Permutations with orders coprime to a given integer

John Bamberg

Centre for the Mathematics of Symmetry and Computation,
Department of Mathematics and Statistics,
University of Western Australia, Australia.

john.bamberg@uwa.edu.au

S. P. Glasby

Centre for the Mathematics of Symmetry and Computation,
Department of Mathematics and Statistics,
University of Western Australia, Australia.

stephen.glasby@uwa.edu.au

Scott Harper

School of Mathematics,
The University of Bristol, United Kingdom.

scott.harper@bristol.ac.uk

Cheryl E. Praeger

Centre for the Mathematics of Symmetry and Computation,
Department of Mathematics and Statistics,
University of Western Australia, Australia.

cheryl.praeger@uwa.edu.au

Submitted: Apr 20, 2019; Accepted: Dec 3, 2019; Published: Jan 10, 2020

Abstract

Let m be a positive integer and let $\rho(m,n)$ be the proportion of permutations of the symmetric group $\mathrm{Sym}(n)$ whose order is coprime to m. In 2002, Pouyanne proved that $\rho(n,m)n^{1-\frac{\phi(m)}{m}} \sim \kappa_m$ where κ_m is a complicated (unbounded) function of m. We show that there exists a positive constant $C(m)$ such that, for all $n \geqslant m$,

$$C(m)\left(\frac{n}{m}\right)^{\frac{\phi(m)}{m}-1} \leqslant \rho(n,m) \leqslant \left(\frac{n}{m}\right)^{\frac{\phi(m)}{m}-1}$$

where ϕ is Euler's totient function.

Mathematics Subject Classifications: 20B30, 05A15, 68W20.

1 Introduction

In a series of papers between 1965 and 1972, Erdős and Turán initiated a systematic study of probabilistic aspects of group theory (see, for example, [7]). One topic which has been of particular interest since this time is the distribution of element orders in finite symmetric groups, and their most relevant work for us on this topic began in [8, 9] where they studied the proportion $p_{\neg m}(n)$ of elements in $\mathrm{Sym}(n)$ with no cycle of length divisible by a fixed prime m. Erdős and Turán obtained an explicit formula for $p_{\neg m}(n)$ and determined the limiting proportion, as n grows, as

$$(1) \qquad p_{\neg m}(n) = k(m)\left(\frac{n}{m}\right)^{-\frac{1}{m}} + O(n^{-1-\frac{1}{m}}),$$

where $k(m) = \Gamma\left(1-\frac{1}{m}\right)^{-1}$, noting that $\pi^{-1/2} \leqslant k(m) < 1$ [8, Sections 3 and 4]. Although m was assumed to be a prime in [8], the formula for $p_{\neg m}(n)$ in (1) holds for an arbitrary positive integer m, see [11], and their asymptotic arguments can be extended to give explicit convergence bounds [3, Theorem 2.3(b)], again for arbitrary m. These explicit bounds, together with analogous results for alternating groups [3, Section 3], were used to analyse algorithms for constructing transpositions and 3-cycles [3, Section 6], procedures used as components of the constructive recognition algorithms for black-box alternating and symmetric groups in [4]. Many other authors have also considered the proportion $p_{\neg m}(n)$, see for example [5, 6, 16] and the discussion in [17].

Let us introduce the specific topic of interest for this paper. For positive integers n and m, let $R(n,m)$ be the set of elements of $\mathrm{Sym}(n)$ whose order is coprime to m, and write

$$\rho(n,m) := \frac{|R(n,m)|}{n!}.$$

The proportion $\rho(n,m)$ is equal to the proportion $p_{\neg m}(n)$ of Erdős and Turán discussed above if and only if m is a prime power. Moreover, in [8, Lemma II], Erdős and Turán demonstrate that if n is sufficiently large and m is the product of two distinct primes p and q satisfying $(\log n)^{3/4} \leqslant p, q \leqslant 10\log n/\log\log n$, then

$$(2) \qquad \rho(n,m) = n^{-\frac{1}{p}-\frac{1}{q}}(1 + O(\log^{-\frac{1}{2}} n)).$$

Pouyanne [19, Proposition, p. 7] used a singularity analysis on the generating function $C(x) = \sum_{i\geqslant 0} \rho(n,m)X^m$ for $\rho(n,m)$ to give an asymptotic value of $\rho(n,m)$ for arbitrary m. He gives a nice proof that $\rho(n,m)n^{1-\phi(m)/m} \sim \kappa_m$ where κ_m is a function of m involving Gamma and Möbius functions, see (12). Unfortunately the elusive nature [19, Figure 1] of κ_m makes it hard to apply this result. In particular, upper and lower bounds $\rho(n,m)$ cannot be extracted from the asymptotics in [19], and our major contribution is to bound the quantity $\lambda_m := \kappa_m/m^{1-\phi(m)/m}$, where ϕ is Euler's totient function. We need these bounds for applications to randomised (1-sided Monte Carlo) permutation group algorithms where explicit bounds on the probability/proportions are required to assign explicit upper bounds on the probability that the algorithm returns an incorrect answer, i.e. to prove that it is a Monte Carlo algorithm. Examples of the use of such probability bounds for exhibiting a Monte Carlo algorithm, and analysing its complexity, are given for example in [4]. Specifically, our algorithm for testing whether a subgroup $\langle X\rangle$ of $\mathrm{Sym}(n)$ contains the alternating group $\mathrm{Alt}(n)$ either returns the answer "Yes" with no chance of error, or returns an answer "No" with a (preset arbitrarily) small probability of error, say 10^{-6}.

