

Proportions of elements with given 2-part order in the symmetric group

Simon Guest and Cheryl E. Praeger

Communicated by Robert M. Guralnick

Abstract. For an element g in a group X , we say that g has 2-part order 2^b if 2^b is the largest power of 2 dividing the order of g . Using results of Erdős and Turán, and Beals et al., we give explicit lower bounds on the proportion of elements of the symmetric group S_n with certain 2-part orders. Some of these lower bounds are constant; for example we show that at least 23.5% of the elements in S_n ($n \geq 3$) have a certain 2-part order and furthermore, more than half of the elements in S_n have one of three 2-part orders. Also, for all $n \geq 2$, at least $\sqrt{5} - 2$ of the elements in S_n have the same 2-part order and we show that $\sqrt{5} - 2$ is best possible.

1 Introduction

Erdős and Turán [5] proved that for a prime power $p_0 \leq n$, the proportion $s_{\neg p_0}(n)$ of elements in S_n whose order does not divide p_0 is

$$s_{\neg p_0}(n) = \prod_{u=1}^{\lfloor n/p_0 \rfloor} \left(1 - \frac{1}{up_0}\right). \quad (1.1)$$

Thus, the proportion $p_n(2^b)$ of elements in S_n of 2-part order 2^b (that is to say, elements whose order is divisible by 2^b but not by 2^{b+1}) can be evaluated explicitly using the formula

$$p_n(2^b) = s_{\neg 2^{b+1}}(n) - s_{\neg 2^b}(n). \quad (1.2)$$

Furthermore, Erdős and Turán also note that if $\alpha > 0$ is fixed and if the real number $p_0 = (\alpha + o(1)) \log(n)$ is prime, then $s_{\neg p_0}(n) \rightarrow e^{-1/\alpha}$, as $n \rightarrow \infty$. This suggests that the proportion of elements of 2-part order of the form $2^b = (\alpha + o(1)) \log(n)$ might be bounded below by a positive constant. Indeed, if $2c > 1$, then every interval of the form $[c, 2c)$ contains a unique power of 2. In particular, if $n \geq 3$, then there is an integer $b \geq 0$ such that 2^b is contained in $[\frac{1}{2}a \log(n), a \log(n))$,

This research forms part of Australian Research Council Federation Fellow project FF0776186 of the second author.

where $a \approx 1.03$. We were surprised to find that the proportion of elements in S_n of this 2-part order 2^b is at least 0.235. We also find constant lower bounds for other powers of 2 roughly of this magnitude, which we describe in Theorem 1.1.

Theorem 1.1. *Let $p_n(2^b)$ be as above and let $a := 1/\log(\frac{1}{2}(3 + \sqrt{5})) \approx 1.03904$ so that $I_0 := [\frac{1}{4}a \log(n), 4a \log(n))$ contains at most three powers of 2. Then*

- (i) *more than half of the elements in S_n have 2-part order in I_0 ,*
- (ii) *if I , N_I and p_I are as in Table 1, and if $\alpha \in I$ is such that $\alpha \log(n)$ is an integer power of 2, then $p_n(\alpha \log(n)) \geq p_I$ provided $n \geq N_I$.*

In fact, an anonymous referee of an earlier version of our work showed us that there exists a positive integer b such that $p_n(2^b) \geq \sqrt{5} - 2 \approx 0.236067977$ and that this lower bound is the best possible in a sense that is made precise in Theorem 1.2.¹

Theorem 1.2. *With the notation above, the following statements hold.*

- (i) *For all positive integers n , there exists a positive integer b such that*

$$p_n(2^b) \geq \sqrt{5} - 2.$$

- (ii) *For all $\epsilon > 0$, there exist infinitely many positive integers n such that*

$$p_n(2^b) \leq \sqrt{5} - 2 + \epsilon$$

for all possible values of b .

- (iii) *For all $\epsilon > 0$, there exists a positive integer N_ϵ such that for all $n \geq N_\epsilon$ we have*

$$p_n(2^b) \leq \frac{1}{4} + \epsilon$$

for all possible values of b .

The lower bounds in Theorems 1.1 and 1.2 can be used to bound below by constants the proportion of elements of certain 2-part orders in classical groups (see [6]). Not only is this of independent interest, but it can also be used to analyze certain Black Box recognition algorithms for classical groups (in particular an important part of Yalçinkaya's algorithm [8] is analyzed in [6] using these results).

We also note that the analogous question about the distribution of element orders in a fixed Sylow p -subgroup of the symmetric group has been considered in the literature, and there it also turned out that the distribution is very concentrated (see, for example [1, Proposition 2.8 and Theorem 1]).

¹ Unfortunately for us, the referee chose to remain anonymous and we were unable to persuade them to co-author this paper.

I	N_I	pI
$[\frac{a}{8}, \frac{a}{4})$	47	0.0165662676
$[\frac{a}{4}, \frac{a}{2})$	7	0.1170040878
$[\frac{a}{2}, a)$	3	0.2351203790
$[a, 2a)$	2	0.1531015975
$[2a, 4a)$	8	0.0605468750
$[4a, 8a)$	16	0.0307617187
$[8a, 16a)$	64	0.0155029296
$[16a, 32a)$	128	0.0065085752

Table 1. Description of lower bounds for Theorem 1.1.

Using the explicit bounds in [3], we prove weaker lower bounds on the proportion of elements in S_n of any possible 2-part order in Theorem 5.1. We show that if $1 \leq 2^b \leq n$, then $p_n(2^b)$ satisfies

$$p_n(2^b) \geq \frac{K_b}{n^{1/2^{b+1}}}, \tag{1.3}$$

where K_b is a constant depending only on b .

The proofs of Theorems 1.1 and 1.2 are in Sections 4 and 3 respectively.

2 Preliminaries

We use the following theorem of Beals, Leedham-Green, Niemeyer, Praeger and Seress [3], which gives useful bounds on the proportion of elements in the symmetric group whose order is not divisible by a given prime power. The bounds involve the *Gamma function* Γ , which is defined for all $z \in \mathbb{C}$, with $\text{Re } z > 0$, by the equation $\Gamma(z) := \int_0^\infty y^{z-1} e^{-y} dy$.

