Mathematics

https://www.aimspress.com/journal/Math

AIMS Mathematics, 9(9): 24394–24400.
DOI: 10.3934/math.20241188
Received: 26 March 2024
Revised: 10 August 2024
Accepted: 14 August 2024
Published: 19 August 2024

Research article

On the proportion of elements of order a product of two primes in finite symmetric groups

Hailin Liu*, **Longzhi Lu** and **Liping Zhong**

School of Science, Jiangxi University of Science and Technology, Ganzhou 341000, China

* **Correspondence:** Email: hailinliuqp@163.com.

Abstract: This is one of a series of papers that aims to give an explicit upper bound on the proportion of elements of order a product of two primes in finite symmetric groups. This one presents such a bound for the elements as the product of two distinct odd primes.

Keywords: symmetric groups; elements; order; proportion; upper bound
Mathematics Subject Classification: 20B30, 05A05

1. Introduction

The famous Cayley theorem reveals a basic fact: A finite group G of order n is isomorphic to a subgroup of the finite symmetric group S_n. This means that G can be given as a group generated by a set M of permutations in S_n, that is, $G = \langle M \rangle$. To construct a generating set of G, we need to seek special kinds of elements in S_n, which are usually sought randomly. Further, to understand the complexity of such searches, we need to estimate the proportions of various kinds of elements, such as those with order p, $2p$, or pq in S_n for the odd primes p and q. For examples, a transposition is constructed by searching for an element g of order $2m$ in S_n for some odd positive integer $m \leq n^{18 \log n}$; see [1]. The upper bound for m is chosen so that the proportion of such elements is large enough to find such an element g with high probability, and also to construct the transposition g^m at a reasonable cost. This method is better than a direct search for a transposition by examining random elements, as the proportion of transpositions is very small. The proportion of elements with order a multiple of p in S_n, called p-singular elements, is far greater than the proportion of elements with order p; see [9, Section 1]. This means that constructing elements of order p by taking powers of p-singular elements is much more efficient than searching for such elements directly by random selection.

The proportion of elements of a given prime order p in finite symmetric groups has been extensively studied. For example, in [4], Jacabsthal gave recursive formulas and an asymptotic expansion on this proportion for the first time. Chowla, Herstein, and Scott [2] and Moser and Wyman [6] extended

Jacabsthal's result in 1952 and 1955, respectively. In 2022, Praeger and Suleiman [9] gave an explicit upper bound on the proportion of permutations of a given prime order p in finite symmetric groups. More results can be found in [3, 7, 8].

In fact, a product of disjoint 2-cycles and p-cycles is a permutation of order $2p$. But we note that a permutation of order $2p$ may be obtained by other cycles, such as $2p$-cycles, a product of disjoint $2p$-cycles and p-cycles, or 2-cycles, and so on. In 2024, the first and third authors in [5] addressed an upper bound on the proportion of permutations of twice a prime order, acting on a set of given size n. In this paper, we generalize the result in [5] and present an upper bound for the elements that have order a product of two distinct odd primes in finite symmetric groups.

This paper is organized as follows: After this introduction, we give some preliminary results in Section 2. Then, the main result is given and proved in Section 3. Finally, we make a conjecture on the proportion of elements with a given order in finite symmetric groups in Section 4.

2. Preliminaries

In this section, we give a lemma and several propositions, which will be used to prove our main result in the next section.

Let m be a positive integer, and let $[m] = \{1, 2, \cdots, m\}$ and S_m be the symmetric group on $[m]$. First, we record a basic fact.

Lemma 2.1. *For each positive integer m, there are exactly* $(m-1)!$ *pairwise distinct m-cycles in* S_m.