The set $\pi(m)$ of prime divisors of m is significant as $\rho(n,m)=\rho(n,m')$ and $\phi(m)/m = \phi(m')/m'$ when $\pi(m)=\pi(m')$. Given this fact, we will henceforth assume that m is *square-free*. We implicitly also assume that the primes in $\pi(m)$ are at most n, since $\rho(n,m)=\rho(n,mp)$ for primes $p>n$. With this in mind, and observing that $\frac{\phi(m)}{m}-1\leqslant 0$, we now present our main result.

Theorem 1. *Let m be a positive square-free integer. There exists a positive constant $C(m)$ such that, for all $n\geqslant m$,*

$$C(m)\left(\frac{n}{m}\right)^{\frac{\phi(m)}{m}-1}\leqslant \rho(n,m)\leqslant \left(\frac{n}{m}\right)^{\frac{\phi(m)}{m}-1}.$$

The exponent $\frac{\phi(m)}{m}-1$ in Theorem 1 is negative, and hence $\lceil\frac{n}{m}\rceil^{\frac{\phi(m)}{m}-1}\leqslant(\frac{n}{m})^{\frac{\phi(m)}{m}-1}$ and $\lfloor\frac{n}{m}\rfloor^{\frac{\phi(m)}{m}-1}\geqslant(\frac{n}{m})^{\frac{\phi(m)}{m}-1}$, for $n\geqslant m$. Thus, in order to prove Theorem 1 it is sufficient to prove that

$$C(m)\left\lfloor\frac{n}{m}\right\rfloor^{\frac{\phi(m)}{m}-1}\leqslant \rho(n,m)\leqslant \left\lceil\frac{n}{m}\right\rceil^{\frac{\phi(m)}{m}-1}. \tag{3}$$

We prove these inequalities in Section 2. In fact the upper bound holds for $n\geqslant 1$. We conclude with a conjecture in Section 3 based on computational evidence.

First we make a few remarks concerning the constant $C(m)$ and links between Theorem 1 and the results (1) and (2).

Remark 2.

(a) We prove Theorem 1 with the constant

$$C(m) := \min\{\rho(n,m)\mid m\leqslant n\leqslant 2m-1\}. \tag{4}$$

In particular, if m is a prime then $C(m)=1-\frac{1}{m}$.

(b) If an element of $\mathrm{Sym}(n)$ has order coprime to m, then the length of each of its cycles is certainly not divisible by m. Hence, we have the upper bound $\rho(n,m)\leqslant p_{\neg m}(n)=\prod_{i=1}^{\lfloor\frac{n}{m}\rfloor}(1-\frac{1}{im})$ by [11]. However, this bound grows too quickly as remarked on in (c).

(c) If m is prime, then the exponent is $\frac{\phi(m)}{m}-1=\frac{m-1}{m}-1=-\frac{1}{m}$, and we obtain from Theorem 1 the result (1), apart from determining the constant $k(m)$. In fact, the exponent $\frac{\phi(m)}{m}-1$ is equal to $-\frac{1}{m}$ if and only if m is a power of a prime, and in all other cases the exponent is strictly less than $-\frac{1}{m}$. In other words, if m is divisible by at least two primes then $\rho(n,m)$ grows more slowly, as n increases, than $p_{\neg m}(n)$ does.

(d) Suppose $m = pq$ where $p < q$ are primes. Then $\frac{\phi(m)}{m} - 1 = -\frac{1}{p} - \frac{1}{q} + \frac{1}{pq}$ and Theorem 1 appears to differ from (2) by a multiplicative factor of $n^{1/pq}$. However, in our context m is fixed and n increases without bound, whereas Erdős and Turán assume for (2) that both p and q are bounded:

$$(\log n)^{3/4} \leqslant p < q \leqslant \frac{10 \log n}{\log \log n}. \tag{5}$$

Thus, both m and n are assumed to increase in (2). The apparent inconsistency can be resolved by showing that (5) implies

$$n^{\frac{1}{pq}} = 1 + O((\log n)^{-1/2}).$$

For an upper bound, from (5) we have

$$n^{1/(pq)} \leqslant n^{(\log n)^{-3/2}} = n^{(\log n)^{-1}(\log n)^{-1/2}} = e^{(\log n)^{-1/2}} = 1 + O((\log n)^{-1/2}).$$

For a lower bound we show

$$n^{\frac{1}{pq}} \geqslant n^{(\log \log n)^2/(100(\log n)^2)} \geqslant 1 + O((\log n)^{-1/2}).$$

Establishing the last inequality is the same as bounding (above) the function

$$f(n) := (n^{x(\log n)^{-1}} - 1)(\log n)^{1/2} \quad \text{where} \quad x = \frac{(\log \log n)^2}{100 \log n}.$$

Rewriting $f(n)$ using the identity $n^{(\log n)^{-1}} = e$ gives

$$f(n) = (e^x - 1)(\log n)^{1/2}.$$

Since $x \to 0$ as $n \to \infty$, we can choose n large enough so that $x < 1/2$. However, $0 \leqslant e^x - 1 < 2x$ for $0 \leqslant x < 1/2$ so

$$0 \leqslant f(n) < 2x(\log n)^{1/2} = \frac{(\log \log n)^2}{50(\log n)^{1/2}}.$$

Hence $f(n) \to 0$ as $n \to \infty$, so $f(n)$ is bounded above as claimed.

(e) The proofs by Erdős and Turán of results such as (1) and (2) draw heavily on tools from complex analysis. In [8, Section 5], Erdős and Turán state that it would be desirable to obtain a proof of (2) using more direct means:

> *"A more direct (real-variable or algebraic) approach to the determination of this coefficient would be desirable."*

The proof of Theorem 1 is principally algebraic: we determine and exploit a recursive formula for ρ.

