# THE PROBABILITY OF GENERATING THE SYMMETRIC GROUP 

SEAN EBERHARD AND STEFAN-CHRISTOPH VIRCHOW


#### Abstract

We consider the probability $p\left(S_{n}\right)$ that a pair of random permutations generates either the alternating group $A_{n}$ or the symmetric group $S_{n}$. Dixon (1969) proved that $p\left(S_{n}\right)$ approaches 1 as $n \rightarrow \infty$ and conjectured that $p\left(S_{n}\right)=1-1 / n+o(1 / n)$. This conjecture was verified by Babai (1989), using the Classification of Finite Simple Groups. We give an elementary proof of this result; specifically we show that $p\left(S_{n}\right)=1-1 / n+\mathcal{O}\left(n^{-2+\epsilon}\right)$. Our proof is based on character theory and character estimates, including recent work by Schlage-Puchta (2012).


## 1. Introduction

Let $G=A_{n}$ or $G=S_{n}$. We consider the probability

$$
p(G):=\frac{\#\left\{(\pi, \sigma) \in G \times G:\langle\pi, \sigma\rangle \geqslant A_{n}\right\}}{|G|^{2}}
$$

of ordered pairs $(\pi, \sigma) \in G \times G$ generating either the alternating group $A_{n}$ or the symmetric group $S_{n}$.
E. Netto [16, p.90] conjectured that almost all pairs of elements from $S_{n}$ will generate either $A_{n}$ or $S_{n}$. J. D. Dixon [6] was the first to prove Netto's conjecture. More precisely, he established that

$$
p\left(S_{n}\right)>1-\frac{2}{(\log \log n)^{2}}
$$

for all sufficiently large $n$. Dixon conjectured that the term $2 /(\log \log n)^{2}$ can be replaced by one of order $1 / n$. J. Bovey and A. Williamson [3] improved Dixon's estimate to

$$
p\left(S_{n}\right)>1-\exp (-\sqrt{\log n})
$$

This was subsequently amended by Bovey [2] to

$$
p\left(S_{n}\right)>1-n^{-1+o(1)}
$$

Finally, L. Babai [1] proved Dixon's conjecture and showed that

$$
p\left(S_{n}\right)=1-\frac{1}{n}+\mathcal{O}\left(n^{-2}\right)
$$

for all sufficiently large $n$.
In 2005, Dixon [5] established an even better asymptotic formula for $p\left(S_{n}\right)$ and for $p\left(A_{n}\right)$. For $m \in \mathbb{N}$ the asymptotic formula is

$$
p\left(S_{n}\right)=1+\frac{c_{1}}{n}+\frac{c_{2}}{n^{2}}+\ldots+\frac{c_{m}}{n^{m}}+\mathcal{O}\left(n^{-(m+1)}\right)
$$

where the coefficients $c_{m}$ are effectively computable. The same expansion holds for $p\left(A_{n}\right)$. The expansion begins

$$
p\left(S_{n}\right)=1-\frac{1}{n}-\frac{1}{n^{2}}-\frac{4}{n^{3}}-\frac{23}{n^{4}}-\frac{171}{n^{5}}-\frac{1542}{n^{6}}+\mathcal{O}\left(n^{-7}\right)
$$

See [20] for more terms.
Babai's proof of Dixon's conjecture and Dixon's preceding asymptotic formulas for $p\left(S_{n}\right)$ and $p\left(A_{n}\right)$ rest on consequences of the Classification of Finite Simple Groups (CFSG). Babai points out [1, Remark 1] that it would be desirable to find an elementary proof of Dixon's conjecture. Our aim is to give such an elementary proof. Our methods are based on character estimates and recent work by J.-C. Schalge-Puchta [19] and do not need the Classification of Finite Simple Groups. Our main results are

Theorem 1.1. Let $\epsilon>0$. Then we have

$$
p\left(S_{n}\right)=1-\frac{1}{n}+\mathcal{O}\left(n^{-2+\epsilon}\right)
$$

for all sufficiently large $n$.
Theorem 1.2. Let $\epsilon>0$. Then we get

$$
p\left(A_{n}\right)=1-\frac{1}{n}+\mathcal{O}\left(n^{-2+\epsilon}\right)
$$

for all sufficiently large $n$.
The main challenge in proving these Theorems is bounding the probability that a pair of random permutations generates a primitive subgroup other than $A_{n}$ or $S_{n}$. In [5] Dixon gave an asymptotic series for the proportion of pairs generating a transitive subgroup, and in [6] he proved that the proportion of pairs generating a transitive, imprimitive subgroup is $\leqslant n 2^{-n / 4}$, so all that is left is to bound

$$
P_{2}(n)=P\left(\left\{(\pi, \sigma) \in S_{n}^{2}: \pi, \sigma \in H \text { for some primitive } H \ngtr A_{n}\right\}\right),
$$

where $P$ denotes the uniform distribution on $S_{n} \times S_{n}$. Using CFSG, Babai 11 proved that $P_{2}(n) \leqslant n^{\sqrt{n}} / n$ !. Without CFSG, Bovey [2] proved that $P_{2}(n) \leqslant n^{-1+o(1)}$. We will improve this to $P_{2}(n) \leqslant n^{-2+o(1)}$ : once we have this then Theorems 1.1 and 1.2 follow from the above mentioned results and [5, Theorem 2].
Theorem 1.3. $P_{2}(n) \leqslant n^{-2+o(1)}$ as $n \rightarrow \infty$.
Let us briefly outline the proof. The main insight, borrowed from SchlagePuchta [19, is that if $\pi$ and $\sigma$ are random then the $N$ elements $\pi, \pi \sigma, \ldots, \pi \sigma^{N-1}$ are approximately pairwise independent. Thus we can use the second moment method to show that there is some $i$ such that $\pi \sigma^{i} \in \mathfrak{C}$, where

$$
\mathfrak{C}=\left\{\pi \in S_{n}: \exists p \in \Pi_{n} \text { such that } \pi \text { contains a } p \text {-cycle }\right\}
$$

and $\Pi_{n}$ is the set of all primes $p$ in the range $n / 2<p<3 n / 5$. Some power of $\pi \sigma^{i}$ is then a $p$-cycle, and we can apply the following classical result of C. Jordan (see 7. Theorem 3.3E] or [21, Theorem 13.9]).

