http://ijgt.ui.ac.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. x No. x (202x), pp. xx-xx.

www.ui.ac.ir

ON THE PROPORTION OF ELEMENTS OF PRIME ORDER IN FINITE SYMMETRIC GROUPS

CHERYL E. PRAEGER* AND ENOCH SULEIMAN

Dedicated to Daniela Nikolva
on the occasion of her 70^{th} *birthday.*

Abstract. We give a short proof for an explicit upper bound on the proportion of permutations of a given prime order p, acting on a set of given size n, which is sharp for certain n and p. Namely, we prove that if $n \equiv k \pmod{p}$ with $0 \leq k \leq p-1$, then this proportion is at most $(p \cdot k!)^{-1}$ with equality if and only if $p \leq n < 2n$.

1. Introduction

The proportion $\rho_p(n)$ of permutations of a given prime order p and acting on a set of given size n has been extensively studied. In particular, for fixed p as n grows, recursive formulas and an asymptotic expansion have been known for more than 70 years, first by Jacabsthal [5] in 1949 who, in particular, gave the following explicit formula:

$$\rho_p(n) = \sum_{i=1}^{[n/p]} \frac{1}{(n-ip)!i!p^i}. \tag{1.1}$$

Communicated by Patrizia Longobardi.

MSC(2010): Primary: 20B30; Secondary: 05A05.

Keywords: Finite symmetric groups, element proportions, elements of prime order.

Article Type: 2022 CCGTA IN SOUTH FLA.

Received: 25 October 2022, Accepted: 08 April 2023.

*Corresponding author.

http://dx.doi.org/10.22108/ijgt.2023.135509.1810 .

The reader may recognise the denominator of the summand for i as the centraliser order of a permutation with i cycles of length p and $n - ip$ fixed points. Extensions of [5] were obtained in the early 1950s by Chowla, Herstein and Scott [3] and Moser and Wyman [7]. We give a brief discussion of these results in Section 1.1.

It may not be immediately obvious, from the expression (1.1), what upper or lower bounds for $\rho_p(n)$ apply. Our interest is in explicit estimates, especially upper bounds, even if they are not asymptotically best possible. The simple upper bounds we obtain in our main result Theorem 1.1 are sharp for certain n, p. Such explicit estimates are relevant in discussing various group theoretic algorithms, which we mention briefly in Section 1.2.

Theorem 1.1. *Let p be a prime and n a positive integer, and write $n = ap + k$ where $a \geq 0$ and $0 \leq k < p$. Then the proportion $\rho_p(n)$ of elements of order p in the symmetric group S_n satisfies*

$$\rho_p(n) \leq \frac{1}{p \cdot k!} \quad \textit{with equality if and only if } p \leq n < 2p.$$

Theorem 1.1 is proved in Section 2.

1.1. **Asymptotic estimates.** Let p be a prime and n an integer such that $n \geq p$. Let $\rho_p^*(n)$ be the proportion of elements in the symmetric group S_n of order dividing p, that is to say, elements $x \in S_n$ such that $x^p = 1$. Thus $\rho_p^*(n) = \rho_p(n) + 1/n!$. The proportions $\rho_p^*(n)$ and $\rho_p(n)$ have been extensively studied in the literature, even when p is not prime, and asymptotic results are available which determine the value, when p is fixed and n is unbounded. The original result of Jacobstahl [5] from 1949 gives the following expression for $\rho_p(n)$, and also a generating function for $\rho_p(n)$, for a prime p.

$$\rho_p(n) = \sum_{i=1}^{[n/p]} \frac{1}{(n-ip)!i!p^i}, \quad \text{and} \quad \sum_{n=1}^{\infty} \rho_p(n)x^n = \exp(x)(\exp(x^p/p) - 1).$$

While this expression for $\rho_p(n)$ could have been applied to obtain our result in Theorem 1.1, we believe that the short inductive proof we provide is helpful, yielding a useful bound for several applications.