(f) In a different direction, restricting m to a prime number and determining the proportion $\rho(G,m)$ of elements of an arbitrary finite group G whose order is coprime to m has been the subject of papers by many authors. For example, see [14] when G is a permutation group of degree n and see [1, 12, 13] when G is a finite simple classical group.

(g) The set $\mathrm{Sym}(n)^{(m)} = \{\pi^m \mid \pi \in \mathrm{Sym}(n)\}$ of mth powers, and its cardinality, have been extensively studied, e.g. [15, 18]. As every permutation of order coprime to m is an mth power, we have $R(n,m) \subseteq \mathrm{Sym}(n)^{(m)}$. The containment is proper in general, for example $(1,3)(2,4) \in \mathrm{Sym}(4)^{(2)} \setminus R(4,2)$. However, if m divides the exponent e of $\mathrm{Sym}(n)$ and $\gcd(m,e/m)=1$, then $R(n,m) = \mathrm{Sym}(n)^{(m)}$. Hence, one may guess that $|\mathrm{Sym}(n)^{(m)}|$ and $|R(m,n)|$ have the same asymptotic density. This follows from [15, 18] and [19].

2 Proof of Theorem 1

For the remainder of the paper, fix m as a square-free positive integer. Recall that $R(n,m)$ is the set of elements in $\mathrm{Sym}(n)$ of order coprime to m. Since m is fixed we will write $R(n) := R(n,m)$ and similarly (except in some formal statements) we write $\rho(n) := \rho(n,m)$. Additionally, we denote the greatest common divisor of integers c and d by (c,d), and we write

$$\Phi = \Phi(m) \coloneqq \{1 \leqslant i \leqslant m \mid (i,m) = 1\},$$

noting that $\phi \coloneqq \phi(m) = |\Phi|$.

The following lemma generalises [3, Lemma 2.1]. For convenience, we adopt the convention that $\rho(0) = 1$.

Lemma 3. *The following recursive formula holds for integers $n \geqslant m > 0$,*

$$n\rho(n) = (n-m)\rho(n-m) + \sum_{k\in\Phi} \rho(n-k).$$

Proof. The permutations $x \in R(n)$ can be enumerated according to the length k of the cycle containing the point 1. The number of choices for the cycle $(1, i_2, \ldots, i_k)$ of x is $(n-1)(n-2)\cdots(n-k+1)$. Note that $(k,m)=1$ and that the permutation induced by x on the $n-k$ points outside $\{1, i_2, \ldots, i_k\}$ lies in $R(n-k)$. Thus

$$|R(n)| = \sum_{\substack{1\leqslant k\leqslant n\\ (k,m)=1}} (n-1)(n-2)\cdots(n-k+1)|R(n-k)|.$$

Dividing this equation by $(n-1)!$, and noting that $|R(a)| = a!\rho(a)$ for all $a \in \mathbb{N}$, we obtain

$$n\rho(n) = \sum_{\substack{1\leqslant k\leqslant n\\ (k,m)=1}} \rho(n-k).$$

Replacing n above with $n-m$ and observing that $(k+m,m)=(k,m)$ yields

$$(n-m)\rho(n-m)=\sum_{\substack{1\leqslant k\leqslant n-m\\(k,m)=1}}\rho(n-m-k)=\sum_{\substack{m+1\leqslant k\leqslant n\\(k,m)=1}}\rho(n-k).$$

Subtracting these two equations gives

$$n\rho(n)-(n-m)\rho(n-m)=\sum_{k\in\Phi}\rho(n-k). \qquad \square$$

We now present a technical lemma which will be of use in the proof of Theorem 1.

Lemma 4. *Let y and a be real numbers such that $-1<y<0$ and $a\geqslant 2$. Then*

$$0<1-\frac{y+1}{a}\left(1-\frac{y}{a}\right)\leqslant\left(\frac{a-1}{a}\right)^{y+1}<1-\frac{y+1}{a}.$$

Proof. Let $x=-1/a$ and $x_0=-1/2$, and note that $x_0\leqslant x<0$. We seek upper and lower bounds for $f(x):=(1+x)^{y+1}=(\frac{a-1}{a})^{y+1}$. As $|x|<1$, the binomial series below converges absolutely

$$f(x)=\sum_{i\geqslant 0}\binom{y+1}{i}x^i.$$

Since $-1<y<0$, for each $i>0$, the binomial coefficient

$$\binom{y+1}{i}=\frac{(y+1)y(y-1)\cdots(y-(i-2))}{i!}$$

has $i-1$ negative factors. Hence, the product $\binom{y+1}{i}x^i$ is negative for each $i>0$. Therefore,

$$f(x)=\sum_{i\geqslant 0}\binom{y+1}{i}x^i<1+(y+1)x=1-\frac{y+1}{a}$$

yielding the desired upper bound.