Proof. Each m-cycle in S_m has a unique expression of the form $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ where $\alpha_i \in [m] = \{1, 2, \cdots, m\}$ for $1 \le i \le m$ and $\alpha_j = 1$ for some $j \in [m]$. To count the number of possibilities for the m-cycles, there are exactly $m-1$ choices for $\alpha_1 \in [m]\backslash\{1\}$, and exactly $m-2$ choices for α_2 from $[m]\backslash\{1, \alpha_1\}$ when α_1 is gven, and so on. This implies that there are exactly $(m-1)!$ m-cycles in S_m. ∎

For two distinct odd primes p and q, the element g of order pq in S_n can be written out explicitly in one of the following forms:

$$\text{(I)}\ \underbrace{\overbrace{(\cdots)}^{p\text{-}cycle}\overbrace{(\cdots)}^{p\text{-}cycle}\cdots\overbrace{(\cdots)}^{p\text{-}cycle}}_{s_1}\underbrace{\overbrace{(\cdots)}^{q\text{-}cycle}\overbrace{(\cdots)}^{q\text{-}cycle}\cdots\overbrace{(\cdots)}^{q\text{-}cycle}}_{t_2};$$

$$\text{(II)}\ \underbrace{\overbrace{(\cdots)}^{pq\text{-}cycle}\overbrace{(\cdots)}^{pq\text{-}cycle}\cdots\overbrace{(\cdots)}^{pq\text{-}cycle}}_{s_2};$$

$$\text{(III)}\ \underbrace{\overbrace{(\cdots)}^{p\text{-}cycle}\overbrace{(\cdots)}^{p\text{-}cycle}\cdots\overbrace{(\cdots)}^{p\text{-}cycle}}_{s_3}\underbrace{\overbrace{(\cdots)}^{pq\text{-}cycle}\overbrace{(\cdots)}^{pq\text{-}cycle}\cdots\overbrace{(\cdots)}^{pq\text{-}cycle}}_{t_3};$$

$$\text{(IV)}\ \underbrace{\overbrace{(\cdots)}^{q\text{-}cycle}\overbrace{(\cdots)}^{q\text{-}cycle}\cdots\overbrace{(\cdots)}^{q\text{-}cycle}}_{s_4}\underbrace{\overbrace{(\cdots)}^{pq\text{-}cycle}\overbrace{(\cdots)}^{pq\text{-}cycle}\cdots\overbrace{(\cdots)}^{pq\text{-}cycle}}_{t_4};\ \text{or}$$

$$\text{(V)}\ \underbrace{\overbrace{(\cdots)}^{p\text{-}cycle}\overbrace{(\cdots)}^{p\text{-}cycle}\cdots\overbrace{(\cdots)}^{p\text{-}cycle}}_{s_5}\underbrace{\overbrace{(\cdots)}^{q\text{-}cycle}\overbrace{(\cdots)}^{q\text{-}cycle}\cdots\overbrace{(\cdots)}^{q\text{-}cycle}}_{t_5}\underbrace{\overbrace{(\cdots)}^{pq\text{-}cycle}\overbrace{(\cdots)}^{pq\text{-}cycle}\cdots\overbrace{(\cdots)}^{pq\text{-}cycle}}_{m};$$

where $s_i \geq 1$, $t_j \geq 1$ for $1 \leq i \leq 5$, $2 \leq j \leq 5$, and $m \geq 1$.

Second, we find an upper bound on the proportion of elements in each form above. Let $\mathcal{P}_n(pq)$ and $\mathcal{P}_n^*(pq)$ denote the set consisting of all the elements of order pq, and the set of elements with form (*) in S_n, respectively, where * is one of I, II,..., V above. The corresponding proportions are denoted by $\rho_n(pq) = \frac{|\mathcal{P}_n(pq)|}{n!}$ and $\rho_n^*(pq) = \frac{|\mathcal{P}_n^*(pq)|}{n!}$, respectively. In order to prove Theorem 3.1, we need the following recursion for $\rho_n^*(pq)$.

