Hacettepe Journal of Mathematics & Statistics

Hacet. J. Math. Stat.
Volume XX (x) (XXXX), 1 – 7
DOI : 10.15672/hujms.xx

Research Article

On the proportion of elements of order $2p$ in finite symmetric groups

Hailin Liu*, Liping Zhong

School of Science, Jiangxi University of Science and Technology, Ganzhou 341000, P.R. China

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 with order twice a prime.

Mathematics Subject Classification (2020). 20B30, 05A05

Keywords. symmetric group, element, proportion, order

1. Introduction

The famous Cayley theorem reveals a basic fact that 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 estimates for the proportions of various kinds of elements, such as those with order p or $2p$ in S_n for a prime p.

The proportion of elements of a given prime order p in the finite symmetric group S_n has been extensively studied. For example, in [3], Jacabsthal gave recursive formulas and an asymptotic expansion on this proportion for the first time. Chowla, Herstein and Scott [1] and Moser and Wyman [4] extended Jacabsthal's result in 1952 and 1955, respectively. In 2022, Praeger and Suleiman [7] gave an explicit upper bound on the proportion of permutations of a given prime order p in S_n. More results can be found in [2, 5, 6].

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. Naturally, we need to estimate the proportion of all elements of order $2p$. In this paper, we present an upper

*Corresponding Author.
Email addresses: liuhailin@jxust.edu.cn (H.L. Liu), zhongliping2022@126.com (L.P. Zhong)
Received: 27.09.2023; Accepted: 08.02.2024

bound for the elements that have order twice a prime in finite symmetric groups. Our main result is as follows.

Theorem 1.1. Let n be a positive integer and p an odd prime, and write $n = a \cdot 2p + k$ where $0 \le k \le 2p-1$ and $a \ge 0$. Let $\rho_n(2p)$ be the proportion of elements of order $2p$ in the symmetric group S_n. Then one of the following holds:

(1) $n < p+2$, $\rho_n(2p) = 0$;
(2) $p+2 \le n < 2p-1$, $\rho_n(2p) \le \frac{1}{2p}$, with equality if and only if $n = p+2$ or $p+3$;
(3) $2p \le n \le 2p+1$, $\rho_n(2p) < \frac{1}{p}$;
(4) $2p+2 \le n \le 3p-1$, $\rho_n(2p) < \frac{3k!+2}{4p\cdot k!}$, where $2 \le k \le p-1$;
(5) $3p \le n \le 3p+1$, $\rho_n(2p) < \frac{(3p+2)k!+2p}{4p^2\cdot k!}$, where $p \le k \le p+1$;
(6) $n \ge 3p+2$, $\rho_n(2p) < \frac{(3p+1)k!+2p+2}{4p^2\cdot k!}$, where $0 \le k \le p-1$; or
(7) $n \ge 3p+2$, $\rho_n(2p) < \frac{[(3p+1)k!+2p](k-p)!+2k!}{4p^2\cdot k!(k-p)!}$, where $p \le k \le 2p-1$.

Remark 1.1. The upper bound in (1) and (2) is sharp, but that in (3) to (7) is not.

2. Proof of Theorem 1.1

In this section, we will prove Theorem 1.1. Let n be a positive integer, and let $[n] = \{1, 2, \cdots, n\}$ and S_n be the symmetric group on $[n]$. 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. ∎

Since a permutation can be written as a product of disjoint cycles, the element g of order $2p$ in S_n can be written out explicitly in one of the following forms:

(I) $\underbrace{(2)\ldots(2)}_{s_1} \cdot \underbrace{(p)\ldots(p)}_{t_2}$;

(II) $\underbrace{(2p)\ldots(2p)}_{s_2}$;

(III) $\underbrace{(2)\ldots(2)}_{s_3} \cdot \underbrace{(2p)\ldots(2p)}_{t_3}$;

(IV) $\underbrace{(p)\ldots(p)}_{s_4} \cdot \underbrace{(2p)\ldots(2p)}_{t_4}$; or

(V) $\underbrace{(2)\ldots(2)}_{s_5} \cdot \underbrace{(p)\ldots(p)}_{t_5} \cdot \underbrace{(2p)\ldots(2p)}_{m}$,

where $s_i \ge 1$, $t_j \ge 1$ for $1 \le i \le 5$, $2 \le j \le 5$ and $m \ge 1$.