Now we consider the lower bound. Temporarily we assume that $i\geqslant 2$. Since $(y-1)\cdots(y-(i-2))$ has $i-2$ negative factors, the product $(y-1)\cdots(y-(i-2))x^{i-2}$ is positive for each $i\geqslant 2$. Hence,

$$0<\prod_{j=1}^{i-2}(y-j)x=\prod_{j=1}^{i-2}(j-y)(-x)\leqslant\prod_{j=1}^{i-2}(j+1)(-x_0)=(i-1)!(-x_0)^{i-2}.$$

This in turn shows that

$$0>\binom{y+1}{i}x^i=\frac{(y+1)y(y-1)\cdots(y-(i-2))x^i}{i!}\geqslant\frac{(y+1)y(-x_0)^{i-2}x^2}{i}.$$

Taking the terms with $0 \leqslant i < 2$, together with the above lower bound for the sum of the terms with $i \geqslant 2$, gives

$$\begin{aligned} f(x) &\geqslant 1 + (y+1)x + \sum_{i\geqslant 2} \frac{(y+1)y(-x_0)^{i-2}x^2}{i} \\ &= 1 + (y+1)x + \frac{(y+1)y}{x_0^2}\left(\sum_{i\geqslant 2}\frac{(-x_0)^i}{i}\right)x^2. \end{aligned}$$

Now $\sum_{i\geqslant 1} \frac{(-x_0)^i}{i} = -\log(1+x_0)$, and hence, since $x_0 = -1/2$, we have

$$x_0^{-2}\sum_{i\geqslant 2}\frac{(-x_0)^i}{i} = x_0^{-2}(x_0 - \log(1+x_0)),$$

and this lies in the open interval $(0,1)$. Then since $(y+1)yx^2 < 0$, we obtain the desired lower bound

$$f(x) = (1+x)^{y+1} > 1 + (y+1)x + (y+1)yx^2 = 1 - \frac{y+1}{a}\left(1 - \frac{y}{a}\right).$$

Finally, since $-1 < y < 0$ and $a \geqslant 2$, this lower bound is positive. □

We now prove our main result.

Proof of Theorem 1. The result is true when $m = 1$ and $C(1) = 1$. Suppose $n \geqslant m \geqslant 2$. Recall the notation $\Phi = \Phi(m)$ and $\phi = |\Phi|$, and write

$$y := \frac{\phi}{m} - 1.$$

Observe that $-1 < y < 0$. In addition, for $0 \leqslant i \leqslant m-1$, write

$$x_i = |\{k \in \Phi \mid k < m - i\}| \quad \text{and} \quad y_i = |\{k \in \Phi \mid k \leqslant i\}|. \tag{6}$$

Note that $x_i \leqslant m - i - 1$, $y_i \leqslant i$, $x_i + i \geqslant \phi(m)$ and $y_i + (m-i) \geqslant \phi(m)$. In summary

$$\phi(m) - i \leqslant x_i \leqslant m - i - 1 \quad \text{and} \quad \phi(m) - m + i \leqslant y_i \leqslant i. \tag{7}$$

We begin by proving the required upper bound, namely

$$\rho(n) \leqslant \left\lceil \frac{n}{m} \right\rceil^y \qquad \text{for } n \geqslant m \geqslant 2. \tag{8}$$

Although we do not require it for this proof, the upper bound above holds trivially if $1 \leqslant n \leqslant m$ as then $\rho(n) \leqslant 1 = \left\lceil \frac{n}{m} \right\rceil^y = 1$. We proceed by induction on n. Now let $n \geqslant m+1$, so that $a := \left\lceil \frac{n}{m} \right\rceil \geqslant 2$. Write $n = am - b$, and note that $0 \leqslant b \leqslant m-1$.

Assume the upper bound in (8) holds for all positive integers strictly less than n. By Lemma 3,

$$\rho(am-b) = \frac{(a-1)m-b}{am-b}\rho((a-1)m-b) + \frac{1}{am-b}\sum_{k\in\Phi}\rho(am-b-k).$$

By the inductive hypothesis, $\rho((a-1)m-b) \leqslant (a-1)^y$. Similarly, for each $k \in \Phi$, if $k < m-b$ then $am-b-k > (a-1)m$ so by induction $\rho(am-b-k) \leqslant a^y$, and if $k \geqslant m-b$ then $\rho(am-b-k) \leqslant (a-1)^y$. Therefore, using the definition of x_i in (6), we obtain

$$\begin{aligned}\rho(am-b) &\leqslant \frac{(a-1)m-b}{am-b}(a-1)^y + \frac{x_b a^y + (\phi - x_b)(a-1)^y}{am-b} \\ &= a^y\left(\left(\frac{a-1}{a} - \frac{b/a}{am-b}\right)\left(\frac{a-1}{a}\right)^y + \frac{x_b + (\phi - x_b)\left(\frac{a-1}{a}\right)^y}{am-b}\right) \\ &= a^y\left(\left(\frac{a-1}{a}\right)^{y+1}\left(1 - \frac{b - a\phi + ax_b}{(a-1)(am-b)}\right) + \frac{x_b}{am-b}\right).\end{aligned}$$

By Lemma 4, $(\frac{a-1}{a})^{y+1} < 1 - \frac{y+1}{a}$, and as $y+1 = \frac{\phi}{m}$ and $a \geqslant 2$, we have

$$\rho(am-b) \leqslant a^y Y \text{ where } Y = \left(1 - \frac{\phi}{am}\right)\left(1 - \frac{b - a\phi + ax_b}{(a-1)(am-b)}\right) + \frac{x_b}{am-b}.$$

We want to show that $Y \leqslant 1$, so we write $Y = 1 - Y_0$ where Y_0 is an algebraic fraction in a, b, x_b, m, ϕ. It suffices, therefore, to show that $Y_0 \geqslant 0$ for all input values satisfying $a \geqslant 2$, $0 \leqslant b < m$, and $\phi \leqslant \min\{b + x_b, m\}$ *c.f.* (7). We use a computer to factor Y_0 giving

$$Y_0 = 1 - Y = \frac{(m-\phi)(b + x_b - \phi)}{m(a-1)(am-b)} \geqslant 0.$$

Thus $Y \leqslant 1$ and hence $\rho(am-b) \leqslant a^y$, proving the upper bound (8) for all $n \geqslant 1$.