Lemma 1.4. Let $H$ be a primitive subgroup of $S_{n}$. Suppose that $H$ contains at least one permutation which is a p-cycle for a prime $p \leqslant n-3$. Then either $H=S_{n}$ or $H=A_{n}$.

Additionally, as something of technical trick, we will use the concept of minimal degree. Recall that the minimal degree $m(H)$ of a non-trivial subgroup $H \leqslant S_{n}$ is the minimal number of points moved by a non-identity element of $H$. The following bound is due to Babai (see [7, Theorem 5.3A and Theorem 5.4A]).

Lemma 1.5. Let $H<S_{n}$ be a primitive permutation group not containing $A_{n}$. Then $m(H)>\sqrt{n} / 2$.

This Lemma allows us to restrict $\sigma$ to the set

$$
\mathfrak{M}=\left\{\sigma \in S_{n}: m(\langle\sigma\rangle)>\sqrt{n} / 2\right\},
$$

which slightly boosts the approximate pairwise independence of $\pi, \pi \sigma, \ldots, \pi \sigma^{N-1}$. (A bound of the form $m(H)>c \sqrt{n} / \log n$ due to Jordan would also suffice for us.) To bound the variance in the second moment method we use character theory, and thus the proof comes down to a certain bound in terms of characters. Finally, we apply a character bound due to Müller and Schlage-Puchta [14] to conclude.

We can use basically the same method to bound

$$
P_{3}(n)=P\left(\left\{(\pi, \sigma, \tau) \in S_{n}^{3}: \pi, \sigma, \tau \in H \text { for some primitive } H \ngtr A_{n}\right\}\right),
$$

and in this case we have significantly more leverage as we can consider the collection of all words of the form $\pi w(\sigma, \tau)$ with $w$ a short word in two letters. Again we have approximate pairwise independence, so again we can use the second moment method. This idea leads to the following bound.

Theorem 1.6. $P_{3}(n) \leqslant \exp \left(-c n^{1 / 3}\right)$ as $n \rightarrow \infty$.
By combining this with [5, Section 4] we have

$$
P\left(\langle\pi, \sigma, \tau\rangle \geqslant A_{n}\right)=1-\frac{1}{n^{2}}-\frac{3}{n^{4}}-\frac{6}{n^{5}}+\mathcal{O}\left(n^{-6}\right)
$$

(and more terms can be mechanically computed).
Finally, we should mention

$$
P_{1}(n)=P\left(\left\{\pi \in S_{n}: \pi \in H \text { for some primitive } H \ngtr A_{n}\right\}\right) .
$$

On CFSG it is known that $P_{1}(n) \leqslant n^{-1+o(1)}$ (see [8, Theorem 1.3]), and this is the best possible bound which depends only on the crude size of $n$. The best CFSG-free bound is still $P_{1}(n) \leqslant|\mathfrak{M}| / n!=n^{-1 / 2+o(1)}$ due to Bovey [2].

## 2. Some character theory

In this section we review some results from character theory which are essential for our proof. We denote by $\operatorname{Irr}\left(S_{n}\right)$ the set of irreducible characters of $S_{n}$. For a conjugacy class $C$ of $S_{n}$ and $\chi \in \operatorname{Irr}\left(S_{n}\right)$ we write $\chi(C)$ to denote $\chi(\pi)$ for $\pi \in C$. We write $\langle\cdot, \cdot\rangle$ for the usual inner product on the space $\mathbb{C}^{S_{n}}$, i.e.,

$$
\langle f, g\rangle=\frac{1}{n!} \sum_{\pi \in S_{n}} f(\pi) \overline{g(\pi)}
$$

Lemma 2.1. Let $C_{1}$ and $C_{2}$ be conjugacy classes of $S_{n}$ and let $\tau \in S_{n}$. Then

$$
\#\left\{(x, y) \in C_{1} \times C_{2}: x y=\tau\right\}=\frac{\left|C_{1}\right|\left|C_{2}\right|}{n!} \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)} \frac{\chi\left(C_{1}\right) \chi\left(C_{2}\right) \chi\left(\tau^{-1}\right)}{\chi(1)}
$$

Thus if $C_{1}, C_{2}$, and $C_{3}$ are conjugation-invariant subsets of $S_{n}$ we have

$$
\#\left\{(x, y) \in C_{1} \times C_{2}: x y \in C_{3}\right\}=n!^{2} \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)} \frac{\left\langle\chi, \mathbb{1}_{C_{1}}\right\rangle\left\langle\chi, \mathbb{1}_{C_{2}}\right\rangle\left\langle\chi, \mathbb{1}_{C_{3}}\right\rangle}{\chi(1)}
$$

Proof. For the first equation, see [4, Proposition 9.33] or [12, Theorem 6.3.1]. The second equation follows from partitioning $C_{1}$ and $C_{2}$ into conjugacy classes and adding.

Recall that the irreducible characters of $S_{n}$ are explicitly parameterized by partitions of $n$, or sequences $\lambda=\left(\lambda_{1}, \lambda_{2}, \ldots, \lambda_{l}\right)$, where $\lambda_{1} \geqslant \cdots \geqslant \lambda_{l}$ are positive integers such that $\lambda_{1}+\cdots+\lambda_{l}=n$. We write $\lambda \vdash n$ to indicate that $\lambda$ is a partition of $n$, and we write $\chi^{\lambda}$ for the irreducible character of $S_{n}$ corresponding to $\lambda$. The Ferrers diagram of $\lambda$ is an array of $n$ boxes having $l$ left-justified rows with row $i$ containing $\lambda_{i}$ boxes for $1 \leqslant i \leqslant l$. We write $(i, j) \in \lambda$ to indicate that $(i, j)$ is a box in row $i$ and column $j$ in the Ferrers diagram of $\lambda$.