Several years after Jacobstahl's work appeared, Moser and Wyman [7, (3.41)] obtained the following asymptotic expression for $\rho_p^*(n)$ for p an odd prime:

$$\rho_p^*(n) \sim \frac{1}{\sqrt{p} \cdot n!} \left(\frac{n}{e}\right)^{n(1-1/p)} e^{n^{1/p}}$$

which, in the light of Stirling's formula $n! \sim (2\pi n)^{1/2} \cdot (n/e)^n$, shows that for fixed p as n grows, $\rho_p^*(n) \sim n^{-n/p}$. There are many similar asymptotic results, for example, where the primality condition on p is removed, see in particular the paper of Wilf [10]. A helpful survey of these results is included in [9, Section 2.2.6] or the explicit bounds in [1]. Most of these estimates are asymptotic, whereas it is sometimes preferable to have explicit upper and/or lower bounds for such proportions.

http://dx.doi.org/10.22108/ijgt.2023.135509.1810

1.2. **Some algorithmic considerations.** For computational purposes a finite group G may be given as a group of permutations or a group of matrices over a finite field, usually by specifying a small generating set $G = \langle X \rangle$. We may know, or suspect, that G is isomorphic to a group such as S_n, and we may wish to prove or exploit this computationally. Algorithms to recognise G, or to construct a standard generating set for G, typically seek special kinds of elements. These elements are usually sought, or constructed from, randomly selected elements, and to understand the complexity of such searches we need estimates for the proportions of various kinds of elements in the group.

For example, in [2], as part of constructing a standard generating set for a 'black-box group' G isomorphic to S_n, a transposition was constructed by searching, via random selection, for an element $b \in G$ of order $2f$ for some odd positive integer $f \leq n^{18 \log n}$, such that b^f corresponds to a transposition in S_n. The choice of the upper bound $n^{18 \log n}$ for f was chosen so that the proportion of such elements was large enough to find such an element b with high probability (at least $0.318n^{1/2}$ for $n \geq 5$, [2, Theorem 5.1(a)]), and also to construct the transposition b^f at a reasonable cost, [2, Proposition 6.1]. The benefit of this method over a direct search for a transposition, by examining random elements, is obvious as the proportion of transpositions is only $(2 \cdot (n-2)!)^{-1}$. The paper [2] contains an analogous analysis for construction of 3-cycles in alternating groups. More details about algorithmic applications of proportions of elements in symmetric groups are given in [9, Section 2.2.8].

Let us turn now to primes larger than 2 or 3. Just as transpositions and 3-cycles can be constructed by taking powers of elements with a single cycle of length x and all other cycles of length coprime to x (where $x = 2$ or 3) so also, for any prime p, we can construct a *p-cycle* (that is, a permutation with one cycle of length p and fixing all other points) by taking an appropriate power of a permutation g which has a single cycle of length p and all other cycles of length coprime to p. Such elements g are called *pre-p-cycles*, and are useful for algorithms involving both permutation groups and classical matrix groups (see for example [4, 6, 8]). Let $s_{\neg p}(n)$ denote the proportion of elements of S_n with no cycle length divisible by p, equivalently the proportion of *p-regular* elements – permutations with order coprime to p. It was proved in [8, Lemma 3.1(ii)] that the proportion of pre-p-cycles in S_n is $s_{\neg p}(n-p)/p$, and explicit upper and lower bounds for $s_{\neg p}(n-p)$ were obtained in [2, Theorem 2.3b], with simpler bounds derived in [6, Lemma 4.2] and [8, Lemma 3.1(i)]. These bounds imply that the proportion of pre-p-cycles in S_n lies between

$$\frac{1}{4p \cdot (n-p)^{1/p}} \quad \text{and} \quad \frac{3}{p \cdot (n-p)^{1/p}}.$$

This is far greater than the proportion of p-cycles, namely $(p \cdot (n-p)!)^{-1}$.

Along the same lines, we note that the proportion of *p-singular* elements of S_n, that is to say, elements with order a multiple of p, is $1 - s_{\neg p}(n)$ which, by our comments above, is greater than $1 - 3n^{-1/p}$. The simple upper bound given in Theorem 1.1 shows that the proportion of p-singular elements of S_n is far greater than $\rho_p(n)$. This is an easy confirmation that constructing elements of

http://dx.doi.org/10.22108/ijgt.2023.135509.1810

order p by taking powers of p-singular elements is much more efficient than searching for such elements directly by random selection.

2. Proof of the main theorem

Let n be a positive integer, and let $\Omega = \{1, \ldots, n\}$ and $\mathrm{Sym}(\Omega)$ be the symmetric group S_n on Ω. Let $\mathcal{P}(n,p)$ denote the subset of $\mathrm{Sym}(\Omega)$ consisting of all the elements of order p, so that

$$\rho_p(n) := \frac{|\mathcal{P}(n,p)|}{n!}. \tag{2.1}$$

First we record some basic facts.