Second, we find an upper bound on the proportion of elements in each form above. Let $\mathcal{P}_n(2p)$ and $\mathcal{P}_n^*(2p)$ denote the subset consisting of all elements of order $2p$, and the set of elements with form (*) in S_n, respectively, where * is one of I, II,…, V above. The corresponding proportions are $\rho_n(2p) = \frac{|\mathcal{P}_n(2p)|}{n!}$ and $\rho_n^*(2p) = \frac{|\mathcal{P}_n^*(2p)|}{n!}$, respectively. In order to prove Theorem 1.1, we need the following recursion for $\rho_n^*(2p)$.

Proposition 2.1. Let p be an odd prime and n a positive integer. Then the proportion $\rho_n^*(2p)$ of elements with form (*) as above in S_n satisfies the following relations:

(1) if $* = I$ and $n \geq p+3$, then

$$n\rho_n^I(2p) = \rho_{n-1}^I(2p) + \rho_{n-2}(p) + \rho_{n-2}^I(2p) + \rho_{n-p}(2) + \rho_{n-p}^I(2p);$$

(2) if $* = II$ and $n \geq 2p+1$, then

$$n\rho_n^{II}(2p) = \rho_{n-1}^{II}(2p) + \rho_{n-2p}^{II}(2p) + \frac{1}{(n-2p)!};$$

(3) if $* = III$ and $n \geq 2p+3$, then

$$n\rho_n^{III}(2p) = \rho_{n-1}^{III}(2p) + \rho_{n-2}^{II}(2p) + \rho_{n-2}^{III}(2p) + \rho_{n-2p}(2) + \rho_{n-2p}^{III}(2p);$$

(4) if $* = IV$ and $n \geq 3p+1$, then

$$n\rho_n^{IV}(2p) = \rho_{n-1}^{IV}(2p) + \rho_{n-p}^{II}(2p) + \rho_{n-p}^{IV}(2p) + \rho_{n-2p}(p) + \rho_{n-2p}^{IV}(2p);$$

(5) if $* = V$ and $n \geq 3p+3$, then

$$n\rho_n^{V}(2p) = \rho_{n-1}^{V}(2p) + \rho_{n-2}^{IV}(2p) + \rho_{n-2}^{V}(2p) + \rho_{n-p}^{III}(2p) + \rho_{n-p}^{V}(2p) + \rho_{n-2p}^{I}(2p) + \rho_{n-2p}^{V}(2p).$$

Proof. (1) We partition $\mathcal{P}_n^I(2p)$ as ${}_1\mathcal{P}_n^I(2p) \cup {}_2\mathcal{P}_n^I(2p)$, where ${}_1\mathcal{P}_n^I(2p)$ and ${}_2\mathcal{P}_n^I(2p)$ consist of all elements $g \in \mathcal{P}_n^I(2p)$ such that $1^g = 1$ and $1^g \neq 1$, respectively. We observe that ${}_1\mathcal{P}_n^I(2p)$ is precisely the set of elements having form (I) in $S_\Delta \cong S_{n-1}$ where $\Delta = [n]\backslash\{1\}$, and hence $|{}_1\mathcal{P}_n^I(2p)| = (n-1)!\rho_{n-1}^I(2p)$.

It suffices to calculate ${}_2\mathcal{P}_n^I(2p)$. Since $1^g \neq 1$, 1 lies in a cycle h of g of length 2 or p for each such element g.

Case 1: h is a 2-cycle.

The number of such cycles is equal to the number $\binom{n-1}{1}$ of subsets Δ' of 1-element subsets of $\Delta\backslash\{1\}$. Then, for each of $g \in {}_2\mathcal{P}_n^I(2p)$, $g = hg'$ where $g' \in S_{[n]\backslash\{\Delta',1\}} \cong S_{n-2}$. The number of such elements g' is equal to the number $|\mathcal{P}_{n-2}^I(2p)| = (n-2)!\rho_{n-2}^I(2p)$ of elements with the form (I) in S_{n-2}, together with the number $|\mathcal{P}_{n-2}(p)| = (n-2)!\rho_{n-2}(p)$ of elements of order p in S_{n-2}. Thus

$$\begin{aligned}|{}_2\mathcal{P}_n^I(2p)| &= \tbinom{n-1}{1}((n-2)!\rho_{n-2}^I(2p) + (n-2)!\rho_{n-2}(p)) \\ &= (n-1)!(\rho_{n-2}^I(2p) + \rho_{n-2}(p)).\end{aligned}$$