We shall apply the Murnaghan-Nakayama rule.
Definition 2.2. Let $\lambda \vdash n$ be a partition. $A$ rim hook $h$ is an edgewise connected part of the Ferrers diagram of $\lambda$, obtained by starting from a box at the right end of a row and at each step moving downwards or leftwards only, which can be removed to leave a proper Ferrers diagram denoted by $\lambda \backslash h$. An r-rim hook is a rim hook containing r boxes.
The leg length of a rim hook $h$ is

$$
l l(h):=(\text { the number of rows of } h)-1 .
$$

Let $\pi \in S_{n}$ be a permutation with cycle type $\left(1^{\alpha_{1}}, \ldots, q^{\alpha_{q}}, \ldots, n^{\alpha_{n}}\right)$ and $\alpha_{q} \geqslant 1$. Denote $\pi \backslash q \in S_{n-q}$ a permutation with cycle type $\left(1^{\alpha_{1}}, \ldots, q^{\alpha_{q}-1}, \ldots,(n-q)^{\alpha_{n-q}}\right)$.

Lemma 2.3 (Murnaghan-Nakayama Rule). Let $\lambda \vdash n$ be a partition. Suppose that $\pi \in S_{n}$ is a permutation which contains a q-cycle. Then we have

$$
\chi^{\lambda}(\pi)=\sum_{\substack{h \\ \text { q-rim hook } \\ \text { of } \lambda}}(-1)^{l l(h)} \chi^{\lambda \backslash h}(\pi \backslash q) .
$$

Proof. See [15, §9] or [18, Theorem 4.10.2].
The dimension $\chi^{\lambda}(1)$ of the irreducible representation associated with $\lambda$ can be computed via the hook formula.

Definition 2.4. Let $\lambda \vdash n$ be a partition. The hook of $(i, j) \in \lambda$ is

$$
H_{i, j}(\lambda):=\left\{\left(i, j^{\prime}\right) \in \lambda: j^{\prime} \geqslant j\right\} \cup\left\{\left(i^{\prime}, j\right) \in \lambda: i^{\prime} \geqslant i\right\} .
$$

Lemma 2.5 (Hook Formula). Let $\lambda \vdash n$ be a partition. Then

$$
\chi^{\lambda}(1)=\frac{n!}{\prod_{(i, j) \in \lambda}\left|H_{i, j}(\lambda)\right|}
$$

Proof. See [10, Theorem 1] or [18, Theorem 3.10.2].
We combine the Murnaghan-Nakayama rule and hook formula to show that $\chi(1)$ is exponentially large whenever $\chi$ is nontrivial and $\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle \neq 0$.

Note that $\mathfrak{C}$ is the union of conjugacy classes from $S_{n}$, since a conjugacy class consists of all permutations with the same cycle type. For fixed $p \in \Pi_{n} \operatorname{let} C_{1}, \ldots, C_{s}$ denote all conjugacy classes of $\mathfrak{C}$ which contain a $p$-cycle. By removing a $p$-cycle from $C_{i}$ we obtain a conjugacy class $C_{i} \backslash p$ from $S_{n-p}$. Apparently, we have $S_{n-p}=$ $\dot{U}_{i=1, \ldots s} C_{i} \backslash p$. In addition, computing the cardinality of $C_{i}$ and $C_{i} \backslash p$ (see [18, Formula (1.2)]) we obtain

$$
\left|C_{i}\right|=\frac{n!}{(n-p)!p}\left|C_{i} \backslash p\right| .
$$

Let $\lambda \vdash n, \lambda \neq(n)$. We now apply the Murnaghan-Nakayama rule (Lemma 2.3):

$$
\begin{aligned}
\sum_{1 \leqslant i \leqslant s}\left|C_{i}\right| \chi^{\lambda}\left(C_{i}\right) & =\sum_{1 \leqslant i \leqslant s} \frac{n!}{(n-p)!p}\left|C_{i} \backslash p\right| \sum_{\substack{h \\
p \text {-rim hook } \\
\text { of } \lambda}}(-1)^{l l(h)} \chi^{\lambda \backslash h}\left(C_{i} \backslash p\right) \\
& =\sum_{\substack{h \\
p \text {-rim hook } \\
\text { of } \lambda}}(-1)^{l l(h)} \cdot \frac{n!}{p} \cdot\left\langle\chi^{(n-p)}, \chi^{\lambda \backslash h}\right\rangle \\
& = \begin{cases}(-1)^{l l(h)} \frac{n!}{p}, & \text { if } \exists p \text {-rim hook } h \text { of } \lambda \text { with } \lambda \backslash h=(n-p), \\
0, & \text { otherwise. }\end{cases}
\end{aligned}
$$

Thus we can have $\left\langle\chi^{\lambda}, \mathbb{1}_{\mathfrak{C}}\right\rangle \neq 0$ only if $\lambda \in \Lambda_{n, p}$ for some $p \in \Pi_{n}$, where

$$
\Lambda_{n, p}=\{\lambda \vdash n: \lambda \neq(n) \text { and } \exists p \text {-rim hook } h \text { such that } \lambda \backslash h=(n-p)\} .
$$

Lemma 2.6. Let $n$ be sufficiently large. If $p \in \Pi_{n}$ and $\lambda \in \Lambda_{n, p}$ then

$$
\chi^{\lambda}(1) \geqslant \exp (n / 4)
$$

Proof. First, we investigate the set $\Lambda_{n, p}$. We claim the following: Let $p \in \Pi_{n}$ and $\lambda \in \Lambda_{n, p}$. Then we have $\lambda \in \Lambda_{n, p}$ if and only if $\lambda=\left(\lambda_{1}, \lambda_{2}, 1^{n-\lambda_{1}-\lambda_{2}}\right)$, where either (a) $\lambda_{1}=n-p$ and $1 \leqslant \lambda_{2} \leqslant n-p$, or (b) $n-p<\lambda_{1} \leqslant p-1$ and $\lambda_{2}=n-p+1$. (See Figure 1.)