Theorem 2.1. *Let n and p_0 be positive integers such that $2 \leq p_0 \leq n$ and p_0 is a prime power. If $c(p_0) := p_0^{1/p_0} \Gamma(1 - \frac{1}{p_0})^{-1}$, then*

$$c(p_0)n^{-1/p_0}(1 - n^{-1}) \leq s_{-p_0}(n) \leq c(p_0)n^{-1/p_0}(1 + 2n^{-1}).$$

Remark 2.2. In particular, $c(2) = (\frac{\pi}{2})^{-1/2} \cong 0.798$, $c(4) \cong 1.154$, $c(8) \cong 1.190$ and $c(16) \cong 1.143$. In Lemma 2.6, we show that $\Gamma(1 - \frac{1}{2^{p_0}})^{-1} \geq \Gamma(1 - \frac{1}{p_0})^{-1}$, and that $c(p_0)$ is decreasing for $p_0 \geq 8$. We also note that $\lim_{p_0 \rightarrow \infty} c(p_0) = 1$ so that $s_{-p_0}(n)n^{1/p_0} \geq 1 - n^{-1}$ whenever $n \geq p_0 \geq 8$.

2.1 Inequalities

The following lemmas will be useful to bound the proportions of elements in S_n that have 2-part order 2^b .

Lemma 2.3. *If $x \geq 2$, then*

$$-\frac{2}{x} \leq -\frac{1}{x} - \frac{1}{x^2} \leq \log\left(1 - \frac{1}{x}\right) \leq -\frac{1}{x} - \frac{1}{2x^2} \leq -\frac{1}{x}, \quad (2.1)$$

and if $0 < x \leq 1$, then

$$1 + x + \frac{x^2}{2} < e^x < 1 + x + \frac{3x^2}{4}. \quad (2.2)$$

Remark 2.4. We will also find the following restatement of (2.1) useful. If $x \geq 2$, then

$$-\frac{2}{x} \leq -\frac{1}{x} - \frac{1}{x^2} \leq \log(x-1) - \log(x) \leq -\frac{1}{x} - \frac{1}{2x^2} \leq -\frac{1}{x}.$$

Proof. For the first inequality, observe that for $x > 1$, we have the Taylor series

$$\log\left(1 - \frac{1}{x}\right) = -\sum_{i=1}^{\infty} \frac{1}{ix^i},$$

hence

$$\log\left(1 - \frac{1}{x}\right) \leq -\frac{1}{x} - \frac{1}{2x^2}.$$

Also

$$\log\left(1 - \frac{1}{x}\right) = -\sum_{i=1}^{\infty} \frac{1}{ix^i} \geq -\frac{1}{x} - \frac{1}{x^2},$$

since if $x \geq 2$, then $\frac{1}{2x^2} \geq \sum_{i=3}^{\infty} \frac{1}{ix^i}$. Indeed, we have

$$\sum_{i=3}^{\infty} \frac{1}{ix^i} \leq \frac{1}{3} \sum_{i=3}^{\infty} \frac{1}{x^i} = \frac{1}{3x^2(x-1)},$$

and $\frac{1}{3x^2(x-1)} \leq \frac{1}{2x^2}$ when $x \geq 5/3$. Inequalities in (2.2) are proved in [7] using the first terms of the Taylor series. \square

Lemma 2.5. *If $x > 1$, then*

$$(2x)^{1/2x} - x^{1/x} \geq \frac{\log(2) - \log(x)}{2x} - \frac{3\log^2(x)}{4x^2} + \frac{\log^2(2x)}{8x^2}. \quad (2.3)$$

Proof. Observe that if $x > 1$, then

$$(2x)^{1/2x} \geq 1 + \frac{\log(2x)}{2x} + \frac{\log^2(2x)}{8x^2}$$

since

$$(2x)^{1/2x} = e^{\log(2x)/2x}$$

and we can apply Lemma 2.3. Similarly

$$x^{1/x} = e^{\log(x)/x},$$

thus

$$x^{1/x} < 1 + \frac{\log(x)}{x} + \frac{3 \log^2(x)}{4x^2}$$

and (2.3) follows since

$$\begin{aligned} (2x)^{1/2x} - x^{1/x} &\geq \frac{\log(2x)}{2x} + \frac{\log^2(2x)}{8x^2} - \frac{\log(x)}{x} - \frac{3 \log^2(x)}{4x^2} \\ &= \frac{\log(2) - \log(x)}{2x} - \frac{3 \log^2(x)}{4x^2} + \frac{\log^2(2x)}{8x^2}. \quad \square \end{aligned}$$

Lemma 2.6. *Let $c : [2, \infty) \rightarrow \mathbb{R}$ be defined as in Theorem 2.1. On the interval $[8, \infty)$, c is decreasing, and bounded below by 1. The function $x \mapsto \Gamma(1 - 1/x)^{-1}$ is increasing on the interval $(1, \infty)$ and, in particular, for $x > 1$,*

$$\frac{1}{\Gamma(1 - \frac{1}{2x})} \geq \frac{1}{\Gamma(1 - \frac{1}{x})}. \tag{2.4}$$

Also, if $x \in [2, \infty)$, then $c(x) < 3/2$.

Proof. To show that c is decreasing on the interval $[8, \infty)$, we differentiate

$$\frac{d}{dx}c(x) = \frac{\Gamma(1 - \frac{1}{x})x^{1/x}(\frac{1-\log(x)}{x^2}) - x^{1/x}\Psi(1 - \frac{1}{x})\Gamma(1 - \frac{1}{x})x^{-2}}{(\Gamma(1 - \frac{1}{x}))^2}, \tag{2.5}$$

where Ψ is the digamma function, or in other words, the logarithmic derivative of the Gamma function (so that $\Gamma' = \Gamma \Psi$). We can simplify (2.5) to give

$$\frac{d}{dx}c(x) = -\frac{x^{-2+1/x}(\log(x) - 1 + \Psi(1 - \frac{1}{x}))}{\Gamma(1 - \frac{1}{x})}.$$

