# Dixon's asymptotic without the classification of finite simple groups

Eberhard, S. (2023). Dixon's asymptotic without the classification of finite simple groups. *Random Structures and Algorithms*. Advance online publication. https://doi.org/10.1002/rsa.21205

**Published in:**
Random Structures and Algorithms

**Document Version:**
Publisher's PDF, also known as Version of record

Received: 17 July 2023 | Accepted: 29 November 2023

DOI: 10.1002/rsa.21205

RESEARCH ARTICLE

WILEY

# Dixon's asymptotic without the classification of finite simple groups

**Sean Eberhard**

Mathematical Sciences Research Centre, Queen's University Belfast, Belfast, UK

**Correspondence**
Sean Eberhard, Mathematical Sciences Research Centre, Queen's University Belfast, Belfast, BT7 1NN, UK.
Email: s.eberhard@qub.ac.uk

**Funding information**
Royal Society

**Abstract**

Without using the classification of finite simple groups (CFSG), we show that the probability that two random elements of $S_n$ generate a primitive group smaller than $A_n$ is at most $\exp\left(-c(n\log n)^{1/2}\right)$. As a corollary we get Dixon's asymptotic expansion

$$1 - 1/n - 1/n^2 - 4/n^3 - 23/n^4 - \cdots$$

for the probability that two random elements of $S_n$ (or $A_n$) generate a subgroup containing $A_n$.

KEYWORDS

alternating group, CFSG, permutation groups, primitive groups, random generation, symmetric group

## 1 | INTRODUCTION

We give a CFSG-free proof of the following result.

**Theorem 1.** *Let $G$ be the subgroup of $S_n$ generated by two random elements. The probability that $G$ is contained in a primitive subgroup of $S_n$ smaller than $A_n$ is bounded by* $\exp\left(-c(n\log n)^{1/2}\right)$ *for some $c > 0$.*

This improves [8, Theorems 1.3 and 1.6]. By combining with the results of [5] we have the following corollary. (See also [10, A113869].)

**Corollary 2.** *The probability that two random elements of $A_n$ generate the group is*

$$1 - 1/n - 1/n^2 - 4/n^3 - 23/n^4 - 171/n^5 - \cdots.$$

*The same asymptotic expansion is valid for the probability that two random elements of $S_n$ generate at least $A_n$.*

## 2 | SATISFACTION PROBABILITY FOR UNIMODAL WORDS

Let $F_2 = F\{x, y\}$ be the free group on two letters $x, y$. We write $\{x, y\}^*$ for the set of positive words, that is, the submonoid generated by $\{x, y\}$. Let $G = S_n = Sym(\Omega)$ for $\Omega = \{1, \dots, n\}$.

**Proposition 3.** *Let $u, v \in \{x, y\}^*$ be distinct and let $w = uv^{-1} \in F_2$. Let $\ell = \ell(w) = \ell(u) + \ell(v)$ be the length of $w$. For a random evaluation $\overline{w} = w(\overline{x}, \overline{y})$ with $\overline{x}, \overline{y} \in S_n$ uniformly random and independent, we have*

$$\text{Prob}(\overline{w} = 1) \leq (2\ell/n)^{\lfloor n/2\ell \rfloor}.$$

*Proof.* Write $w = w_1 \cdots w_\ell$ with $\ell > 0$ and $w_i \in \{x^{\pm 1}, y^{\pm 1}\}$ for each $i$. We may assume this expression is cyclically reduced.