You can see this as follows: Let $\lambda \in \Lambda_{n, p}$. Then the Ferrers diagram of $\lambda$ has a block of $n-p$ boxes in the first row and around this block there is a $p$-rim hook $h$. If the rim hook $h$ does not contain a box from the first row of $\lambda$, then $\lambda_{1}=n-p$ and $1 \leqslant \lambda_{2} \leqslant n-p$, i.e., (a) is satisfied. If $h$ contains a box from the first row, then since $\lambda \neq(n)$ it follows immediately that $n-p<\lambda_{1}$ and $\lambda_{2}=n-p+1$. As $h$ is a $p$-rim hook, we also have $\lambda_{1} \leqslant p-1$. So (b) is fulfilled. Conversely, if $\lambda=\left(\lambda_{1}, \lambda_{2}, 1^{n-\lambda_{1}-\lambda_{2}}\right)$ such that (a) or (b) is satisfied, then there obviously exists a $p$-rim hook $h$ such that $\lambda \backslash h=(n-p)$. Thus $\lambda \in \Lambda_{n, p}$.

Second, let $p \in \Pi_{n}$ and $\lambda \in \Lambda_{n, p}$. Using the above description of $\Lambda_{n, p}$ yields, for the product of hook lengths of $\lambda$,

$$
T:=\prod_{(i, j) \in \lambda}\left|H_{i, j}(\lambda)\right| \leqslant n \lambda_{1}!p\left(\lambda_{2}-1\right)!\left(n-\lambda_{1}-\lambda_{2}\right)!.
$$

We can bound this expression as follows:
Case (a): $T \leqslant n(n-p)!p\left(\lambda_{2}-1\right)!\left(p-\lambda_{2}\right)!\leqslant n(n-p)!p!$.
Case (b): $T \leqslant n \lambda_{1}!p(n-p)!\left(p-1-\lambda_{1}\right)!\leqslant n(n-p)!p!$.
(a)

(b)


Figure 1. The two cases of $\lambda \backslash h=(n-p), \lambda \neq(n)$ for $n=10, p=7$

Thus it follows from the hook formula (Lemma 2.5) for sufficiently large $n$ that

$$
\chi^{\lambda}(1) \geqslant \frac{1}{n}\binom{n}{p} \geqslant \frac{1}{n}\left(\frac{n}{p}\right)^{p} \geqslant \exp \left(\frac{1}{4} n\right)
$$

Finally, we will use the following estimate, due to T. W. Müller and J.-C. SchlagePuchta [14, Theorem 1], which improves the trivial bound $|\chi(\sigma)| \leqslant \chi(1)$ for an irreducible character $\chi$ of $S_{n}$, if the number $f(\sigma)$ of fixed points of $\sigma \in S_{n}$ is not too large.

Lemma 2.7. Let $\chi \in \operatorname{Irr}\left(S_{n}\right)$ be an irreducible character, let $\sigma \in S_{n}$ be a permutation and let $n$ be sufficiently large. Then we have

$$
|\chi(\sigma)| \leqslant \chi(1)^{1-\delta(\sigma)}
$$

where

$$
\delta(\sigma):= \begin{cases}\frac{1}{13}, & \text { if } f(\sigma)=0 \\ \frac{\log (n / f(\sigma))}{32 \log n}, & \text { if } 1 \leqslant f(\sigma) \leqslant n\end{cases}
$$

## 3. Two Permutations

If $\sigma \in H$ for some primitive $H \ngtr A_{n}$, then we know from Lemma 1.5 that $\sigma \in \mathfrak{M}$. Suppose then that we pick $(\pi, \sigma) \in S_{n} \times \mathfrak{M}$ uniformly at random, and let $X$ be the number of $i \in\{0, \ldots, N-1\}$ such that $\pi \sigma^{i} \in \mathfrak{C}$. If $X>0$ then by Lemma 1.4 we cannot have $\pi, \sigma \in H$ for any primitive $H \nsupseteq A_{n}$. Thus by Chebyshev's inequality we get

$$
\begin{equation*}
P_{2}(n) \leqslant \frac{|\mathfrak{M}|}{n!} Q(X=0) \leqslant \frac{|\mathfrak{M}|}{n!} \frac{\operatorname{Var} X}{(\mathrm{E} X)^{2}} \tag{1}
\end{equation*}
$$

where $Q$ denotes the uniform distribution on $S_{n} \times \mathfrak{M}$. Now since we are still taking $\pi$ uniformly at random from $S_{n}$ we clearly have

$$
\mathrm{E} X=N \frac{|\mathfrak{C}|}{n!}
$$

while

$$
\operatorname{Var} X=N \frac{|\mathfrak{C}|}{n!}\left(1-\frac{|\mathfrak{C}|}{n!}\right)+2 \sum_{0 \leqslant i<j<N}\left(Q\left(\pi \sigma^{i}, \pi \sigma^{j} \in \mathfrak{C}\right)-\left(\frac{|\mathfrak{C}|}{n!}\right)^{2}\right)
$$

Now we express $Q\left(\pi \sigma^{i}, \pi \sigma^{j} \in \mathfrak{C}\right)$ in terms of characters. Define

$$
r_{\nu}(\tau)=\#\left\{\sigma \in \mathfrak{M}: \sigma^{\nu}=\tau\right\} .
$$