Lemma 2.1. *Let $n, p, \Omega, \mathcal{P}(n,p)$ and $\rho_p(n)$ be as above.*

(a) *If $n < p$ then $\rho_p(n) = 0$, and $\rho_p(p) = 1/p$.*

(b) *If $n \geq p$, then, for each subset $\Delta \subseteq \Omega$ with $|\Delta| = p$, there are exactly $(p-1)!$ distinct p-cycles permuting the points of Δ (that is, p-cycles in $\mathrm{Sym}(\Delta)$).*

Proof. If $n < p$ then $\mathcal{P}(n,p)$ is empty and $\rho_p(n) = 0$. So assume that $n \geq p$ and let $\Delta = \{\delta_1, \ldots, \delta_p\}$ be a p-element subset of Ω. Each p-cycle in $\mathrm{Sym}(\Delta)$ has a unique expression of the form $(\delta_1, \alpha_2, \ldots, \alpha_p)$ where $\alpha_2, \ldots, \alpha_p$ are precisely the points in $\Delta \setminus \{\delta_1\} = \{\delta_2, \ldots, \delta_p\}$ in some order. There are exactly $(p-1)!$ ways to order $\{\delta_2, \ldots, \delta_p\}$ and hence exactly $(p-1)!$ distinct p-cycles permuting the points of Δ. In particular, if $n = p$ then $\Omega = \Delta$, and we have therefore just shown that $|\mathcal{P}(p,p)| = (p-1)!$, so $\rho_p(p) = |\mathcal{P}(p,p)|/p! = 1/p$. □

We note that Lemma 2.1 proves Theorem 1.1 for n such that $1 \leq n \leq p$. The main proof will be by induction on n with these as the 'base cases'. It will use the following recursion for $\rho_p(n)$.

Lemma 2.2. *Let p be a prime and n an integer such that $n \geq p+1$. Then*

$$n \cdot \rho_p(n) = \rho_p(n-1) + \rho_p(n-p) + \frac{1}{(n-p)!}.$$

Proof. By (2.1), $|\mathcal{P}(n,p)| = n!\rho_p(n)$ for each positive integer n. We establish the recursion by enumerating $\mathcal{P}(n,p)$ as follows. We partition $\mathcal{P}(n,p)$ as $\mathcal{P}_1(n,p) \cup \mathcal{P}_2(n,p)$, where $\mathcal{P}_1(n,p)$ consists of all elements $g \in \mathcal{P}(n,p)$ such that $1^g = 1$, and $\mathcal{P}_2(n,p)$ consists of all elements $g \in \mathcal{P}(n,p)$ such that $1^g \neq 1$. Now $\mathcal{P}_1(n,p)$ is precisely the set of elements of order p in $\mathrm{Sym}(\Delta)$, where $\Delta = \{2, 3, \ldots, n\}$ and hence $|\mathcal{P}_1(n,p)| = (n-1)!\rho_p(n-1)$, by (2.1).

Consider now the complement $\mathcal{P}_2(n,p)$. To enumerate the elements of $\mathcal{P}_2(n,p)$, we note that, for each such element g, the point 1 lies in a cycle h of g of length p, since $1^g \neq 1$. The number of such cycles is equal to the number $\binom{n-1}{p-1}$ of $(p-1)$-element subsets Δ' of $\Omega \setminus \{1\}$ such that the p-cycle h permutes the points of $\Delta := \Delta' \cup \{1\}$, times the number $(p-1)!$ of p-cycles in $\mathrm{Sym}(\Delta)$ (using Lemma 2.1(b)). Then, for each of these $\binom{n-1}{p-1}(p-1)!$ cycles, say h on a subset Δ containing the point 1, the elements $g \in \mathcal{P}_2(n,p)$ which have h as a p-cycle are precisely the permutations $g = hg'$ where g'

http://dx.doi.org/10.22108/ijgt.2023.135509.1810

is an element of $\mathrm{Sym}(\Omega \setminus \Delta) = S_{n-p}$ of order dividing p. The number of such elements g' is equal to the number $|\mathcal{P}(n-p,p)| = (n-p)!\rho_p(n-p)$ of elements of S_{n-p} of order p, together with the identity element. Thus

$$\begin{aligned}|\mathcal{P}_2(n,p)| &= \binom{n-1}{p-1}(p-1)!\left((n-p)!\,\rho_p(n-p)+1\right)\\ &= (n-1)!\left(\rho_p(n-p)+\frac{1}{(n-p)!}\right),\end{aligned}$$

and the recursion $n\cdot\rho_p(n) = \rho_p(n-1)+\rho_p(n-p)+\frac{1}{(n-p)!}$ follows. □

We now use Lemma 2.1 and 2.2 to prove Theorem 1.1.