Now the digamma function Ψ satisfies the equation

$$\Psi\left(1 - \frac{1}{x}\right) = -\gamma - \sum_{k=1}^{\infty} \frac{1}{k(kx - 1)}, \tag{2.6}$$

where γ is Euler's constant; see e.g. [2, 6.3.16]. To show that c is decreasing on the interval $[8, \infty)$, it suffices to show that the expression $\log(x) - 1 + \Psi(1 - \frac{1}{x})$

is positive for $x \geq 8$. We can use equation (2.6) to do this; indeed

$$\begin{aligned} \log(x) - 1 + \Psi\left(1 - \frac{1}{x}\right) &= \log(x) - 1 - \gamma - \sum_{k=1}^{\infty} \frac{1}{k(kx - 1)} \\ &\geq \log(8) - 1 - \gamma - \sum_{k=1}^{\infty} \frac{1}{k(8k - 1)} \\ &\geq \log(8) - 1 - \gamma - \sum_{k=1}^{\infty} \frac{1}{7k^2} = \log(8) - 1 - \gamma - \frac{\pi^2}{42} \\ &> 0. \end{aligned}$$

Hence c is decreasing on the interval $[8, \infty)$. Now observe that

$$\lim_{x \rightarrow \infty} c(x) = \frac{1}{\Gamma(1)} = 1;$$

thus c must be bounded below by 1 on $[8, \infty)$ since c is decreasing on $[8, \infty)$. Similarly, we differentiate the function $x \mapsto \Gamma(1 - \frac{1}{x})^{-1}$ to get

$$\frac{d}{dx} \Gamma\left(1 - \frac{1}{x}\right)^{-1} = \frac{-\Psi\left(1 - \frac{1}{x}\right)}{x^2 \Gamma\left(1 - \frac{1}{x}\right)}.$$

If $x \in (1, \infty)$, then the denominator is positive, and the numerator is also positive by (2.6); thus the function $x \mapsto \Gamma(1 - \frac{1}{x})^{-1}$ is increasing on $(1, \infty)$. In particular, this shows that if $x \in [2, \infty)$, then $\Gamma(1 - \frac{1}{x})^{-1} \leq \Gamma(1)^{-1} = 1$, and elementary calculus shows that $x^{1/x} < 3/2$; thus we have $c(x) < 3/2$. \square

Corollary 2.7. *If p_0 is a power of 2 and $p_0 \geq 2^{16}$, then*

$$\begin{aligned} c(2p_0) - c(p_0) &\geq -\frac{1}{\Gamma(1 - 2^{-16})} \left(\frac{\log(p_0)}{2p_0} + \frac{3 \log^2(p_0)}{4p_0^2} \right) \\ &\geq -\frac{1}{\Gamma(1 - 2^{-16})} \left(\frac{16 \log(2)}{2^{17}} + \frac{3 \log^2(2)}{2^{26}} \right), \end{aligned}$$

and in particular $c(2p_0) - c(p_0) \geq -0.000085$.

Proof. Observe that Lemma 2.6 implies that

$$\begin{aligned} c(2p_0) - c(p_0) &= \frac{(2p_0)^{1/2p_0}}{\Gamma(1 - \frac{1}{2p_0})} - \frac{p_0^{1/p_0}}{\Gamma(1 - \frac{1}{p_0})} \\ &\geq \frac{(2p_0)^{1/2p_0}}{\Gamma(1 - \frac{1}{p_0})} - \frac{p_0^{1/p_0}}{\Gamma(1 - \frac{1}{p_0})}. \end{aligned}$$

Also, Lemma 2.5 implies that

$$\begin{aligned} & \frac{(2p_0)^{1/2p_0}}{\Gamma(1 - \frac{1}{p_0})} - \frac{p_0^{1/p_0}}{\Gamma(1 - \frac{1}{p_0})} \\ & \geq \frac{1}{\Gamma(1 - \frac{1}{p_0})} \left(-\frac{\log(p_0)}{2p_0} - \frac{3 \log^2(p_0)}{4p_0^2} + \frac{\log^2(2p_0)}{8p_0^2} \right) \\ & \geq -\frac{1}{\Gamma(1 - \frac{1}{p_0})} \left(\frac{\log(p_0)}{2p_0} + \frac{3 \log^2(p_0)}{4p_0^2} \right), \end{aligned}$$

and using Lemma 2.6 again, together with the fact that $x \mapsto \frac{\log(x)}{x}$ is decreasing for $x \geq e$, we have for all $p_0 \geq 2^{16}$,

$$\begin{aligned} c(2p_0) - c(p_0) & \geq -\frac{1}{\Gamma(1 - \frac{1}{p_0})} \left(\frac{\log(p_0)}{2p_0} + \frac{3 \log^2(p_0)}{4p_0^2} \right) \\ & \geq -\frac{1}{\Gamma(1 - 2^{-16})} \left(\frac{\log(2)}{2^{13}} + \frac{3 \log^2(2)}{2^{26}} \right) \geq -0.000085. \quad \square \end{aligned}$$

Lemma 2.8. Consider the function $f : (0, \infty) \rightarrow \mathbb{R}$ given by $f(\alpha) = e^{-\frac{1}{2\alpha}} - e^{-\frac{1}{\alpha}}$.

Let

$$a := \frac{1}{\log(\frac{1}{2}(3 + \sqrt{5}))} \approx 1.03904.$$

If α is contained in one of the intervals I in column 1 of Table 2, then $f(\alpha)$ is bounded below by the value in column 2.

Interval I	Lower bound on $f(\alpha)$
$[\frac{a}{8}, \frac{a}{4}]$	0.0208331323
$[\frac{a}{4}, \frac{a}{2}]$	0.1246117974
$[\frac{a}{2}, a]$	0.2360679774
$[a, 2a]$	0.1681173890
$[2a, 4a]$	0.1005004015
$[4a, 8a]$	0.0549701083
$[8a, 16a]$	0.0287501480
$[16a, 32a]$	0.0147025988

Table 2. Lower bounds on f .

Proof. Observe that f is differentiable and has no local minima on $(0, \infty)$. Thus the minimum value of $f(\alpha)$ for $\alpha \in [c, d]$ is $\min\{f(c), f(d)\}$. The lower bounds of $f(\alpha)$ on the given intervals now follow easily. \square

Remark 2.9. The value for a was chosen to maximize the lower bound for $f(\alpha)$ on the interval $[a/2, a]$.

