. Acad. Sci. Hungar.* **32** 129–155.

https://doi.org/10.1017/S0963548302005217 Published online by Cambridge University Press