We now turn to the lower bound. Recall the definition of $C := C(m)$ in (4), and note that $C > 0$ since $\rho(n) > 0$ for all $n \geqslant 1$. We will prove that,

$$\rho(n) \geqslant C\left\lfloor \frac{n}{m} \right\rfloor^y \qquad \text{for } n \geqslant m \geqslant 2. \tag{9}$$

As for the proof of the upper bound, we use induction on n. Observe that if $m \leqslant n \leqslant 2m-1$, then $\left\lfloor \frac{n}{m} \right\rfloor = 1$, and hence $\rho(n) \geqslant C = C\left\lfloor \frac{n}{m} \right\rfloor^y$ holds by (4). Now suppose $n \geqslant 2m$. Then $a := \left\lfloor \frac{n}{m} \right\rfloor \geqslant 2$. Write $n = am + b$, and note that $0 \leqslant b \leqslant m-1$. (Be aware that the definitions of a and b differ from their definitions in the proof of the upper bound.) Assume that the lower bound (9) holds for all positive integers strictly less than n. By Lemma 3,

$$\rho(am+b) = \frac{(a-1)m+b}{am+b}\rho((a-1)m+b) + \frac{1}{am+b}\sum_{k\in\Phi}\rho(am+b-k).$$

By the inductive hypothesis, $\rho((a-1)m+b) \geqslant C(a-1)^y$. Similarly, for each $k \in \Phi$, if $k \leqslant b$ then $am+b-k \geqslant am$ so by induction, $\rho(am+b-k) \geqslant Ca^y$, and if $k > b$ then $am > am+b-k \geqslant (a-1)m$ so by induction $\rho(am+b-k) \geqslant C(a-1)^y$. Therefore, using the definition of y_b in (6), we obtain

$$\begin{aligned}\rho(am+b) &\geqslant C\left(\frac{(a-1)m+b}{am+b}(a-1)^y + \frac{y_b a^y + (\phi - y_b)(a-1)^y}{am+b}\right)\\ &= Ca^y\left(\left(\frac{a-1}{a} + \frac{b/a}{am+b}\right)\left(\frac{a-1}{a}\right)^y + \frac{y_b + (\phi - y_b)\left(\frac{a-1}{a}\right)^y}{am+b}\right)\\ &= Ca^y\left(\left(\frac{a-1}{a}\right)^{y+1}\left(1 + \frac{b + a\phi - ay_b}{(a-1)(am+b)}\right) + \frac{y_b}{am+b}\right).\end{aligned}$$

By Lemma 4, since $a \geqslant 2$, $y = \frac{\phi}{m} - 1$ and $-1 < y < 0$, we have $\left(\frac{a-1}{a}\right)^{y+1} > 1 - \frac{y+1}{a}\left(1 - \frac{y}{a}\right)$, so

$$\rho(am+b) \geqslant Ca^y\left(\left(1 - \frac{\phi}{am}\left(1 + \frac{m-\phi}{am}\right)\right)\left(1 + \frac{b + a\phi - ay_b}{(a-1)(am+b)}\right) + \frac{y_b}{am+b}\right).$$

Write the above expression as Ca^yY where Y is an algebraic fraction in a, b, y_b, m, ϕ. We want to show that $Y \geqslant 1$, so we write $Y = 1 + Y_0$. It suffices, therefore, to show that $Y_0 \geqslant 0$ for all input values satisfying $a \geqslant 2$, $0 \leqslant b < m$, $m \geqslant \phi$ and $\phi - m + b \leqslant y_b \leqslant b$ (see (7)). We use a computer to factor Y_0 giving

$$Y_0 = Y - 1 = \frac{(m-\phi)(am(b-y_b) + \phi(y_b - b + m - \phi))}{m^2 a(a-1)(am+b)} \geqslant 0.$$

Therefore, $\rho(am+b) \geqslant Ca^yY \geqslant Ca^y$ and the claim in (9) holds for all $n \geqslant m$. This establishes the lower bound and completes the proof of the theorem. □

3 Computational evidence

Let $n \geqslant m > 1$ and assume that m is square-free. First suppose that m is prime. Recall that $p_{\neg m}(n)$ is the proportion of elements in $\mathrm{Sym}(n)$ with no cycle of length divisible by m, so $p_{\neg m}(n) = p_{\neg m}(n+i)$ for $0 \leqslant i < m$. Since $\rho(n,m) = p_{\neg m}(n)$, it follows that for all $a \geqslant 1$,

$$\rho(am, m) = \rho(am+1, m) = \cdots = \rho(am + (m-1), m). \tag{10}$$

Moreover, in this case (since m is prime),

$$\rho(n,m) = k(m)\left(\frac{n}{m}\right)^{\frac{\phi(m)}{m}-1} + O(n^{\frac{\phi(m)}{m}-2}), \tag{11}$$

where $k(m) = \Gamma(1 - \frac{1}{m})^{-1}$, noting that $\pi^{-1/2} \leqslant k(m) < 1$ (see [8, Sections 3 and 4] and [3, Theorem 2.3]).

In this final section we investigate the extent to which an analogue of the relationship in (11) holds for general positive integers m. We do this by presenting some computational evidence which led the authors to the statement of Theorem 1 and to Question 5 below.