3 Proof of Theorem 1.2

(i) First observe that if $t \leq n$, then

$$\begin{aligned} s_{-2t}(n)^2 &= \prod_{u=1}^{\lfloor n/2t \rfloor} \left(1 - \frac{1}{2tu}\right)^2 = \prod_{u=1}^{\lfloor n/2t \rfloor} \left(1 - \frac{1}{tu} + \frac{1}{4t^2u^2}\right) \\ &> \prod_{u=1}^{\lfloor n/2t \rfloor} \left(1 - \frac{1}{tu}\right) \geq s_{-t}(n). \end{aligned}$$

Next suppose that there exists a nonnegative integer b such that

$$\frac{3 - \sqrt{5}}{2} \leq s_{-2^{b+1}}(n) \leq \frac{-1 + \sqrt{5}}{2}.$$

Then

$$\begin{aligned} p_n(2^b) &= s_{-2^{b+1}}(n) - s_{-2^b}(n) > s_{-2^{b+1}}(n) - s_{-2^{b+1}}(n)^2 \\ &> \frac{3 - \sqrt{5}}{2} - \frac{(-1 + \sqrt{5})^2}{4} = \sqrt{5} - 2. \end{aligned}$$

If there is no such b , then since $s_{-2^b}(n)$ increases from 0 to 1 as b increases from 0, there exists a nonnegative integer b such that

$$s_{-2^b}(n) < \frac{3 - \sqrt{5}}{2} < \frac{-1 + \sqrt{5}}{2} < s_{-2^{b+1}}(n).$$

Now it follows easily that $p_n(2^b) > \sqrt{5} - 2$ in this case as well.

(ii) Let $\epsilon > 0$. We shall show that there exist infinitely many integers n such that $p_n(2^b) \leq \sqrt{5} - 2 + \epsilon$ for all nonnegative integers b . Using Theorem 2.1, we find that if $2^b \geq 2$, then

$$p_n(2^b) \leq c(2^{b+1})n^{-1/2^{b+1}} \left(1 + \frac{2}{n}\right) - c(2^b)n^{-1/2^b} \left(1 - \frac{1}{n}\right).$$

Since the function c is decreasing on $[8, \infty)$, we have

$$\begin{aligned} p_n(2^b) &\leq c(2^b)(n^{-1/2^{b+1}} - n^{-1/2^b}) + \frac{1}{n}(2c(2^{b+1})n^{-1/2^{b+1}} + c(2^b)n^{-1/2^b}) \\ &\leq c(2^b)(n^{-1/2^{b+1}} - n^{-1/2^b}) + \frac{10}{n} \end{aligned}$$

for $b \geq 3$, since we can take the crude bound

$$2c(2^{b+1})n^{-1/2^{b+1}} + c(2^b)n^{-1/2^b} \leq 10.$$

If we write $2^b = \alpha \log(n)$, then this inequality becomes

$$p_n(2^b) \leq c(\alpha \log(n))(e^{-1/2\alpha} - e^{-1/\alpha}) + \frac{10}{n} \tag{3.1}$$

for $b \geq 3$. Similarly, since $c(2) \leq c(8)$ and $c(4) \leq c(8)$, we have

$$p_n(2^b) \leq c(8)(e^{-1/2\alpha} - e^{-1/\alpha}) + \frac{10}{n} \tag{3.2}$$

for $b = 1$ and 2 .

We can use elementary calculus to show that the function f defined by $f(\alpha) := e^{-1/2\alpha} - e^{-1/\alpha}$ is increasing on $(0, 1/\log(4))$ and decreasing on $(1/\log(4), \infty)$. It follows that if $\alpha > 0$ and $\alpha \notin [a/2, a]$, then

$$f(\alpha) \leq \min\{f(a/2), f(a)\} = \sqrt{5} - 2.$$

In light of estimates (3.1) and (3.2), to prove (ii), we will find $\delta > 0$ and an interval of the form $[(a - \delta) \log(n), a \log(n)]$ such that if N is sufficiently large and $[(a - \delta) \log(n), a \log(n)]$ contains a power of 2, then $c(2^b)f(\alpha) \leq \sqrt{5} - 2 + 2\epsilon/3$ for all possible values of b . We do this separately for various ranges of α . Moreover for each δ there exist infinitely many integers n such that the considered interval $[(a - \delta) \log(n), a \log(n)]$ contains a power of 2, and therefore proving this assertion will yield a proof of part (ii), namely that there are infinitely many n such that $p_n(2^b) \leq \sqrt{5} - 2 + \epsilon$, for all nonnegative integers b .

If $\alpha \in [1/4, a/2]$ or $[a, 2]$, then since the function c in Lemma 2.6 is decreasing on $[8, \infty)$ and $\lim_{x \rightarrow \infty} c(x) = 1$, we can choose N_1 such that if $n \geq N_1$, then

$$c(\alpha \log(n))f(\alpha) \leq \sqrt{5} - 2 + \frac{\epsilon}{3}. \tag{3.3}$$

If $\alpha \in [2, \infty)$ or $(0, 1/4]$, then $f(\alpha) \leq f(2) \leq 0.17228$ and in particular, since $c(2^b) \leq c(8)$ for all positive integers b , we have

$$c(2^b)f(\alpha) \leq c(8)f(2) < 0.21, \tag{3.4}$$

which is less than $\sqrt{5}-2$. If $\alpha \in [1/4, 2]$, then first choose N_2 such that if $n \geq N_2$, then

$$c(\alpha \log(n))(\sqrt{5}-2) < \sqrt{5}-2 + \frac{\epsilon}{3}.$$

Now choose $\epsilon' > 0$ such that if $\alpha \in [1/4, 2]$ and $n \geq N_2$, then

$$c(\alpha \log(n))\epsilon' \leq \frac{\epsilon}{3}.$$

Since f is decreasing on $(1/\log(4), \infty)$, we can choose $\delta > 0$ such that $\delta < 0.015$ and if $\alpha \in [a-\delta, a]$, then $f(\alpha) \leq \sqrt{5}-2 + \epsilon'$. In particular,

$$c(\alpha \log(n))f(\alpha) \leq c(\alpha \log(n))(\sqrt{5}-2) + c(\alpha \log(n))\epsilon' \leq \sqrt{5}-2 + 2\frac{\epsilon}{3}$$

if $\alpha \in [a-\delta, a]$.