Then by Lemma 2.1] we have

$$
\begin{aligned}
Q\left(\pi \sigma^{i}, \pi \sigma^{j} \in \mathfrak{C}\right) & =\frac{1}{n!|\mathfrak{M}|} \sum_{(\pi, \sigma) \in S_{n} \times \mathfrak{M}} \mathbb{1}_{\mathfrak{C}}\left(\pi \sigma^{i}\right) \mathbb{1}_{\mathfrak{C}}\left(\pi \sigma^{j}\right) \\
& =\frac{1}{n!|\mathfrak{M}|} \sum_{x, y \in S_{n}} \mathbb{1}_{\mathfrak{C}}(x) \mathbb{1}_{\mathfrak{C}}(y) r_{j-i}\left(x^{-1} y\right) \\
& =\frac{n!}{|\mathfrak{M}|} \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)} \frac{\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle^{2}\left\langle\chi, r_{j-i}\right\rangle}{\chi(1)}
\end{aligned}
$$

The contribution from the trivial character $\chi=1$ is precisely $(|\mathfrak{C}| / n!)^{2}$, since $\left\langle 1, r_{j-i}\right\rangle=|\mathfrak{M}| / n$ !. Thus it follows

$$
\begin{equation*}
\operatorname{Var} X=N \frac{|\mathfrak{C}|}{n!}\left(1-\frac{|\mathfrak{C}|}{n!}\right)+\frac{2 n!}{|\mathfrak{M}|} \sum_{\nu=1}^{N}(N-\nu) \sum_{\chi \neq 1} \frac{\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle^{2}\left\langle\chi, r_{\nu}\right\rangle}{\chi(1)} \tag{2}
\end{equation*}
$$

Note that

$$
\left\langle\chi, r_{\nu}\right\rangle=\frac{1}{n!} \sum_{\sigma \in \mathfrak{M}} \chi\left(\sigma^{\nu}\right)
$$

Therefore we obtain

$$
\begin{aligned}
\frac{\left|\left\langle\chi, r_{\nu}\right\rangle\right|}{\chi(1)} & \leqslant \frac{1}{n!} \sum_{\sigma \in \mathfrak{M}} \frac{\left|\chi\left(\sigma^{\nu}\right)\right|}{\chi(1)} \\
& \leqslant \frac{\#\left\{\sigma: \sigma^{\nu}=1\right\}}{n!}+\max _{\sigma \in \mathfrak{M}: \sigma^{\nu} \neq 1} \frac{\left|\chi\left(\sigma^{\nu}\right)\right|}{\chi(1)}
\end{aligned}
$$

By Lemma 2.6 we know that $\chi(1) \geqslant \exp (n / 4)$ whenever $\left\langle\chi, \mathbb{1}_{\mathfrak{c}}\right\rangle \neq 0$, and by definition of $\mathfrak{M}$ we know that $\sigma^{\nu}$ has at most $n-n^{1 / 2} / 2$ fixed points whenever $\sigma^{\nu} \neq 1$, so Lemma 2.7 yields

$$
\max _{\sigma \in \mathfrak{M}: \sigma^{\nu} \neq 1} \frac{\left|\chi\left(\sigma^{\nu}\right)\right|}{\chi(1)} \leqslant \exp (n / 4)^{-\delta}
$$

where

$$
\delta=\frac{\log \left(n /\left(n-n^{1 / 2} / 2\right)\right)}{32 \log n} \geqslant \frac{n^{-1 / 2}}{64 \log n}
$$

Thus

$$
\max _{\sigma \in \mathfrak{M}: \sigma^{\nu} \neq 1} \frac{\left|\chi\left(\sigma^{\nu}\right)\right|}{\chi(1)} \leqslant \exp \left(-\frac{n^{1 / 2}}{2^{8} \log n}\right)
$$

By orthogonality of characters it follows that

$$
\begin{aligned}
& \sum_{\nu=1}^{N}(N-\nu)
\end{aligned} \begin{aligned}
& \sum_{\chi \neq 1} \frac{\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle^{2}\left\langle\chi, r_{\nu}\right\rangle}{\chi(1)} \\
& \quad \leqslant N \sum_{\nu=1}^{N} \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)}\left|\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle\right|^{2}\left(\frac{\#\left\{\sigma: \sigma^{\nu}=1\right\}}{n!}+\exp \left(-\frac{n^{1 / 2}}{2^{8} \log n}\right)\right) \\
& \quad=N \frac{|\mathfrak{C}|}{n!}\left(\sum_{\nu=1}^{N} \frac{\#\left\{\sigma: \sigma^{\nu}=1\right\}}{n!}+N \exp \left(-\frac{n^{1 / 2}}{2^{8} \log n}\right)\right)
\end{aligned}
$$

To finish we need to count pairs $(\sigma, \nu)$ such that $\sigma^{\nu}=1$.
We will need the following simple bound for the number of permutations without long cycles. (See [13, 17] for more precise estimates involving the Dickman function.)
Lemma 3.1. Let $r$ and $m$ be positive integers such that $r \leqslant m / 2$. Then the number of $\pi \in S_{m}$ all of whose cycles have length at most $r$ is bounded by

$$
\left(\frac{2 r}{m}\right)^{\frac{m}{2 r}} m!
$$

Proof. Let $p(m, r)$ be the probability that a random $\pi \in S_{m}$ has no cycle of length greater than $r$. Recall that we can sample $\pi$ as follows: First we choose the length $j$ of the cycle containing 1 uniformly from $\{1, \ldots, m\}$, then we choose the set $\left\{\pi(1), \ldots, \pi^{j-1}(1)\right\}$ uniformly from all possible $(j-1)$-subsets of $\{2, \ldots, m\}$, and then we choose (inductively) a random permutation of $\left\{1, \pi(1), \ldots, \pi^{j-1}(1)\right\}^{c}$. Since the probability that $j \leqslant r$ is clearly $r / m$, we deduce the recurrence

$$
p(m, r) \leqslant \frac{r}{m} \max _{1 \leqslant j \leqslant r} p(m-j, r)
$$

Let $q(m, r)=\max _{m^{\prime} \geqslant m} p\left(m^{\prime}, r\right)$. Then we have

$$
q(m, r) \leqslant \frac{r}{m} q(m-r, r)
$$

whenever $m>r$, while of course $q(m, r)=1$ if $m \leqslant r$. Thus provided $r \leqslant m / 2$ we have

$$
q(m, r) \leqslant \frac{r}{m} \frac{r}{m-r} \cdots \frac{r}{m-\lfloor m /(2 r)\rfloor r} \leqslant\left(\frac{2 r}{m}\right)^{1+\left\lfloor\frac{m}{2 r}\right\rfloor} \leqslant\left(\frac{2 r}{m}\right)^{\frac{m}{2 r}}
$$