The recursive formula for ρ in Lemma 3 provides an efficient means of computing $\rho(n, m)$ from the values $\rho(0, m)$, $\rho(1, m)$, $\ldots$, $\rho(m-1, m)$. In Figures 1–3 we fix the value of m as 6, 15 and 30, respectively, and we plot

$$f(n, m) := \rho(n, m) \cdot \left(\frac{n}{m}\right)^{1-\frac{\phi(m)}{m}}$$

against n for many values of n greater than m.

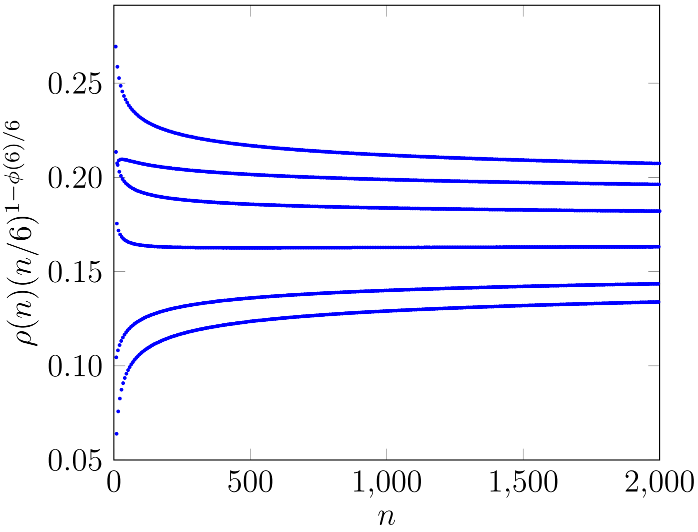

Figure 1: Plot of $f(n, 6)$ versus n for $7 \leqslant n \leqslant 2000$.

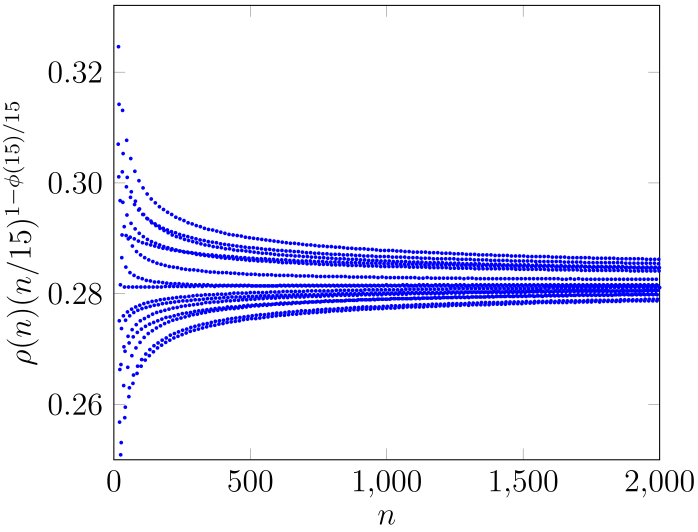

Figure 2: Plot of $f(n, 15)$ versus n for $16 \leqslant n \leqslant 2000$.

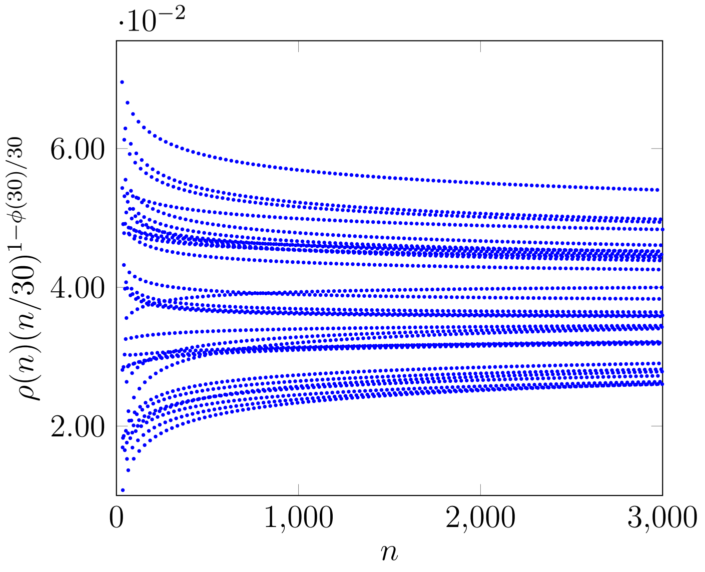

Figure 3: Plot of $f(n,30)$ versus n for $31 \leqslant n \leqslant 3000$.

It is evident from Figures 1–3 that (10) does not hold if m is composite. Figures 1–3 suggest that for fixed $0 \leqslant b < m$ the function $f(n,m)$ is either increasing or decreasing as $n \to \infty$ with $n \equiv b \pmod{m}$, and moreover that the limit is independent of b. This would imply [19, Proposition, p. 7] and give even sharper bounds than in our main theorem as we explain below. Pouyanne [19, Proposition, p. 7] defined a constant κ_m (for not necessarily square-free m) as follows:

$$(12) \qquad \kappa_m = \frac{1}{\Gamma\left(\frac{\phi(m)}{m}\right)} \prod_{d|m} d^{-\frac{\mu(d)}{d}} \quad \text{where} \quad \mu(d) = \begin{cases} (-1)^{|\pi(d)|} & \text{if } d \text{ is square-free,} \\ 0 & \text{otherwise.} \end{cases}$$

Thus $f(n,m) \sim \lambda_m := \kappa_m / m^{1-\phi(m)/m}$ as $n \to \infty$ paraphrases Pouyanne's result. Theorem 1 proves that $C(m) \leqslant \lambda_m \leqslant 1$. Figures 1–3 show that the convergence as $n \to \infty$ of $f(n,m)$ to λ_m can be very slow. Computational evidence suggests that the sequence $(f(am+b,m))_{a=0}^{\infty}$ is eventually monotonic. This leads us to the following question.