To control the last term in (3.1), choose N_3 such that $\frac{10}{n} \leq \frac{\epsilon}{3}$ for all $n \geq N_3$. We also need to treat the case $2^b = 1$. We note that

$$p_n(1) = s_{-2}(n) \leq c(2)\frac{1}{\sqrt{n}}\left(1 + \frac{2}{n}\right),$$

so we choose N_4 such that if $n \geq N_4$, then $p_n(1) \leq \sqrt{5}-2$. In light of (3.2) and (3.4), we choose N_5 such that if $n \geq N_5$ and $\alpha \log(n) \leq 4$, then $\alpha < 1/4$.

We are now in a position to prove that if $[(a-\delta)\log(n), a\log(n)]$ contains 2^b , then $p_n(2^{b+j}) \leq \sqrt{5}-2 + \epsilon$ for all possible integers j when n is sufficiently large. Let $N := \max\{N_1, N_2, N_3, N_4, N_5\}$. Using inequality (3.1), if $n \geq N$ and $[(a-\delta)\log(n), a\log(n)]$ contains 2^b , then

$$\begin{aligned} p_n(2^b) &\leq c(\alpha \log(n))f(\alpha) + \frac{10}{n} \\ &\leq \left(\sqrt{5}-2 + \frac{2\epsilon}{3}\right) + \frac{\epsilon}{3} = \sqrt{5}-2 + \epsilon. \end{aligned}$$

Moreover, if $j \geq 1$ and $2^b = \alpha \log(n)$ with $\alpha \in [a-\delta, a]$ as above, then we have $\frac{2^{b+j}}{\log(n)} \geq 2$ (since $\delta < 0.015$ and $a > 1.03$); thus by (3.4) we have

$$p_n(2^{b+j}) \leq 0.21 + \epsilon < \sqrt{5}-2 + \epsilon.$$

Similarly, if $-b \leq j \leq -2$, then $\frac{2^{b+j}}{\log(n)} \in (0, 1/4)$ and so

$$p_n(2^{b+j}) < \sqrt{5}-2 + \epsilon.$$

Finally, if $2^b = \alpha \log(n)$ and $\alpha \in [a-\delta, a]$, then $\frac{2^{b-1}}{\log(n)} \in [1/4, a/2]$ and so (3.1) and (3.3) imply that

$$p_n(2^{b-1}) \leq \sqrt{5}-2 + \epsilon.$$

Thus we have shown that if $n \geq N$, then

$$p_n(2^{b+j}) \leq \sqrt{5} - 2 + \epsilon$$

for all integers j .

(iii) If $n \geq N$, then (3.1), (3.3) and (3.4) show that

$$p_n(\alpha \log(n)) \leq \sqrt{5} - 2 + \epsilon < \frac{1}{4} + \epsilon$$

whenever $\alpha \notin [a/2, a]$. Now since f attains an absolute maximum of $\frac{1}{4}$ on $(0, \infty)$ at $\frac{1}{\log(4)}$, we can choose N_6 such that if $n \geq N_6$ and $\alpha \in [a/2, a]$, then

$$c(\alpha \log(n))f(\alpha) \leq \frac{1}{4} + \frac{2\epsilon}{3}.$$

Therefore for all $n \geq N_\epsilon := \max\{N, N_6\}$, by (3.1), we have

$$p_n(2^b) \leq \frac{1}{4} + \epsilon$$

for all possible values of b , which proves the last part of Theorem 1.2.

4 Proof of Theorem 1.1

The proof is divided into a number of cases. In each case, we refer to information summarised in Table 4 below. Throughout the proof, p_0 denotes a power of 2 satisfying $p_0 = \alpha \log(n)$.

Case 1: $n \leq 10^7$

If $n \leq 10^7$, then we verify Theorem 1.1 using MAGMA [4] in the following way. For a fixed interval $I = [c, 2c)$ in column 1 of Table 4, n must be sufficiently large so that $[c \log(n), 2c \log(n))$ contains a power of 2. In column 3 of Table 4, we record the minimum value N_I of n for which this occurs.² For each integer $n \in [N_I, 10^7]$, we find p_0 the unique power of 2 contained in $[c \log(n), 2c \log(n))$, and then compute $p_n(p_0)$ precisely using (1.1) and (1.2). Then we find the minimum value of $p_n(p_0)$ over all integers $n \in [N_I, 10^7]$ and record a lower bound in column 4 of Table 4. Table 3 below gives, for each I , the explicit values of $n_0 \in [N_I, 10^7]$ and $p'_0 = \alpha \log(n)$, with $\alpha \in I$, that minimize $p_n(p_0)$.

² For some intervals I , the minimum value N_I is not sufficiently large to use (1.2) and the value in brackets gives the minimum value of n for which we can use (1.2). It is not relevant to the proof.

I	$[\frac{a}{8}, \frac{a}{4})$	$[\frac{a}{4}, \frac{a}{2})$	$[\frac{a}{2}, a)$	$[a, 2a)$
n_0	2206	46	4870848	2208
p'_0	1	1	16	16

I	$[2a, 4a)$	$[4a, 8a)$	$[8a, 16a)$	$[16a, 32a)$
n_0	47	64	128	2207
p'_0	16	32	64	256

Table 3. Values of $n_0 \in [N_I, 10^7]$ and $p'_0 = \alpha \log(n)$, with $\alpha \in I$, that minimize $p_n(p_0)$.