Lemma 3.2. Assume $N \geqslant n$. Then we have

$$
k(N):=\#\left\{(\nu, \sigma): 1 \leqslant \nu \leqslant N, \sigma \in S_{n}, \sigma^{\nu}=1\right\}=N^{1+o(1)} n!n^{-2}
$$

for all sufficiently large $n$.
In the proof we will find it convenient to use the Vinogradov notation $X \ll Y$ familiar from analytic number theory, which means simply $X \leqslant C Y$ for some implicit constant $C$, or in other words $X \leqslant O(Y)$.
Proof. First, we establish that $k(N) \gg N n!n^{-2}$ : Let $D$ be the conjugacy class of $n$-cycles in $S_{n}$. Obviously, $|D|=\frac{n!}{n}$ and $\operatorname{ord}(\sigma)=n$ for $\sigma \in D$. Thus we obtain

$$
k(N) \geqslant \frac{n!}{n} \cdot\left\lfloor\frac{N}{n}\right\rfloor \geqslant \frac{1}{2} N n!n^{-2}
$$

Second, we prove that $k(N) \leqslant N^{1+o(1)} n!n^{-2}$ : For a permutation $\pi \in S_{m}$ and $1 \leqslant j \leqslant m$ denote by $c_{j}(\pi)$ the number of $j$-cycles of $\pi$. Let $m$ be sufficiently large and let $r(m):=\left\lfloor\frac{m}{\log m}\right\rfloor$. By the previous Lemma we have

$$
\begin{aligned}
A_{1}(m) & :=\#\left\{\sigma \in S_{m}: c_{j}(\sigma)=0 \forall j>r(m)\right\} \\
& \leqslant\left(\frac{2 r(m)}{m}\right)^{\frac{m}{2 r(m)}} m! \\
& \leqslant\left(\frac{2}{\log m}\right)^{\frac{\log m}{2}} m! \\
& \ll \frac{m!}{m^{2}} .
\end{aligned}
$$

In addition, we consider for a given positive integer $\nu$ the number of permutations $\sigma \in S_{m}$ having at least one cycle of length $>r(m)$ such that $\sigma^{\nu}=1$ :

$$
\begin{aligned}
A_{2}(m, \nu) & :=\#\left\{\sigma \in S_{m}: \sigma^{\nu}=1 \wedge\left(\exists j>r(m): c_{j}(\sigma) \neq 0\right)\right\} \\
& \leqslant \sum_{\substack{j \mid \nu \\
j>r(m)}} \frac{m!}{j} \leqslant \frac{m!}{r(m)} \cdot d(\nu),
\end{aligned}
$$

where $d(\nu)$ denotes the number of divisors of $\nu$. Combining the previous two results yields

$$
A_{3}(m, \nu):=\#\left\{\sigma \in S_{m}: \sigma^{\nu}=1\right\} \leqslant A_{1}(m)+A_{2}(m, \nu) \ll \frac{m!}{r(m)} \cdot d(\nu)
$$

Furthermore, we give an upper bound for the sum $\sum_{1 \leqslant \nu \leqslant N} A_{2}(n, \nu)$. Applying the preceding estimate we get for all sufficiently large $n$

$$
\begin{aligned}
\sum_{1 \leqslant \nu \leqslant N} A_{2}(n, \nu) & \leqslant \sum_{1 \leqslant \nu \leqslant N} \sum_{r(n)<j \leqslant n}^{j \mid \nu} \\
& \left.<\begin{array}{c}
n \\
j
\end{array}\right) \frac{j!}{j} A_{3}(n-j, \nu) \\
& <N n!n^{-2}+\sum_{r(n)<j<n} \sum_{\substack{1 \leqslant \nu \leqslant N \\
j \mid \nu}} \frac{n!\log (n-j)}{j(n-j)} \cdot d(\nu) .
\end{aligned}
$$

As $d(\nu) \ll \nu^{1 / \log \log \nu}$ (see [11, Theorem 317]) we have $d(\nu) \leqslant N^{o(1)}$ for $\nu \leqslant N$. Therefore, it follows that

$$
\begin{aligned}
\sum_{1 \leqslant \nu \leqslant N} A_{2}(n, \nu) & \ll N n!n^{-2}+N^{1+o(1)} n!\sum_{r(n)<j<n} \frac{\log (n-j)}{j^{2}(n-j)} \\
& =N^{1+o(1)} n!n^{-2} .
\end{aligned}
$$

Thus, we conclude

$$
k(N) \leqslant \sum_{1 \leqslant \nu \leqslant N}\left(A_{1}(n)+A_{2}(n, \nu)\right) \leqslant N^{1+o(1)} n!n^{-2} .
$$

Combining the preceding Lemma with (2) and (3) we get

$$
\operatorname{Var} X \leqslant N \frac{|\mathfrak{C}|}{n!}+N^{2+o(1)} \frac{|\mathfrak{C}|}{|\mathfrak{M}|} n^{-2}
$$

For each $p \in \Pi_{n}$ there are $\binom{n}{p}(p-1)!(n-p)!=\frac{n!}{p}$ elements of $S_{n}$ containing a $p$-cycle. Therefore we have $|\mathfrak{C}| \geqslant \frac{n!}{n}\left|\Pi_{n}\right|$ and (a weak version of) the prime number theorem yields

$$
|\mathfrak{C}| \geqslant \frac{n!}{2 \log n}
$$

for sufficiently large $n$. Thus it follows from (1) that

$$
P_{2}(n) \leqslant \frac{1}{N} \frac{|\mathfrak{M}|}{|\mathfrak{C}|}+N^{o(1)} \frac{n!}{|\mathfrak{C}|} n^{-2} \leqslant \frac{2 \log n}{N}+N^{o(1)} \frac{\log n}{n^{2}}
$$

Putting $N=n^{2}$ we get

$$
P_{2}(n) \leqslant n^{-2+o(1)}
$$

as required.