Proposition 2.1. *Let p and q be distinct odd primes such that $p < q$. Let n be a positive integer. Then the proportion $\rho_n^*(pq)$ of elements with the form (*) as above in S_n satisfies the following relations:*

(1) If $* = I$ and $n \geq p + q + 1$, then

$$n\rho_n^I(pq) = \rho_{n-1}^I(pq) + \rho_{n-p}(q) + \rho_{n-p}^I(pq) + \rho_{n-q}(p) + \rho_{n-q}^I(pq).$$

(2) If $* = II$ and $n \geq pq + 1$, then

$$n\rho_n^{II}(pq) = \rho_{n-1}^{II}(pq) + \rho_{n-pq}^{II}(pq) + \frac{1}{(n-pq)!}.$$

(3) If $* = III$ and $n \geq pq + p + 1$, then

$$n\rho_n^{III}(pq) = \rho_{n-1}^{III}(pq) + \rho_{n-p}^{II}(pq) + \rho_{n-p}^{III}(pq) + \rho_{n-pq}(p) + \rho_{n-pq}^{III}(pq).$$

(4) If $* = IV$ and $n \geq pq + q + 1$, then

$$n\rho_n^{IV}(pq) = \rho_{n-1}^{IV}(pq) + \rho_{n-q}^{II}(pq) + \rho_{n-q}^{IV}(pq) + \rho_{n-pq}(q) + \rho_{n-pq}^{IV}(pq).$$

(5) If $* = V$ and $n \geq pq + p + q + 1$, then

$$n\rho_n^V(pq) = \rho_{n-1}^V(pq) + \rho_{n-p}^{IV}(pq) + \rho_{n-p}^V(pq) + \rho_{n-q}^{III}(pq) + \rho_{n-q}^V(pq) + \rho_{n-pq}^I(pq) + \rho_{n-pq}^V(pq).$$

Proof. (1) We partition $\mathcal{P}_n^I(pq)$ as ${}_1\mathcal{P}_n^I(pq) \cup {}_2\mathcal{P}_n^I(pq)$, where ${}_1\mathcal{P}_n^I(pq)$ and ${}_2\mathcal{P}_n^I(pq)$ consist of all elements $g \in \mathcal{P}_n^I(pq)$ such that $1^g = 1$ and $1^g \neq 1$, respectively. We observe that ${}_1\mathcal{P}_n^I(pq)$ is precisely the set of elements having form (I) in $S_\Delta \cong S_{n-1}$ where $\Delta = [n] \backslash \{1\}$, and hence $|{}_1\mathcal{P}_n^I(pq)| = (n-1)!\rho_{n-1}^I(pq)$.

Now we enumerate the elements of ${}_2\mathcal{P}_n^I(pq)$. Since $1^g \neq 1$, 1 lies in a cycle h of g of length p or q for each such element g.

Case 1. h is a p-cycle.

The number of such cycles is equal to the number $\binom{n-1}{p-1}$ of subsets Δ' of $(p-1)$-element subsets of $\Delta \backslash \{1\}$, times the number $(p-1)!$ of p-cycles in S_n by Lemma 2.1. Then, for each of $g \in {}_2\mathcal{P}_n^I(pq)$, $g = hg'$ where $g' \in S_{[n]\backslash\{\Delta',1\}} \cong S_{n-p}$. The number of such elements g' is equal to the number $|\mathcal{P}_{n-p}^I(pq)| = (n-p)!\rho_{n-p}^I(pq)$ of elements with the form (I) in S_{n-p}, together with the number $|\mathcal{P}_{n-p}(q)| = (n-p)!\rho_{n-p}(q)$ of elements of order q in S_{n-p}. Thus

$$\begin{aligned}|{}_2\mathcal{P}_n^I(pq)| &= \binom{n-1}{p-1}(p-1)!((n-p)!\rho_{n-p}^I(pq) + (n-p)!\rho_{n-p}(q)) \\ &= (n-1)!(\rho_{n-p}^I(pq) + \rho_{n-p}(q)).\end{aligned}$$

Case 2. h is a q-cycle.