Proof of Theorem 1.1. Let n be a positive and let a, k be the (unique) integers such that $n = ap+k$ where $a \geq 0$ and $0 \leq k \leq p-1$. We refer to this expression as the 'quotient and remainder' representation for n. We will prove that

$$\rho_p(n) \leq \frac{1}{p\cdot k!} \quad \text{with equality if and only if } p \leq n < 2p.$$

This assertion follows from Lemma 2.1(a) if $n \leq p$, so assume that $n \geq p+1$, and assume inductively that the result holds for all integers strictly less than n. Then, by Lemma 2.2,

$$\rho_p(n) = \frac{\rho_p(n-1)}{n} + \frac{\rho_p(n-p)}{n} + \frac{1}{n\cdot(n-p)!}$$

Now the quotient and remainder representations for $n-p$ and $n-1$ are $n-p = (a-1)p+k$, and $n-1 = ap+(k-1)$ if $1 \leq k \leq p-1$ and $n-1 = (a-1)p+(p-1)$ if $k = 0$.

Suppose first that $p+1 \leq n \leq 2p-1$, that is to say, $a = 1$ and $1 \leq k \leq p-1$. Then $n-p = k < p$ so $\rho_p(n-p) = 0$ by Lemma 2.1(a), and by induction, $\rho_p(n-1) = 1/(p\cdot(k-1)!)$. Thus

$$\rho_p(n) = \frac{1}{np\cdot(k-1)!} + 0 + \frac{1}{n\cdot k!} = \frac{k+p}{np\cdot k!} = \frac{1}{p\cdot k!}.$$

Thus we may assume that $n \geq 2p$. If $k > 0$ then, by induction, $\rho_p(n-1) \leq 1/(p\cdot(k-1)!)$ and $\rho_p(n-p) \leq 1/(p\cdot k!)$, so that

$$\rho_p(n) \leq \frac{1}{np\cdot(k-1)!} + \frac{1}{np\cdot k!} + \frac{1}{n\cdot(n-p)!} = \frac{k+1+p\cdot k!/(n-p)!}{np\cdot k!}.$$

Since $n-p \geq p \geq k+1$, we have $p\cdot k!/(n-p)! \leq 1$, and so the numerator $k+1+p\cdot k!/(n-p)! \leq k+2 \leq p+1 < n$, so $\rho_p(n) < 1/(p\cdot k!)$. Suppose finally that $n \geq 2p$ and $k = 0$, that is, $n = ap$ with $a \geq 2$. Then, by induction, $\rho_p(n-p) \leq 1/p$ and $\rho_p(n-1) \leq 1/(p\cdot(p-1)!) = 1/p!$. Thus

$$\rho_p(n) \leq \frac{1}{n\cdot p!} + \frac{1}{np} + \frac{1}{n\cdot(n-p)!} = \frac{1}{np}\left(\frac{1}{(p-1)!} + 1 + \frac{p}{(n-p)!}\right).$$

Since $n-p \geq p$ we have $p/(n-p)! \leq 1/(p-1)!$ and so

$$\rho_p(n) \leq \frac{1}{np}\left(\frac{2}{(p-1)!}+1\right) \leq \frac{3}{np} < \frac{1}{p},$$

which completes the proof by induction of Theorem 1.1.

http://dx.doi.org/10.22108/ijgt.2023.135509.1810

Acknowledgments

The first author acknowledges funding from Australian Research Council Discovery Project grant DP190100450. The authors thank an anonymous referee for advice on the exposition, and carefully reading our manuscript.

References

[1] J. Bamberg, S. P. Glasby, S. Harper and C. E. Praeger, Permutations with orders coprime to a given integer, *Electronic J. Combin.*, **27** (2020) 14 pp.

[2] R. Beals, Charles R. Leedham-Green, A. C. Niemeyer, C. E. Praeger and Á. Seress, Permutations with restricted cycle structure and an algorithmic application, *Combin. Probab. Comput.*, **11** (2002) 447–464.

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

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

[5] 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** (1949) 49–51.

[6] F. Lübeck, A. C. Niemeyer and C. E. Praeger, Finding involutions in finite Lie type groups of odd characteristic, *J. Algebra*, **321** (2009) 3397–3417.

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

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

[9] A. C. Niemeyer, C. E. Praeger and Á. 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, Springer, Berlin, **2070** 2020 35–82.

[10] H. S. Wilf, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc. (N.S.)*, **15** (1986) 228–232.

Cheryl E. Praeger

Centre for the Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, Perth 6009, Australia

Email: cheryl.praeger@uwa.edu.au

Enoch Suleiman

Department of Mathematics, Federal University Gashua, Yobe State, Gashua, Nigeria

Email: enochsuleiman@gmail.com

http://dx.doi.org/10.22108/ijgt.2023.135509.1810