Case 2: 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 $g \in {}_2\mathcal{P}_n^I(2p)$, $g = hg'$ where $g' \in S_{[n]\backslash\{\Delta',1\}} \cong S_{n-p}$. The number of such elements g' is equal to the number $|\mathcal{P}_{n-p}^I(2p)| = (n-p)!\rho_{n-p}^I(2p)$ of elements with the form (I) in S_{n-p}, together with the number $|\mathcal{P}_{n-p}(2)| = (n-p)!\rho_{n-p}(2)$ of elements of order 2 in S_{n-p}. Thus

$$\begin{aligned}|{}_2\mathcal{P}_n^I(2p)| &= \tbinom{n-1}{p-1}(p-1)!((n-p)!\rho_{n-p}^I(2p) + (n-p)!\rho_{n-p}(2)) \\ &= (n-1)!(\rho_{n-p}^I(2p) + \rho_{n-p}(2)).\end{aligned}$$

It follows that

$$\begin{aligned}n!\rho_n^I(2p) &= (n-1)!\rho_{n-1}^I(2p) + (n-1)!(\rho_{n-2}^I(2p) + \rho_{n-2}(p) + \rho_{n-p}^I(2p) + \rho_{n-p}(2)) \\ &= (n-1)!(\rho_{n-1}^I(2p) + \rho_{n-2}^I(2p) + \rho_{n-2}(p) + \rho_{n-p}^I(2p) + \rho_{n-p}(2))\end{aligned}$$

and so $n\rho_n^I(2p) = \rho_{n-1}^I(2p) + \rho_{n-2}^I(2p) + \rho_{n-2}(p) + \rho_{n-p}^I(2p) + \rho_{n-p}(2)$. This completes the proof of (1).

By the same technique as in (1), we can obtain the conclusions of (2)-(5). ∎

We now use Proposition 2.1 to give an upper bound on $\rho_n^*(2p)$ by induction on n, where $* \in \{I, II, \ldots, V\}$.

Proposition 2.2. Let p be an odd prime and n a positive integer. Then

(1) $\rho_n^I(2p) \le \frac{1}{2p}$ with equality if and only if $n = p+2$ or $p+3$;
(2) $\rho_n^{II}(2p) \le \frac{1}{2p\cdot k!}$ with equality if and only if $2p \le n \le 4p-1$, where $n = a\cdot 2p + k$ with $a \ge 0$ and $0 \le k \le 2p-1$;
(3) $\rho_n^{III}(2p) \le \frac{1}{4p}$ with equality if and only if $n = 2p+2$ or $2p+3$;
(4) $\rho_n^{IV}(2p) \le \frac{1}{2p^2\cdot k!}$ with equality if and only if $3p \le n < 4p-1$, where $n = a\cdot p + k$ with $a \ge 0$ and $0 \le k \le p-1$;
(5) $\rho_n^V(2p) \le \frac{1}{4p^2}$ with equality if and only if $n = 3p+2$ or $3p+3$.

Proof. (1) If $n < p+2$ then $\mathcal{P}_n^I(2p)$ is empty and so $\rho_n^I(2p) = 0$. If $n = p+2$ then $|\mathcal{P}_n^I(2p)| = \frac{n!}{2p}$ and so $\rho_n^I(2p) = \frac{1}{2p}$. We now assume that $n \ge p+3$ and assume inductively that the result holds for all positive integers strictly less than n.

Let $n = ap+k$ where $a \ge 0$ and $0 \le k \le p-1$. Then $n-2 = a\cdot p+k-2$ if $2 \le k \le p-1$, and $n-2 = (a-1)\cdot p + p + k - 2$ if $k = 0$ or 1.

Case 1: $a = 1$ and $3 \le k \le p-1$.