Case 2: $n \geq 10^7$

Now suppose that $n \geq 10^7$. In this case, we use Theorem 2.1, which states that if $2 \leq 2^b \leq n$, then

$$c(2^b)n^{-1/2^b}(1 - n^{-1}) \leq s_{-2^b}(n) \leq c(2^b)n^{-1/2^b}(1 + 2n^{-1}).$$

Thus, since $n \geq 10^7$ and therefore $2 \leq p_0 \leq \frac{n}{2}$ for each of the intervals I in Table 4, we have

$$p_n(p_0) = s_{-2p_0}(n) - s_{-p_0}(n) \geq L(n, p_0),$$

where

$$\begin{aligned} L(n, p_0) &:= \frac{c(2p_0)}{n^{1/2p_0}} - \frac{c(p_0)}{n^{1/p_0}} + \frac{1}{n} \left(-\frac{c(2p_0)}{n^{1/2p_0}} - \frac{2c(p_0)}{n^{1/p_0}} \right) \\ &\geq c(p_0) \left(\frac{1}{n^{1/2p_0}} - \frac{1}{n^{1/p_0}} \right) + \frac{(c(2p_0) - c(p_0))}{n^{1/2p_0}} \\ &\quad - \frac{1}{n}(c(2p_0) + 2c(p_0)). \end{aligned} \tag{4.1}$$

Now $p_0 = \alpha \log(n)$ and α is contained in one of the intervals I given in column 1 of Table 4. Note that the last term in (4.1) is

$$-\frac{1}{n}(c(2p_0) + 2c(p_0)) > -\frac{9}{2n} > -\frac{5}{n}$$

by the last part of Lemma 2.6. We also note that

$$n^{1/p_0} = e^{\log(n)/p_0} = e^{1/\alpha},$$

and since $n \geq 10^7$, we have

$$L(n, p_0) \geq c(p_0) \left(e^{-1/2\alpha} - e^{-1/\alpha} \right) + \frac{c(2p_0) - c(p_0)}{e^{1/2\alpha}} - \frac{5}{10^7}. \tag{4.2}$$

For each of the intervals $I = [c, 2c)$, the condition that $n \geq 10^7$ implies that $p_0 = \alpha \log(n)$ has a minimum value P_I over all $n \geq 10^7$, namely the least 2-power $P_I \geq c \log(10^7)$. We record these values in *column 5* of Table 4. For all but one of the intervals I , we have $P_I \geq 8$, and in the other case $P_I = 4$.

Case 2a: $n \geq 10^7$, $p_0 \geq 8$

If $n \geq 10^7$ and $p_0 \geq 8$, then Lemma 2.6 shows that $c(2p_0) - c(p_0) \leq 0$, so the second term in (4.2) can be bounded below on I using an *upper* bound $U(I)$ for the increasing function $\alpha \mapsto e^{-1/2\alpha}$ on I :

$$\frac{c(2p_0) - c(p_0)}{e^{1/2\alpha}} \geq (c(2p_0) - c(p_0))U(I). \tag{4.3}$$

Moreover, the first term in (4.2) can be bounded below on I using the lower bound, $L_1(I)$ say, of $e^{-1/2\alpha} - e^{-1/\alpha}$ on I obtained in Lemma 2.8. We list $L_1(I)$ in *column 2* of Table 4, and we have

$$c(p_0) \left(e^{-1/2\alpha} - e^{-1/\alpha} \right) \geq c(p_0)L_1(I) \tag{4.4}$$

on I . Now applying (4.3) and (4.4) to (4.2) yields

$$L(n, p_0) \geq c(p_0)L_1(I) + (c(2p_0) - c(p_0))U(I) - \frac{5}{10^7} \tag{4.5}$$

on I . To obtain a good estimate of the right hand side of estimate (4.5) for $n \geq 10^7$ and $p_0 \geq 8$, we use two different strategies, namely for the cases $8 \leq p_0 \leq 2^{16}$ (Case 2a (i)) and $p_0 \geq 2^{16}$ (Case 2a (ii)) as follows.

Case 2a (i): $n \geq 10^7$ and $2^{16} \geq p_0 \geq 8$

If $n \geq 10^7$, and if I is such that $P_I \geq 8$, and if $P_I \leq p_0 \leq 2^{16}$, then we compute $c(p_0)$ and $c(2p_0)$ explicitly for each 2-power in the interval $[P_I, 2^{16}]$ and substitute these values into (4.5) to obtain lower bounds for $L(n, p_0)$ for $n \geq 10^7$ and $P_I \leq p_0 \leq 2^{16}$. We record, in *column 6* of Table 4, the minimum value of these lower bounds obtained in (4.5).

This leaves the interval $I = [\frac{a}{8}, \frac{a}{4})$ for which $P_I = 4$, and in this case (4.5) is not applicable for all values of p_0 . For this I , we carry out the procedure in the

previous paragraph to find the minimum value, say L_I , for the lower bound in (4.5) for $n \geq 10^7$ and the values of p_0 for which this is valid, namely $8 \leq p_0 \leq 2^{16}$. We complete this case by comparing L_I with a lower bound in the case $p_0 = 4$, which we describe in Case 2b below.

Case 2a (ii): $n \geq 10^7$ and $p_0 \geq 2^{16}$

If $n \geq 10^7$ and $p_0 \geq 2^{16}$, then $c(p_0)$ is sufficiently close to 1 to make the lower bound $c(p_0) \geq 1$ effective. Also,

$$-0.000085 \leq c(2p_0) - c(p_0) \leq 0$$

by Lemma 2.6 and Corollary 2.7. Thus, (4.5) implies that

$$\begin{aligned} p_n(p_0) &\geq L(n, p_0) \geq c(p_0)L_1(I) + (c(2p_0) - c(p_0))U(I) - \frac{5}{10^7} \\ &\geq L_1(I) - 0.000085 U(I) - \frac{5}{10^7}. \end{aligned} \quad (4.6)$$

We record these lower bounds in *column 7* of Table 4.

Case 2b: $n \geq 10^7$, $p_0 = 4$ (and $I = [\frac{\alpha}{8}, \frac{\alpha}{4})$)

If $n \geq 10^7$, $I = [\frac{\alpha}{8}, \frac{\alpha}{4})$, and $p_0 = \alpha \log(n) = 4$, then an explicit calculation shows that $c(2p_0) - c(p_0) \geq 0$ and we have

$$\begin{aligned} p_n(4) &\geq L(n, 4) \geq c(8) \left(\frac{1}{n^{1/8}} - \frac{1}{n^{1/4}} \right) + \frac{c(8) - c(4)}{n^{1/4}} - \frac{5}{10^7} \\ &\geq c(8) \left(e^{-1/2\alpha} - e^{-1/\alpha} \right) + \frac{c(8) - c(4)}{e^{1/\alpha}} - \frac{5}{10^7}. \end{aligned} \quad (4.7)$$

We use the same method as before, except that we take a *lower* bound $L_2(I)$ for $e^{-1/\alpha}$ on I , rather than an upper bound for $e^{-1/2\alpha}$ on I . So we have, with $L_1(I)$ as in (4.4),

$$L(n, 4) \geq c(8)L_1(I) + (c(8) - c(4))L_2(I) - \frac{5}{10^7} \quad (4.8)$$

and we can now also record the minimum lower bound of $L(n, p_0)$ for all p_0 satisfying $P_I \leq p_0 \leq 2^{16}$, in *column 6* of Table 4 in the case $I = [\frac{\alpha}{8}, \frac{\alpha}{4})$.