## 4. Three permutations

In this last section we consider

$$
P_{3}(n)=P\left(\left\{(\pi, \sigma, \tau) \in S_{n}^{3}: \pi, \sigma, \tau \in H \text { for some primitive } H \ngtr A_{n}\right\}\right) .
$$

The proof is much like that of the previous section, except that we use the collection of words of the form $\pi w(\sigma, \tau)$ in place of $\pi, \pi \sigma, \ldots, \pi \sigma^{N-1}$.

Let

$$
\mathfrak{M}_{2}=\left\{(\sigma, \tau) \in S_{n}^{2}: m(\langle\sigma, \tau\rangle)>\sqrt{n} / 2\right\} .
$$

By Lemma 1.5 we know that if $\sigma, \tau \in H$ for some primitive $H \ngtr A_{n}$ then $(\sigma, \tau) \in$ $\mathfrak{M}_{2}$, so we may assume that we pick $(\sigma, \tau)$ randomly from $\mathfrak{M}_{2}$. Let $W_{N}$ be the set of all words $w \in F_{2}$ of length at most $N$. Supposing we pick $\pi \in S_{n}$ and $(\sigma, \tau) \in \mathfrak{M}_{2}$ at random, let $X$ be the number of $w \in W_{N}$ of length at most $N$ such that $\pi w(\sigma, \tau) \in \mathfrak{C}$. Then

$$
P_{3}(n) \leqslant \frac{\left|\mathfrak{M}_{2}\right|}{n!^{2}} Q(X=0) \leqslant \frac{\left|\mathfrak{M}_{2}\right|}{n!^{2}} \frac{\operatorname{Var} X}{(\mathrm{E} X)^{2}}
$$

where $Q$ denotes the uniform distribution on $S_{n} \times \mathfrak{M}_{2}$. Now

$$
\mathrm{E} X=\left|W_{N}\right| \frac{|\mathfrak{C}|}{n!}
$$

and

$$
\begin{aligned}
\operatorname{Var} X & =\sum_{w, w^{\prime} \in W_{N}}\left(Q\left(\pi w(\sigma, \tau), \pi w^{\prime}(\sigma, \tau) \in \mathfrak{C}\right)-\frac{|\mathfrak{C}|^{2}}{n!^{2}}\right) \\
& =\left|W_{N}\right| \frac{|\mathfrak{C}|}{n!}\left(1-\frac{|\mathfrak{C}|}{n!}\right)+\sum_{\substack{w, w^{\prime} \in W_{N} \\
w \neq w^{\prime}}}\left(Q\left(\pi w(\sigma, \tau), \pi w^{\prime}(\sigma, \tau) \in \mathfrak{C}\right)-\frac{|\mathfrak{C}|^{2}}{n!^{2}}\right)
\end{aligned}
$$

For $w \in F_{2}$ and $x \in S_{n}$, let

$$
r_{w}(x)=\#\left\{(\sigma, \tau) \in \mathfrak{M}_{2}: w(\sigma, \tau)=x\right\}
$$

Then

$$
\begin{aligned}
\frac{\left|\mathfrak{M}_{2}\right|}{n!^{2}} Q\left(\pi w(\sigma, \tau), \pi w^{\prime}(\sigma, \tau) \in \mathfrak{C}\right) & =\frac{1}{n!^{3}} \sum_{\pi \in S_{n}} \sum_{(\sigma, \tau) \in \mathfrak{M}_{2}} \mathbb{1}_{\mathfrak{C}}(\pi w(\sigma, \tau)) \mathbb{1}_{\mathfrak{C}}\left(\pi w^{\prime}(\sigma, \tau)\right) \\
& =\frac{1}{n!^{3}} \sum_{x, y \in S_{n}} \mathbb{1}_{\mathfrak{C}}(x) \mathbb{1}_{\mathfrak{C}}(y) r_{w^{-1} w^{\prime}}\left(x^{-1} y\right) \\
& =\frac{1}{n!} \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)} \frac{\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle^{2}\left\langle\chi, r_{w^{-1} w^{\prime}}\right\rangle}{\chi(1)}
\end{aligned}
$$

The contribution from the trivial character $\chi=1$ is precisely

$$
\frac{\left|\mathfrak{M}_{2}\right||\mathfrak{C}|^{2}}{n!^{4}}
$$

To bound the other terms note that

$$
\begin{aligned}
\frac{1}{n!} \frac{\left\langle\chi, r_{w}\right\rangle}{\chi(1)} & =\frac{1}{n!^{2}} \sum_{(\sigma, \tau) \in \mathfrak{M}_{2}} \frac{\chi(w(\sigma, \tau))}{\chi(1)} \\
& =\frac{\#\left\{(\sigma, \tau) \in \mathfrak{M}_{2}: w(\sigma, \tau)=1\right\}}{n!^{2}}+\frac{1}{n!^{2}} \sum_{\substack{(\sigma, \tau) \in \mathfrak{M}_{2} \\
w(\sigma, \tau) \neq 1}} \frac{\chi(w(\sigma, \tau))}{\chi(1)}
\end{aligned}
$$

So

$$
\frac{1}{n!} \frac{\left|\left\langle\chi, r_{w}\right\rangle\right|}{\chi(1)} \leqslant \frac{\#\left\{(\sigma, \tau) \in S_{n}^{2}: w(\sigma, \tau)=1\right\}}{n!^{2}}+\max _{\substack{(\sigma, \tau) \in \mathfrak{M}_{2} \\ w(\sigma, \tau) \neq 1}} \frac{|\chi(w(\sigma, \tau))|}{\chi(1)}
$$

Provided that $\chi \neq 1$ and $\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle \neq 0$, the second term is bounded by

$$
\exp \left(-c n^{1 / 2} / \log n\right)
$$

just as in the previous section. The first term is also small, by the following Lemma (see [9, Lemma 2.2]).