If $k = 3$, then by induction we have $\rho_{n-1}^I(2p) = \frac{1}{2p}$, $\rho_{n-2}^I(2p) = 0$ and $\rho_{n-p}^I(2p) = 0$, and we note that $\rho_{n-2}(p) = \frac{1}{p}$ and $\rho_{n-p}(2) = \frac{1}{2}$ by [7, Theorem 1]. Thus by Proposition 2.1 (1),

$$\begin{aligned}\rho_n^I(2p) &= \frac{1}{n}(\rho_{n-1}^I(2p) + \rho_{n-2}^I(2p) + \rho_{n-2}(p) + \rho_{n-p}^I(2p) + \rho_{n-p}(2))\\ &= \frac{1}{n}(\frac{1}{2p} + 0 + \frac{1}{p} + 0 + \frac{1}{2}) = \frac{1}{2p}.\end{aligned}$$

Similarly, if $4 \le k \le p-1$, then by induction we observe that $\rho_{n-1}^I(2p) \le \frac{1}{2p}$, $\rho_{n-2}^I(2p) \le \frac{1}{2p}$ and $\rho_{n-p}^I(2p) = 0$, and we see that $\rho_{n-2}(p) \le \frac{1}{p\cdot(k-2)!}$ and $\rho_{n-p}(2) \le \frac{1}{2}$ by [7, Theorem 1]. So by Proposition 2.1 (1),

$$\begin{aligned}\rho_n^I(2p) &\le \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(k-2)!} + 0 + \frac{1}{2})\\ &= \frac{1}{2p}\cdot\frac{1+1+\frac{2}{(k-2)!}+p}{n}\\ &\le \frac{1}{2p}\cdot\frac{1+1+1+p}{n} < \frac{1}{2p}.\end{aligned}$$

Case 2: $a \ge 2$ and $0 \le k \le p-1$.

Subcase 2.1: $k = 0$.

If $a = 2$ and $p = 3$, then by induction we have $\rho_{n-1}^I(2p) = \frac{1}{2p}$, $\rho_{n-2}^I(2p) = 0$ and $\rho_{n-p}^I(2p) = 0$, and we note that $\rho_{n-2}(p) = \frac{1}{p}$ and $\rho_{n-p}(2) = \frac{1}{2}$ by [7, Theorem 1]. Hence by Proposition 2.1 (1),

$$\rho_n^I(2p) = \frac{1}{n}(\frac{1}{2p} + 0 + \frac{1}{p} + 0 + \frac{1}{2}) = \frac{1}{2p}.$$

If $a = 2$ and $p \geq 5$, then by induction we observe that $\rho^I_{n-1}(2p) \leq \frac{1}{2p}$, $\rho^I_{n-2}(2p) \leq \frac{1}{2p}$ and $\rho^I_{n-p}(2p) = 0$, and we see that $\rho_{n-2}(p) = \frac{1}{p\cdot(p-2)!}$ and $\rho_{n-p}(2) < \frac{1}{2}$ by [7, Theorem 1]. Therefore by Proposition 2.1 (1),

$$\begin{aligned}\rho^I_n(2p) &< \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(p-2)!} + 0 + \frac{1}{2}) \\ &= \frac{1}{2p}\cdot\frac{p+2+\frac{2}{(p-2)!}}{n} < \frac{1}{2p}.\end{aligned}$$

Similarly, if $a \geq 3$, then by induction we have $\rho^I_{n-1}(2p) \leq \frac{1}{2p}$, $\rho^I_{n-2}(2p) \leq \frac{1}{2p}$ and $\rho^I_{n-p}(2p) \leq \frac{1}{2p}$, and we note that $\rho_{n-2}(p) < \frac{1}{p\cdot(p-2)!}$ and $\rho_{n-p}(2) < \frac{1}{2}$ by [7, Theorem 1]. Thus by Proposition 2.1 (1),

$$\begin{aligned}\rho^I_n(2p) &< \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(p-2)!} + \frac{1}{2p} + \frac{1}{2}) \\ &= \frac{1}{2p}\cdot\frac{p+3+\frac{2}{(p-2)!}}{n} < \frac{1}{2p}.\end{aligned}$$

Subcase 2.2: $k = 1$.