The number of such cycles is equal to the number $\binom{n-1}{q-1}$ of subsets $\Delta^{'}$ of $(q-1)$-element subsets of $\Delta\backslash\{1\}$, times the number $(q-1)!$ of q-cycles in S_n by Lemma 2.1. Then, for each of $g \in {}_2\mathcal{P}^I_n(pq)$, $g = hg^{'}$ where $g^{'} \in S_{[n]\backslash\{\Delta^{'},1\}} \cong S_{n-q}$. The number of such elements $g^{'}$ is equal to the number $|\mathcal{P}^I_{n-q}(pq)| = (n-q)!\rho^I_{n-q}(pq)$ of elements with the form (I) in S_{n-q}, together with the number $|\mathcal{P}_{n-q}(p)| = (n-q)!\rho_{n-q}(p)$ of elements of order p in S_{n-q}. Thus

$$
\begin{aligned}
|{}_2\mathcal{P}^I_n(pq)| &= \binom{n-1}{q-1}(q-1)!((n-q)!\rho^I_{n-q}(pq) + (n-q)!\rho_{n-q}(p)) \\
&= (n-1)!(\rho^I_{n-q}(pq) + \rho_{n-q}(p)).
\end{aligned}
$$

It follows that

$$
\begin{aligned}
n!\rho^I_n(pq) &= (n-1)!\rho^I_{n-1}(pq) + (n-1)!(\rho^I_{n-p}(pq) + \rho_{n-p}(q) + \rho^I_{n-q}(pq) + \rho_{n-q}(p)) \\
&= (n-1)!(\rho^I_{n-1}(pq) + \rho^I_{n-p}(pq) + \rho_{n-p}(q) + \rho^I_{n-q}(pq) + \rho_{n-q}(p))
\end{aligned}
$$

and so $n\rho^I_n(pq) = \rho^I_{n-1}(pq) + \rho^I_{n-p}(pq) + \rho_{n-p}(q) + \rho^I_{n-q}(pq) + \rho_{n-q}(p)$. This completes the proof of (1).

For (2) to (5), the proofs are analogous to the proof of (1). ∎

Next, we will use Proposition 2.1 to give an upper bound on $\rho^*_n(pq)$ by induction on n, where $* \in \{I, II, \ldots, V\}$.

Proposition 2.2. *Let p and q be distinct odd primes such that $p < q$, and let n be a positive integer. Write $n = a \cdot pq + k$, where $a \geq 0$ and $0 \leq k \leq pq - 1$. Then*

(1) $\rho^I_n(pq) \leq \frac{1}{pq}$ with equality if and only if $n = p + q$ or $p + q + 1$;
(2) $\rho^{II}_n(pq) \leq \frac{1}{pq \cdot k!}$ with equality if and only if $pq \leq n \leq 2pq - 1$;
(3) $\rho^{III}_n(pq) \leq \frac{1}{p^2 q}$ with equality if and only if $n = 2p + q$ or $2p + q + 1$;
(4) $\rho^{IV}_n(pq) \leq \frac{1}{pq^2}$ with equality if and only if $n = 2q + p$ or $2q + p + 1$;
(5) $\rho^V_n(pq) \leq \frac{1}{p^2 q^2}$ with equality if and only if $n = 2(q + p)$ or $2(q + p) + 1$.

Proof. (1) If $n < p + q$, then $\mathcal{P}^I_n(pq)$ is empty, and so $\rho^I_n(pq) = 0$. If $n = p + q$, then $|\mathcal{P}^I_n(pq)| = \frac{n!}{pq}$, and so $\rho^I_n(pq) = \frac{1}{pq}$. We now assume that $n \geq p + q + 1$ and assume inductively that the result holds for all positive integers strictly less than n.

Case 1. $n = p + q + k$, and $1 \leq k \leq 3$.