Cases 1 and 2 cover all possibilities and *column 8* of Table 4 gives the overall lower bound for $p_n(p_0)$ for each interval I , which is the minimum value from columns 4, 6, and 7 of Table 4.

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6	Column 7	Column 8
Interval I	$L_1(I)$, see (4.4)	N_I	Lower bound for $p_n(p_0)$ from MAGMA $n \leq 10^7$	P_I , where $p_0 \geq P_I$ since $n \geq 10^7$ $n > 10^7$ (for Columns 5,6, and 7)	Lower bound for $L(n, p_0)$; $P_I \leq p_0 \leq 2^{16}$	Lower bound for $L(n, p_0)$; $p_0 \geq 2^{16}$	Overall lower bound for $p_n(p_0)$ $n \geq N_I$
$[\frac{a}{8}, \frac{a}{4}]$	0.0208331323	47	0.0169858815	4	0.0165662677	0.0208202311	0.0165662676
$[\frac{a}{4}, \frac{a}{2}]$	0.1246117974	7	0.1170040878	8	0.1224337255	0.1245788304	0.1170040878
$[\frac{a}{2}, a]$	0.2360679774	3	0.2391737036	16	0.2351203791	0.2360149446	0.2351203790
$[a, 2a]$	0.1681173890	2(10)	0.1531015975	32	0.1553674058	0.1680500661	0.1531015975
$[2a, 4a]$	0.1005004015	8(28)	0.0605468750	64	0.0854832385	0.1004245362	0.0605468750
$[4a, 8a]$	0.0549701083	16(64)	0.0307617187	128	0.0480726377	0.0548895705	0.0307617187
$[8a, 16a]$	0.0287501480	64(128)	0.0155029296	256	0.0210957674	0.0286671664	0.0155029296
$[16a, 32a]$	0.0147025988	128(256)	0.0065085752	512	0.0120580669	0.0146183675	0.0065085752

Table 4. Lower bounds on $p_n(p_0)$, $1 \leq p_0 \leq n$, $p_0 = \alpha \log(n)$.

5 Lower bounds for proportions of elements of arbitrary 2-part order

We now find lower bounds on the proportion of elements in S_n with arbitrary 2-part order 2^b , thus complementing the bounds given in Theorem 1.1. Equation (5.2) in part (b) of Theorem 5.1 is essentially proved in [3, Theorem 2.3].

Theorem 5.1. *The following statements hold:*

(a) *If $2 \leq 2^b \leq n/2$, then*

$$p_n(2^b) \geq c(2^{b+1}) \left(1 - \frac{1}{n}\right) \left(1 - \left(\frac{2^b e}{n + 2^{b+1}}\right)^{\frac{1}{2^{b+1}}}\right) n^{-1/2^{b+1}}, \quad (5.1)$$

and in particular

$$p_n(2^b) \geq K_b n^{-1/2^{b+1}},$$

where $K_b = c(2^{b+1})(1 - 2^{-b-1})(1 - (e/4)^{\frac{1}{2^{b+1}}})$.

(b) *If $2^b \leq n < 2^{b+1}$, then $p_n(2^b) = \frac{1}{2^b}$. Also*

$$p_n(1) = s_{-2}(n) \geq \sqrt{\frac{2}{\pi}} n^{-1/2} \left(1 - \frac{1}{n}\right) \geq \frac{1}{\sqrt{2\pi n}}. \quad (5.2)$$

Remark 5.2. Note that for fixed b , the lower bound for $p_n(2^b)$ in (5.1) tends to $c(2^{b+1})n^{-1/2^{b+1}}$ as $n \rightarrow \infty$.

Proof. For (5.1), we know from (1.1) that if $4 \leq 2^{b+1} \leq n$, then

$$\begin{aligned} p_n(2^b) &= s_{-2^{b+1}}(n) - s_{-2^b}(n) \\ &= \prod_{u=1}^{\lfloor n/2^{b+1} \rfloor} \left(1 - \frac{1}{2^{b+1}u}\right) - \prod_{m=1}^{\lfloor n/2^b \rfloor} \left(1 - \frac{1}{2^b m}\right) \end{aligned} \quad (5.3)$$

$$\begin{aligned} &= \prod_{u=1}^{\lfloor n/2^{b+1} \rfloor} \left(1 - \frac{1}{2^{b+1}u}\right) \left(1 - \prod_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \left(1 - \frac{1}{2^b m}\right)\right) \\ &= s_{-2^{b+1}}(n) \left(1 - \prod_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \left(1 - \frac{1}{2^b m}\right)\right) \\ &\geq s_{-2^{b+1}}(n)(1 - A), \end{aligned} \quad (5.4)$$

where

$$\prod_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \left(1 - \frac{1}{2^b m}\right) \leq A. \tag{5.5}$$

Now (5.5) holds if and only if

$$\sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \log\left(1 - \frac{1}{2^b m}\right) \leq \log A.$$

A left endpoint approximation of $\int_1^{\lfloor n/2^b \rfloor + 2} \log\left(1 - \frac{1}{2^b x}\right) dx$, with subintervals of length 2, is

$$\sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} 2 \log\left(1 - \frac{1}{2^b m}\right).$$

Since the function $x \mapsto \log\left(1 - \frac{1}{x}\right)$ is increasing, we have the inequalities

$$\begin{aligned} \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \log\left(1 - \frac{1}{2^b m}\right) &\leq \frac{1}{2} \int_1^{\lfloor \frac{n}{2^b} \rfloor + 2} \log\left(1 - \frac{1}{2^b x}\right) dx \\ &\leq \frac{1}{2} \int_1^{\frac{n}{2^b} + 2} (\log(2^b x - 1) - \log(2^b x)) dx. \end{aligned}$$