If $a = 2$, then by induction we observe that $\rho^I_{n-1}(2p) \leq \frac{1}{2p}$, $\rho^I_{n-2}(2p) \leq \frac{1}{2p}$ and $\rho^I_{n-p}(2p) = 0$, and we see that $\rho_{n-2}(p) = \frac{1}{p\cdot(p-1)!}$ and $\rho_{n-p}(2) < \frac{1}{2}$ by [7, Theorem 1]. Therefore by Proposition 2.1 (1),

$$\begin{aligned}\rho^I_n(2p) &< \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(p-1)!} + 0 + \frac{1}{2}) \\ &= \frac{1}{2p}\cdot\frac{p+2+\frac{2}{(p-1)!}}{n} < \frac{1}{2p}.\end{aligned}$$

Similarly, if $a \geq 3$, then by induction we have $\rho^I_{n-1}(2p) \leq \frac{1}{2p}$, $\rho^I_{n-2}(2p) \leq \frac{1}{2p}$ and $\rho^I_{n-p}(2p) \leq \frac{1}{2p}$, and we note that $\rho_{n-2}(p) < \frac{1}{p\cdot(p-1)!}$ and $\rho_{n-p}(2) < \frac{1}{2}$ by [7, Theorem 1]. So by Proposition 2.1 (1),

$$\begin{aligned}\rho^I_n(2p) &< \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(p-1)!} + \frac{1}{2p} + \frac{1}{2}) \\ &= \frac{1}{2p}\cdot\frac{p+3+\frac{2}{(p-1)!}}{n} < \frac{1}{2p}.\end{aligned}$$

Subcase 2.3: $k \geq 2$.

In this subcase, we have $\rho^I_{n-1}(2p) \leq \frac{1}{2p}$, $\rho^I_{n-2}(2p) \leq \frac{1}{2p}$ and $\rho^I_{n-p}(2p) \leq \frac{1}{2p}$ by induction, and we see that $\rho_{n-2}(p) < \frac{1}{p\cdot(k-2)!}$ and $\rho_{n-p}(2) < \frac{1}{2}$ by [7, Theorem 1]. Hence by Proposition 2.1 (1),

$$\begin{aligned}\rho^I_n(2p) &< \frac{1}{n}(\frac{1}{2p} + \frac{1}{2p} + \frac{1}{p\cdot(k-2)!} + \frac{1}{2p} + \frac{1}{2}) \\ &= \frac{1}{2p}\cdot\frac{p+3+\frac{2}{(k-2)!}}{n} \leq \frac{1}{2p}.\end{aligned}$$

So we have completed the proof of (1) by induction.

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

Note that $n - 2p = (a-1)\cdot 2p + k$, $n - 1 = a \cdot 2p + k - 1$ if $1 \leq k \leq 2p-1$, and $n - 1 = (a-1)\cdot 2p + 2p - 1$ if $k = 0$.

Case 1: $a = 1$.

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

$$\begin{aligned}\rho_n^{II}(2p) &= \frac{1}{n}\left(\frac{1}{2p\cdot(k-1)!} + 0 + \frac{1}{k!}\right)\\ &= \frac{2p+k}{2p\cdot n\cdot k!} = \frac{1}{2p\cdot k!}.\end{aligned}$$

Case 2: $a \geq 2$.

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

$$\begin{aligned}\rho_n^{II}(2p) &\leq \frac{1}{n}\left(\frac{1}{2p\cdot(2p-1)!} + \frac{1}{2p} + \frac{1}{(n-2p)!}\right)\\ &= \frac{1}{2np}\left(\frac{1}{(2p-1)!} + 1 + \frac{2p}{(n-2p)!}\right) < \frac{3}{2np} < \frac{1}{2p}.\end{aligned}$$

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

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

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

For (3)-(5), the proofs are analogous to the proofs of (1) and (2). ∎

We now use Proposition 2.2 to prove Theorem 1.1.

Proof of Theorem 1.1: Let n be a positive integer and p an odd prime, and write $n = a\cdot 2p + k$ where $0 \leq k \leq 2p-1$ and $a \geq 0$.

If $n < p+2$, then $\mathcal{P}_n(2p)$ is empty, and so $\rho_n(2p) = 0$.

If $p+2 \leq n \leq 2p-1$, then $\mathcal{P}_n(2p) = \mathcal{P}_n^I(2p)$, and thus $\rho_n(2p) = \rho_n^I(2p) \leq \frac{1}{2p}$ with equality if and only if $n = p+2$ or $p+3$ by Proposition 2.2 (1).