By induction, we have $\rho^I_{n-1}(pq) = \frac{1}{pq \cdot (k-1)!}$, $\rho^I_{n-p}(pq) = 0$ and $\rho^I_{n-q}(pq) = 0$, and we note that $\rho_{n-p}(q) \leq \frac{1}{q}$ and $\rho_{n-q}(p) \leq \frac{1}{p}$ by [9, Theorem 1]. Thus, by Proposition 2.1 (1),

$$
\begin{aligned}
\rho^I_n(pq) &= \frac{1}{n}(\rho^I_{n-1}(pq) + \rho^I_{n-p}(pq) + \rho_{n-p}(q) + \rho^I_{n-q}(pq) + \rho_{n-q}(p)) \\
&\leq \frac{1}{n}(\frac{1}{pq \cdot (k-1)!} + 0 + \frac{1}{q} + 0 + \frac{1}{p}) \leq \frac{1}{pq},
\end{aligned}
$$

with equality if and only if $n = p + q + 1$.

Case 2. $n > p + q + 3$.

By induction, we observe that $\rho^I_{n-1}(pq) \leq \frac{1}{pq}$, $\rho^I_{n-p}(pq) \leq \frac{1}{pq}$ and $\rho^I_{n-q}(pq) \leq \frac{1}{pq}$, and we see that $\rho_{n-p}(q) \leq \frac{1}{q}$ and $\rho_{n-q}(p) \leq \frac{1}{p}$ by [9, Theorem 1]. Thus, by Proposition 2.1 (1),

$$
\rho^I_n(pq) \leq \frac{1}{n}(\frac{1}{pq} + \frac{1}{q} + \frac{1}{pq} + \frac{1}{p} + \frac{1}{pq})
$$

$$= \frac{1}{pq}(\frac{3+p+q}{n}) < \frac{1}{pq}.$$

So we complete the proof of (1) by induction.

(2) If $n < pq$, then $\rho_n^{II}(pq) = 0$. If $n = pq$, then $\rho_n^{II}(pq) = \frac{1}{pq}$. We now assume that $n \geq pq + 1$ and assume inductively that the result holds for all positive integers strictly less than n.

Note that $n-pq = (a-1)\cdot pq+k$, $n-1 = a\cdot pq+k-1$ if $1 \leq k \leq pq-1$, and $n-1 = (a-1)\cdot pq+pq-1$ if $k = 0$.

Case 1. $a = 1$.

By induction, $\rho_{n-1}^{II}(pq) = \frac{1}{pq\cdot(k-1)!}$ and $\rho_{n-pq}^{II}(pq) = 0$. Then, by Proposition 2.1 (2),

$$\begin{aligned}\rho_n^{II}(pq) &= \frac{1}{n}(\frac{1}{pq\cdot(k-1)!} + 0 + \frac{1}{k!})\\ &= \frac{pq+k}{pq\cdot n\cdot k!} = \frac{1}{pq\cdot k!}.\end{aligned}$$

Case 2. $a \geq 2$.

If $k = 0$, then by induction, $\rho_{n-1}^{II}(pq) \leq \frac{1}{pq\cdot(pq-1)!}$ and $\rho_{n-2p}^{II}(pq) \leq \frac{1}{pq}$. So by Proposition 2.1 (2),

$$\begin{aligned}\rho_n^{II}(pq) &\leq \frac{1}{n}(\frac{1}{pq\cdot(pq-1)!} + \frac{1}{pq} + \frac{1}{(n-pq)!})\\ &= \frac{1}{npq}(\frac{1}{(pq-1)!} + 1 + \frac{pq}{(n-pq)!}) < \frac{3}{npq} < \frac{1}{pq}.\end{aligned}$$

If $k \geq 1$, then by induction, $\rho_{n-1}^{II}(pq) \leq \frac{1}{pq\cdot(k-1)!}$ and $\rho_{n-pq}^{II}(pq) \leq \frac{1}{pq\cdot k!}$. Thus, by Proposition 2.1 (2),

$$\begin{aligned}\rho_n^{II}(pq) &\leq \frac{1}{n}(\frac{1}{pq\cdot(k-1)!} + \frac{1}{pq\cdot k!} + \frac{1}{(n-pq)!})\\ &= \frac{1}{npq\cdot k!}(k+1+\frac{pq\cdot k!}{(n-pq)!}) < \frac{k+2}{npq\cdot k!} < \frac{1}{pq\cdot k!},\end{aligned}$$

and this completes the proof of (2) by induction.