Question 5. Let m be a positive square-free integer. Does there exists an integer a_0 such that for each b the sequence $(f(am+b,m))_{a \geqslant a_0}$ is monotonic?

Remark 6. If this is true, then for $a \geqslant a_0$, $f(am+b,m)$ is bounded between $f(a_0m+b,m)$ and $\lambda_m = \kappa_m/m^{1-\phi(m)/m}$. When $m = p$ is prime and $0 \leqslant b \leqslant \frac{p-1}{2}$, Theorem 8 below shows $\lambda_p \leqslant f(ap+b,p) \leqslant 1 - \frac{1}{p}$ and for all $a \geqslant 1$. This improves (1).

Remark 7. We used the optimised Magma [2] code in [10], and the recurrence in Lemma 3, to compute values of $\rho(n,m)$ for n up to 10^5 and $m \leqslant 30$. This allowed us to both test the veracity of Question 5, and to discover some surprising patterns. The six curves in Figure 1 (unsurprisingly) correspond to the six possible choices for $b = n \mod 6$, but in a strange order *viz.* $b = 1, 6, 2, 5, 3, 4$ going from the highest curve to the lowest. (Incidentally, this observation motivated our "modulo m" proof of Theorem 1.) We noticed also that for many choices of m and b the sequence $f(am+b,m)$ for $0 \leqslant a \leqslant 1000$ was strictly decreasing, or strictly increasing. However, for very few choices e.g. $(m,b) = (26,24)$, the sequence initially increased (6 times), and then increased (596 times) and then increased (397 times). (The graph is a very flat sawtooth and so looks horizontal.) These unusual patterns lead us to question the existence of a simple proof of Question 5.

Question 5 is true in the very special case when p is a prime.

Theorem 8. *Let p be a prime. The sequence $(f(ap+b,p))_{a\geqslant 0}$ increases strictly for $0 \leqslant b \leqslant \lfloor \frac{p-1}{2} \rfloor$; whereas for $a \geqslant \frac{p-1}{2}$, the sequence decreases strictly for $\lfloor \frac{p-1}{2} \rfloor < b \leqslant p-1$.*

Proof. Write $n = ap+b$ where $0 \leqslant b < p$. It follows from the closed formula $\rho(n,p) = \prod_{i=1}^{a}(1-\frac{1}{ip})$ of [8, Lemma I], that $\rho(n+p,p) = \rho(n,p)(1-\frac{1}{(a+1)p})$. Hence

$$\frac{f(n+p,p)}{f(n,p)} = \left(1 - \frac{1}{(a+1)p}\right) \frac{\binom{n+p}{p}^{1-\frac{\phi(p)}{p}}}{\binom{n}{p}^{1-\frac{\phi(p)}{p}}} = \left(1 - \frac{1}{(a+1)p}\right)\left(1 + \frac{1}{a+\frac{b}{p}}\right)^{\frac{1}{p}}.$$

Fix p and b. Our proof has two cases. Case 1 proves that the above ratio is at least 1 for $0 \leqslant b \leqslant \lfloor \frac{p-1}{2} \rfloor$, and Case 2 shows the ratio is at most 1 for $\lfloor \frac{p-1}{2} \rfloor < b < p$.

Case 1. $0 \leqslant b \leqslant \lfloor \frac{p-1}{2} \rfloor$. The above ratio is at least 1 if and only if

$$\left(1 - \frac{1}{(a+1)p}\right)^p \geqslant \frac{a+c}{a+c+1} \qquad \text{where } c = \frac{b}{p}. \tag{13}$$

Observe that $0 \leqslant c < 1$, and for $0 \leqslant c_1, c_2 < 1$ we have

$$\frac{a+c_1}{a+c_1+1} < \frac{a+c_2}{a+c_2+1} \qquad \text{if and only if } c_1 < c_2. \tag{14}$$

The left-hand side of (13) is independent of c, and by (14) the right-hand side of (13) is largest when c equals $c_0 := \frac{1}{2}(1-\frac{1}{p})$. Set $x = (a+1)p$. Then

$$\frac{a+c_0}{a+c_0+1} = \frac{a+\frac{1}{2}(1-\frac{1}{p})}{a+\frac{1}{2}(1-\frac{1}{p})+1} = \frac{2ap+p-1}{2ap+3p-1} = \frac{2x-p-1}{2x+p-1}.$$

Hence (13) is true if for all $a \geqslant 0$ and all integers $p \geqslant 1$, we have

$$\left(\frac{x-1}{x}\right)^p \geqslant \frac{2x-p-1}{2x+p-1} \qquad \text{for all real numbers } x \geqslant 2. \tag{15}$$

We now prove (15) by induction on p for all integers $p \geqslant 1$. The case $p = 1$ is clearly true. In the following display, the first inequality follows from the inductive hypothesis, and the second requires proof:

$$\left(\frac{x-1}{x}\right)^{p+1} = \left(\frac{x-1}{x}\right)^p \left(\frac{x-1}{x}\right) \overset{\text{IH}}{\geqslant} \left(\frac{2x-p-1}{2x+p-1}\right)\left(\frac{x-1}{x}\right) \overset{?}{\geqslant} \frac{2x-p-2}{2x+p}.$$

The second inequality is equivalent to

$$(2x+p)(2x-p-1)(x-1) \geqslant (2x-p-2)(2x+p-1)x.$$

The left minus the right side is $p^2+p>0$. This proves Case 1.