Calculating this integral gives us

$$\begin{aligned} \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \log\left(1 - \frac{1}{2^b m}\right) &\leq \frac{1}{2^{b+1}} \left((2^b x - 1) \log(2^b x - 1) - 2^b x \log(2^b x) \right) \Big|_1^{n/2^b + 2} \\ &= \frac{1}{2^{b+1}} \left((n + 2^{b+1} - 1) \log(n + 2^{b+1} - 1) \right. \\ &\quad \left. - (n + 2^{b+1}) \log(n + 2^{b+1}) \right. \\ &\quad \left. - (2^b - 1) \log(2^b - 1) + 2^b \log(2^b) \right). \end{aligned}$$

But Lemma 2.3 proves that if $x \geq 2$, then

$$\log(x) - \frac{2}{x} < \log(x - 1) < \log(x) - \frac{1}{x},$$

and thus we have

$$\begin{aligned} \sum_{\substack{m=1 \\ m \text{ odd}}}^{\lfloor n/2^b \rfloor} \log\left(1 - \frac{1}{2^b m}\right) &\leq \frac{1}{2^{b+1}} \left((n + 2^{b+1}) \log(n + 2^{b+1}) \right. \\ &\quad - 1 - \log(n + 2^{b+1} - 1) \\ &\quad - (n + 2^{b+1}) \log(n + 2^{b+1}) \\ &\quad \left. - (2^b - 1) \log(2^b - 1) + 2^b \log(2^b) \right) \\ &\leq \frac{1}{2^{b+1}} \left(-1 - 2^b (\log(2^b) - 2/2^b) + \log(2^b - 1) \right. \\ &\quad \left. + 2^b \log(2^b) - \log(n + 2^{b+1} - 1) \right) \\ &\leq \frac{1}{2^{b+1}} \left(1 + \log\left(\frac{2^b - 1}{n + 2^{b+1} - 1}\right) \right). \end{aligned}$$

Now we can define A using the inequality

$$\begin{aligned} \exp\left\{ \frac{1}{2^{b+1}} \left(1 + \log\left(\frac{2^b - 1}{n + 2^{b+1} - 1}\right) \right) \right\} &= e^{\frac{1}{2^{b+1}}} \left(\frac{2^b - 1}{n + 2^{b+1} - 1} \right)^{\frac{1}{2^{b+1}}} \\ &\leq e^{\frac{1}{2^{b+1}}} \left(\frac{2^b}{n + 2^{b+1}} \right)^{\frac{1}{2^{b+1}}} =: A. \end{aligned}$$

Thus by (5.4) and Theorem 2.1, we have

$$\begin{aligned} p_n(2^b) &\geq s_{-2^{b+1}}(n)(1 - A) \\ &\geq c(2^{b+1}) \left(1 - \frac{1}{n}\right) \left(1 - e^{\frac{1}{2^{b+1}}} \left(\frac{2^b}{n + 2^{b+1}}\right)^{\frac{1}{2^{b+1}}}\right) n^{-1/2^{b+1}}, \quad (5.6) \end{aligned}$$

and this proves (5.1). But $n \geq 2^{b+1}$, so

$$\begin{aligned} p_n(2^b) &\geq c(2^{b+1}) n^{-1/2^{b+1}} \left(1 - \frac{1}{2^{b+1}}\right) \left(1 - \left(\frac{2^b e}{2^{b+1} + 2^{b+1}}\right)^{\frac{1}{2^{b+1}}}\right) \\ &= c(2^{b+1}) \left(\frac{2^{b+1} - 1}{2^{b+1}}\right) \left(1 - \left(\frac{e}{4}\right)^{\frac{1}{2^{b+1}}}\right) n^{-1/2^{b+1}} = K_b n^{-1/2^{b+1}}, \end{aligned}$$

which proves $p_n(2^b) \geq K_b n^{-1/2^{b+1}}$. This proves (a).

To prove (b), we note that if $2^b \leq n < 2^{b+1}$, then $p_n(2^b) = 1 - s_{-2^b}(n)$ and the fact that $s_{-2^b}(n) = 1/2^b$ is well known (see [3, Lemma 2.2] for example). As noted above, since $p_n(1) = s_{-2}(n)$, (5.2) follows from [3, Theorem 2.3]. \square

Acknowledgments. The authors are grateful to an anonymous referee of an earlier version of our results for suggesting that the bounds in Theorem 1.2 hold and for sketching the proof of part (i).

Bibliography

- [1] M. Abért and B. Virág, Dimension and randomness in groups acting on rooted trees, *J. Amer. Math. Soc.* **18** (2005), no. 1, 157–192 (electronic).
- [2] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, National Bureau of Standards Applied Mathematics Series 55, U.S. Government Printing Office, Washington, 1964.
- [3] R. Beals, C. R. Leedham-Green, A. C. Niemeyer, C. E. Praeger and A. Seress, Permutations with restricted cycle structure and an algorithmic application, *Combin. Probab. Comput.* **11** (2002), no. 5, 447–464.
- [4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265.
- [5] P. Erdős and P. Turán, On some problems of a statistical group-theory. II, *Acta Math. Acad. Sci. Hungar.* **18** (1967), 151–163.
- [6] S. Guest and C. E. Praeger, Proportions of elements with given 2-part order in finite classical groups of odd characteristic, preprint (2012), <http://arxiv.org/abs/1007.2983v4>.
- [7] A. C. Niemeyer and C. E. Praeger, Estimating proportions of elements in finite groups of Lie type, *J. Algebra* **324** (2010), no. 1, 122–145.
- [8] S. Yalcinkaya, Construction of long root $SL(2, q)$ -subgroups in black box groups, preprint (2010), <http://arxiv.org/abs/1001.3184v1>.

Received May 20, 2012; revised May 27, 2012.

Author information

Simon Guest, Centre for the Mathematics of Symmetry and Computation (M019), The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia.

Current address: School of Mathematics, University of Southampton, Southampton, SO17 1BJ, UK.

E-mail: s.d.guest@soton.ac.uk

Cheryl E. Praeger, Centre for the Mathematics of Symmetry and Computation (M019), The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia; and King Abdulaziz University, Jeddah, Saudi Arabia.

E-mail: cheryl.praeger@uwa.edu.au