With techniques similar to those in (1) and (2), we can obtain the conclusions of (3) to (5). ∎

3. Main result and proof

We present the main result and use Proposition 2.2 to prove it in this section. Our main result is as follows:

Theorem 3.1. *Let n be a positive integer, and let p and q be odd primes such that $p < q$, and write $n = a\cdot pq + k$, where $0 \leq k \leq pq-1$ and $a \geq 0$. Let $\rho_n(pq)$ be the proportion of elements of order pq in the symmetric group S_n. Then one of the following holds:*

(1) $n < p+q$, $\rho_n(pq) = 0$;
(2) $p+q \leq n \leq pq-1$, $\rho_n(pq) \leq \frac{1}{pq}$, with equality if and only if $n = p+q$ or $p+q+1$;

(3) $pq \le n \le pq + p - 1$, $\rho_n(pq) < \frac{1+k!}{pq \cdot k!}$;
(4) $pq + p \le n \le pq + q - 1$, $\rho_n(pq) < \frac{p+(p+1)k!}{p^2 q \cdot k!}$;
(5) $pq + q \le n \le pq + q + p - 1$, $\rho_n(pq) < \frac{pq+(pq+p+q)k!}{p^2 q^2 \cdot k!}$;
(6) $n \ge pq + p + q$, $\rho_n(pq) < \frac{pq+(pq+p+q+1)k!}{p^2 q^2 \cdot k!}$.

Proof. Let n be a positive integer and p and q odd primes with $p < q$, and write $n = a \cdot pq + k$ where $0 \le k \le pq - 1$ and $a \ge 0$.

If $n < p + q$, then $\mathcal{P}_n(pq)$ is empty, and so $\rho_n(pq) = 0$. Therefore, (1) holds.

If $p + q \le n \le pq - 1$, then $\mathcal{P}_n(pq) = \mathcal{P}_n^I(pq)$, and thus $\rho_n(pq) = \rho_n^I(pq) \le \frac{1}{pq}$ with equality if and only if $n = p + q$ or $p + q + 1$ by Proposition 2.2 (1). Hence, (2) holds.

If $pq \le n \le pq + p - 1$, then $\mathcal{P}_n(pq) = \mathcal{P}_n^I(pq) + \mathcal{P}_n^{II}(pq)$, and so $\rho_n(pq) = \rho_n^I(pq) + \rho_n^{II}(pq) < \frac{1}{pq} + \frac{1}{pq \cdot k!} = \frac{1+k!}{pq \cdot k!}$ by Propositions 2.2 (1) and (2). Thus, (3) holds.

If $pq + p \le n \le pq + q - 1$, then $\mathcal{P}_n(pq) = \mathcal{P}_n^I(pq) + \mathcal{P}_n^{II}(pq) + \mathcal{P}_n^{III}(pq)$, and thus $\rho_n(pq) < \frac{1}{pq} + \frac{1}{pq \cdot k!} + \frac{1}{p^2 q} = \frac{p+(p+1)k!}{p^2 q \cdot k!}$ by Proposition 2.2 (1) to (3). So (4) holds.

If $pq + q \le n \le pq + q + p - 1$, then $\mathcal{P}_n(pq) = \mathcal{P}_n^I(pq) + \mathcal{P}_n^{II}(pq) + \mathcal{P}_n^{III}(pq) + \mathcal{P}_n^{IV}(pq)$, and thus $\rho_n(pq) < \frac{1}{pq} + \frac{1}{pq \cdot k!} + \frac{1}{p^2 q} + \frac{1}{pq^2} = \frac{pq+(pq+p+q)k!}{p^2 q^2 \cdot k!}$ by Proposition 2.2 (1) to (4). Therefore, (5) holds.