Case 2. $\lfloor \frac{p-1}{2} \rfloor < b < p$. In this case it suffices to prove

$$\left(1-\frac{1}{(a+1)p}\right)^p < \frac{a+c}{a+c+1} \qquad \text{where } c=\frac{b}{p}. \tag{16}$$

First note that $\lfloor \frac{p-1}{2} \rfloor + 1 = \lceil \frac{p}{2} \rceil$. Hence $\frac{b}{2} \leqslant \lceil \frac{p}{2} \rceil \leqslant b$ and so $\frac{1}{2} \leqslant c$. For $c \geqslant \frac{1}{2}$, the right-hand side of (16) is smallest for $c=\frac{1}{2}$ by (14). As before, set $x=(a+1)p$. We prove (16) by establishing the inequality below:

$$\left(\frac{x-1}{x}\right)^p < \frac{a+\frac{1}{2}}{a+\frac{3}{2}} = \frac{2a+1}{2a+3} = \frac{2x-p}{2x+p}. \tag{17}$$

Reasoning as in Case 1, we prove (17) for $p \geqslant 1$ by induction on p. Certainly (17) is true for $p=1$. Assume it is true for some $p \geqslant 1$. By the inductive hypothesis:

$$\left(\frac{x-1}{x}\right)^{p+1} = \left(\frac{x-1}{x}\right)^p \left(\frac{x-1}{x}\right) \overset{\text{IH}}{<} \left(\frac{2x-p}{2x+p}\right)\left(\frac{x-1}{x}\right) \overset{?}{\leqslant} \frac{2x-p-1}{2x+p+1},$$

where the last inequality is equivalent to

$$(2x-p)(x-1)(2x+p+1) \leqslant (2x-p-1)x(2x+p) \quad \text{or} \quad p^2+p \leqslant 2x.$$

Finally, $2x \geqslant p^2+p$ is true for $a \geqslant \frac{p-1}{2}$. This proves Case 2, and the theorem. □

Acknowledgements

The work on this paper began at the 2018 Research Retreat of the Centre for the Mathematics of Symmetry and Computation. The third author is grateful for the Cecil King Travel Scholarship from the London Mathematical Society and the hospitality of the University of Western Australia; he also thanks the Engineering and Physical Sciences Research Council and the Heilbronn Institute for Mathematical Research for their financial support. The second and fourth authors gratefully acknowledge support from the Australian Research Council Discovery Grant DP190100450.

References

[1] L. Babai, S. Guest, C. E. Praeger, R. A. Wilson, *Proportions of r-regular elements in finite classical groups*, J. London Math. Soc. **88** (2013), 202–226.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

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

[4] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger, A. Seress, *A black-box algorithm for recognizing finite symmetric and alternating groups, I.*, Trans. Amer. Math. Soc. **355** (2003), 2097–2113.

[5] E. A. Bertram, B. Gordon, *Counting special permutations*, Eur. J. Comb. **10** (1989), 221–226.

[6] M. Bóna, A. McLennan, D. White, *Permutations with roots*, Random Struct. Algorithm **17** (2000), 157–167.

[7] P. Erdős, P. Turán, *On some problems of a statistical group-theory. I*, Z. Wahrsch. Verw. Gebiete **4** (1965), 175–186.

[8] P. Erdős, P. Turán, *On some problems of a statistical group-theory. II*, Acta Math. Acad. Sci. Hungar. **18** (1967), 151–163.

[9] P. Erdős, P. Turán, *On some problems of a statistical group-theory. III*, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320.

[10] S. Harper and S. P. Glasby, *Permutations with orders coprime to a given integer:* Magma *code*, doi:10.5281/zenodo.2647478

[11] S. P. Glasby, *Using recurrence relations to count certain elements in symmetric groups*, Europ. J. Combin. **22** (2001), 497–501.

[12] S. Guest, C. E. Praeger, *Proportions of elements with given 2-part order in finite classical groups of odd characteristic*, J. Algebra **372** (2012), 637–660.

[13] R. M. Guralnick , F. Lübeck, *On p-singular elements in Chevalley groups in characteristic p*, In: Groups and computation, III (Columbus, OH, 1999), pp. 169–182, Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001.

[14] I. M. Isaacs, W. M. Kantor, N. Spaltenstein, *On the probability that a group element is p-singular*, J. Algebra **176** (1995), 139–181.

[15] M. P. Mineev and A.I. Pavlov, *The number of permutations of a special form.* (Russian) Mat. Sb. (N.S.) **99**(141) (1976), no. 3, 468–476, 480.

[16] A. C. Niemeyer, T. Popiel, C. E. Praeger, S. Yalçınkaya, *On semiregular permutations of a finite set*, Math. Comp. **81** (2011), 605–622.

[17] A. C. Niemeyer, C. E. Praeger, A. Seress, *Estimation problems and randomised group algorithms*, In: Probabilistic Group Theory, Combinatorics and Computing, Editors: A. Detinko, D. Flannery and E O'Brien, pp. 35–82, Lecture Notes in Mathematics, vol. 2070, Springer, Berlin, 2013.

[18] A. I. Pavlov, Limit distribution of the number of cycles and of the logarithm of order of a class of permutations. (Russian) Mat. Sb. (N.S.) **114**(156) (1981), no. 4, 611–642, 655.

[19] N. Pouyanne, On the number of permutations admitting an m-th root. Electron. J. Combin. **9** (2002), #R3.