If $2p \leq n \leq 2p+1$, then $\mathcal{P}_n(2p) = \mathcal{P}_n^I(2p) + \mathcal{P}_n^{II}(2p)$, and thus $\rho_n(2p) = \rho_n^I(2p) + \rho_n^{II}(2p) < \frac{1}{2p} + \frac{1}{2p} = \frac{1}{p}$ by Proposition 2.2 (1) and (2).

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

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

If $n \geq 3p+2$, then $\mathcal{P}_n(2p) = \mathcal{P}_n^I(2p) + \mathcal{P}_n^{II}(2p) + \mathcal{P}_n^{III}(2p) + \mathcal{P}_n^{IV}(2p) + \mathcal{P}_n^V(2p)$, and thus $\rho_n(2p) < \frac{1}{2p} + \frac{1}{2p\cdot k!} + \frac{1}{4p} + \frac{1}{2p^2\cdot k!} + \frac{1}{4p^2} = \frac{(3p+1)k!+2p+2}{4p^2\cdot k!}$ by Proposition 2.2 (1) to (5), where $0 \leq k \leq p-1$.

If $n \geq 3p+2$, then $\mathcal{P}_n(2p) = \mathcal{P}_n^I(2p) + \mathcal{P}_n^{II}(2p) + \mathcal{P}_n^{III}(2p) + \mathcal{P}_n^{IV}(2p) + \mathcal{P}_n^V(2p)$, and thus $\rho_n(2p) < \frac{1}{2p} + \frac{1}{2p\cdot k!} + \frac{1}{4p} + \frac{1}{2p^2\cdot (k-p)!} + \frac{1}{4p^2} = \frac{[(3p+1)k!+2p](k-p)!+2k!}{4p^2\cdot k!(k-p)!}$ by Proposition 2.2 (1) to (5), where $p \leq k \leq 2p-1$. ∎

From the results in Theorem 1.1 on the proportion of elements of order twice a prime in finite symmetric groups, we can observe an interesting phenomenon: the upper bound of the proportion is controlled by a function f defined on $[2p-1] = \{0, 1, 2, \cdots, 2p-1\}$. This motivates the following natural problem:

Problem 1. Find an upper bound on the proportion $\rho_n(pq)$ of elements of order pq in S_n, where p and q are distinct odd primes.

We will work on Problem 1 in a later paper in this series papers.

Acknowledgment. This work was partially supported by China Scholarship Council (202208360148), National Natural Science Foundation of China (12126415,12261042,12301026), Jiangxi Provincial Natural Science Foundation (20232BAB211006), and the Science and Technology Research Project of Jiangxi Education Department (GJJ2200841).

References

[1] S. Chowla, I. N. Herstein and W. R. Scott, *The solutions of $x^d = 1$ in symmetric groups*, Norske Vid. Selsk. Forh. Trondheim **25**, 29-31, 1952.

[2] S. P. Glasby, C. E. Praeger and W. R. Unger, *Most permutations power to a cycle of small prime length*, Proc. Edinburgh Math. Soc. **64**, 234-246, 2021.

[3] E. Jacobsthal, *Sur le nombre d'éléments du groupe symétrique* S_n *dont l'ordre est un nombre premier*, Norske Vid. Selsk. Forh. Trondheim **21** (12), 49-51, 1949.

[4] L. Moser and M. Wyman, *On solutions of $x^d = 1$ in symmetric groups*, Canad. J. Math. **7**, 159-168, 1955.

[5] A. C. Niemeyer, T. Popiel and C. E. Praeger, *On proportions of pre-involutions in finite classical groups*, J. Algebra **324**, 1016-1043, 2010.

[6] A. C. Niemeyer, C. E. Praeger and A. Seress, *Estimation problems and randomised group algorithms*, In Probabilistic Group Theory, Combinatorics and Computing, Editors: Alla Detinko, Dane Flannery and Eamonn O'Brien. Lecture Notes in Mathematics, Volume **2070** Chapter 2, 35-82 Springer, Berlin,2020.

[7] C. E. Praeger and E. Suleiman, *On the proportion of elements of prime order in finite symmetric groups*, Int. J. Group Theory **13**, 251-256, 2024.