Lemma 4.1. Let $w \in F_{2}$ be a non-trivial word of length at most $k \leqslant \sqrt{n / 2}$. If $\sigma, \tau \in S_{n}$ are chosen uniformly at random then the probability that $w(\sigma, \tau)=1$ is bounded by $\exp \left(-c n / k^{2}\right)$.

Thus provided $w \neq 1$ and $N \leqslant c n^{1 / 3}$ we have

$$
\frac{1}{n!} \frac{\left|\left\langle\chi, r_{w}\right\rangle\right|}{\chi(1)} \leqslant \exp \left(-c n^{1 / 3}\right)
$$

Therefore, it follows for $w \neq w^{\prime}$ that

$$
\begin{aligned}
\left|\frac{1}{n!} \sum_{\substack{\chi \in \operatorname{Irr}\left(S_{n}\right) \\
\chi \neq 1}} \frac{\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle^{2}\left\langle\chi, r_{w^{-1} w^{\prime}}\right\rangle}{\chi(1)}\right| & \leqslant \sum_{\chi \in \operatorname{Irr}\left(S_{n}\right)}\left|\left\langle\chi, \mathbb{1}_{\mathfrak{C}}\right\rangle\right|^{2} \exp \left(-c n^{1 / 3}\right) \\
& =\frac{|\mathfrak{C}|}{n!} \exp \left(-c n^{1 / 3}\right) \\
& \leqslant \exp \left(-c n^{1 / 3}\right) .
\end{aligned}
$$

Thus

$$
\frac{\left|\mathfrak{M}_{2}\right|}{n!^{2}} \operatorname{Var} X \leqslant\left|W_{N}\right| \frac{|\mathfrak{C}|}{n!}+\left|W_{N}\right|^{2} \exp \left(-c n^{1 / 3}\right)
$$

so we deduce

$$
P_{3}(n) \leqslant \frac{\mathcal{O}(\log n)}{\left|W_{N}\right|}+\exp \left(-c n^{1 / 3}\right) .
$$

Note that $\left|W_{N}\right|=4 \cdot 3^{N-1}$. Taking $N=\left\lfloor c n^{1 / 3}\right\rfloor$, we conclude

$$
P_{3}(n) \leqslant \exp \left(-c n^{1 / 3}\right)
$$

## Acknowledgements

I, Stefan-Christoph, would like to express my deep gratitude to Jan-Christoph Schlage-Puchta for his proposal to consider this theme and for the many inspiring discussions we had. Furthermore, I would like to offer my special thanks to Andrzej Zuk for his interest in the subject. Moreover, I am very grateful to the referees for their helpful suggestions. Finally, I would like to express my very great appreciation to my family for their support and encouragement throughout my study.

## References

[1] L. Babai: The probability of generating the symmetric group, J. Combin. Theory Ser. A 52 (1989), 148-153.
[2] J. Bovey: The probability that some power of a permutation has small degree, Bull. Lond. Math. Soc. 12 (1980), 47-51.
[3] J. Bovey, A. Williamson: The probability of generating the symmetric group, Bull. Lond. Math. Soc. 10 (1978), 91-96.
[4] C. W. Curtis, I. Reiner: Methods of Representation Theory, Volume I, Wiley, New York (1990).
[5] J. D. Dixon: Asymptotics of generating the symmetric and alternating groups, Electron. J. Combin. 12 (2005), Research Paper \#R56.
[6] J. D. Dixon: The probability of generating the symmetric group, Math. Z. 110 (1969), 199-205.
[7] J. D. Dixon, B. Mortimer: Permutation Groups, Springer, New York (1996).
[8] S. Eberhard, K. Ford, D. Koukoulopoulos: Permutations contained in transitive subgroups, Discrete Analysis 12 (2016).
[9] S. Eberhard: The trivial lower bound for the girth of $S_{n}$, arXiv:1706.09972 (2017).
[10] J. S. Frame, G. de B. Robinson, R. M. Thrall: The hook graphs of the symmetric group, Canad. J. Math. 6 (1954), 316-324.
[11] G. H. Hardy, E. M. Wright: An Introduction to the Theory of Numbers, Clarendon, Oxford (1954).
[12] A. Kerber: Algebraic Combinatorics Via Finite Group Actions, BI-Wissenschaftsverlag, Mannheim-Wien-Zürich (1991).
[13] E. Manstavičius, R. Petuchovas: Permutations without long or short cycles, Electron. Notes Discrete Math. 49 (2015), 153-158.
[14] T. W. Müller, J.-C. Schlage-Puchta: Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks, Adv. Math. 213 (2007), 919-982.
[15] T. Nakayama: On some modular properties of irreducible representations of a symmetric group, I, Jap. J. Math. 17 (1940), 165-184.
[16] E. Netto: The Theory of Substitutions and its Applications to Algebra, The Inland Press, Ann Arbor (1892).
[17] R. Petuchovas: Asymptotic analysis of the cyclic structure of permutations, arXiv:1611.02934 (2016), 1-77.
[18] B. E. Sagan: The Symmetric Group, Springer, New York (2001).
[19] J.-C. Schlage-Puchta: Applications of character estimates to statistical problems for the symmetric group, Combinatorica 32 (2012), 309-323.
[20] N. J. A. Sloane: The On-Line Encyclopedia of Integer Sequences, http://oeis.org. Sequence A113869.
[21] H. Wielandt: Finite Permutation Groups, Academic Press, New York (1964).

Author information<br>Sean Eberhard, London, UK<br>E-mail: eberhard.math@gmail.com<br>Stefan-Christoph Virchow, Institut für Mathematik, Universität Rostock<br>Ulmenstr. 69 Haus 3, 18057 Rostock, Germany<br>E-mail: stefan.virchow@uni-rostock.de