If $pq + p + q \le n$, then $\mathcal{P}_n(pq) = \mathcal{P}_n^I(pq) + \mathcal{P}_n^{II}(pq) + \mathcal{P}_n^{III}(pq) + \mathcal{P}_n^{IV}(pq) + \mathcal{P}_n^{V}(pq)$, and so $\rho_n(pq) < \frac{1}{pq} + \frac{1}{pq \cdot k!} + \frac{1}{p^2 q} + \frac{1}{pq^2} + \frac{1}{p^2 q^2} = \frac{pq+(pq+p+q+1)k!}{p^2 q^2 \cdot k!}$ by Proposition 2.2 (1) to (5). Thus, (6) holds. ∎

4. Conclusions

We note that the upper bound of (1) and (2) is sharp in Theorem 3.1, but that in (3) to (6) it is not. Besides, from the results in Theorem 3.1 on the proportion of elements of order twice distinct odd primes in finite symmetric groups, we observe that the upper bound of the proportion is a function f defined on $[pq - 1] = \{0, 1, 2, \cdots, pq - 1\}$. With this in mind, we make the following conjecture:

Conjecture 4.1. *The proportion $\rho_n(m)$ of elements of order m in S_n is controlled by a function f defined on $[m - 1] = \{0, 1, 2, \cdots, m - 1\}$.*

Author contributions

Hailin Liu, Longzhi Lu and Liping Zhong: Writing-Original Draft, Writing-Review and Editing. All authors contributed equally to the manuscript. All authors have read and approved the final version of the manuscript for publication.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was partially supported by China Scholarship Council (Grant No.202208360148), National Natural Science Foundation of China (Grant No.12126415, NO.12261042, NO.12301026) and Jiangxi Provincial Natural Science Foundation (Grant No.20232BAB211006).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, A. Seress, Permutations with restricted cycle structure and an algorithmic application, *Comb. Probab. Comput.*, **11** (2002), 447–464. http://doi.org/10.1017/S0963548302005217
2. S. Chowla, I. N. Herstein, W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh. Trondheim*, **25** (1952), 29–31.
3. S. P. Glasby, C. E. Praeger, W. R. Unger, Most permutations power to a cycle of small prime length, *P. Edinburgh Math. Soc.*, **64** (2021), 234–246. https://doi.org/10.1017/S0013091521000110
4. E. Jacobsthal, Sur le nombre d'*élé*ments du groupe sym*é*trique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk. Forh. Trondheim,* **21** (1949), 49–51.
5. H. L. Liu, L. P. Zhong, On the proportion of elements of order $2p$ in finite symmetric groups, *Hacet. J. Math. Stat.*, 2024. Available from: https://doi.org/10.15672/hujms.1367438
6. L. Moser, On solutions of $x^d = 1$ in symmetric groups, *Can. J. Math.*, **7** (1955), 159–168. https://doi.org/10.4153/CJM-1955-021-8
7. A. C. Niemeyer, T. Popiel, C. E. Praeger, On proportions of pre-involutions in finite classical groups, *J. Algebra*, **324** (2010), 1016–1043. https://doi.org/10.1016/j.jalgebra.2010.03.026
8. A. C. Niemeyer, C. E. Praeger, A. Seress, *Estimation problems and randomised group algorithms. In Probabilistic Group Theory, Combinatorics and Computing*, London: Springer Press, 2013, 35–82. https://doi.org/10.1007/978-1-4471-4814-2_2
9. C. E. Praeger, E. Suleiman, On the proportion of elements of prime order in finite symmetric groups, *Int. J. Group Theory*, **13** (2024), 251–256. http://dx.doi.org/10.22108/ijgt.2023.135509.1810