We use the query model for random permutations (see [4] or [7, Section A.1]). We gradually expose a random permutation $\pi \in Sym(\Omega)$ by querying values of our choice. At every stage $\overline{x}$ and $\overline{y}$ are partially defined permutations. We may query the value of any $\pi \in \left\{\overline{x}^{\pm 1}, \overline{y}^{\pm 1}\right\}$ at any point $\omega \in \Omega$. If $\omega$ is already in the known domain of $\pi$, the known value is returned; this is a *forced choice*. Otherwise, a random value is chosen uniformly from the remaining possibilities (the complement of the known domain of $\pi^{-1}$); this is a *free choice*. If the result of a free choice is a point in the known domain of any of $\overline{x}^{\pm 1}, \overline{y}^{\pm 1}$ we say there was a *coincidence*. It is standard and easy to see that this process results in uniformly random permutations $\overline{x}$ and $\overline{y}$ once all values are revealed.

Begin by choosing any $\omega_1 \in \Omega$ and exposing the trajectory

$$\omega_1^{\overline{w}_1}, \omega_1^{\overline{w}_1\overline{w}_2}, \dots, \omega_1^{\overline{w}_1\cdots\overline{w}_\ell}.$$

Let $E_1$ be the event that $\omega_1^{\overline{w}_1\cdots\overline{w}_\ell} = \omega_1$. For this event to occur we claim it is necessary there was some coincidence among our queries of the form $\omega^{\overline{w}_t} = \omega_1$ (this is the crucial part of the argument). If $\ell(u) = 0$ or $\ell(v) = 0$ the argument is easy, so assume $u$ and $v$ have positive length. We may assume $w_1 = x$ and $w_\ell = y^{-1}$ since $w$ is cyclically reduced. If there is no coincidence of the given form, the trajectory of $\omega_1$ under $\bar{u}$ does not return to $\omega_1$, so $\omega_1$ cannot be added to the known domain of $\overline{y}$. Subsequently, during the negative part of the trajectory, unless there is a coincidence of the given form, $\omega_1$ can be added to the known domains of $\overline{x}^{-1}$ and $\overline{y}^{-1}$ only. Therefore at the final step $\omega_1$ is not in the known domain of $\overline{y}$, so if the final step is forced then the result is not $\omega_1$, and if the final step is free then the result is not $\omega_1$ by hypothesis. This proves the claim.

Since the probability that any given free choice results in $\omega_1$ is at most $1/(n - \ell)$, it follows by a union bound that

$$\text{Prob}\left(\omega_1^{\overline{w}} = \omega_1\right) \leq \ell/(n - \ell).$$

Conditional on the event $E_1$ choose a new point $\omega_2$ outside the trajectory of $\omega_1$, examine the trajectory of $\omega_2$, and so on. In general, at iteration $i$, conditional on the event $\bigcap_{j<i} E_j$ where $E_j = \left\{\omega_j^{\overline{w}} = \omega_j\right\}$, choose a point $\omega_i \in \Omega$ outside the union of the trajectories of $\omega_1, \dots, \omega_{i-1}$ and query the trajectory of $\omega_i$. In order for the event $E_i = \left\{\omega_i^{\overline{w}} = \omega_i\right\}$ to occur it is necessary that there be a coincidence of the form $\omega^{\overline{w}_t} = \omega_i$. Therefore

$$\text{Prob}\left(\omega_i^{w} = \omega_i \mid E_1, \dots, E_{i-1}\right) \leq \ell/(n - i\ell).$$

Let $k = \lfloor n/2\ell \rfloor$. Since the event $\{\overline{w} = 1\}$ is contained in $E_1 \cap \cdots \cap E_k$, it follows that

$$Prob(\overline{w} = 1) \leq \prod_{i=1}^{k} \frac{\ell}{n - i\ell} \leq \left(\frac{2\ell}{n}\right)^{\lfloor n/2\ell \rfloor}.$$

■

*Remark* 4. The proof above is essentially that of [9, Section 3]. An error in that argument was identified in [6], but the problem does not arise for words of the special form $w = uv^{-1}$, as explained in the third paragraph of the proof.

## 3 | THE ORDER OF THE GROUP

Now let $\overline{x}, \overline{y} \in S_n$ be uniformly random and let $G = \langle \overline{x}, \overline{y} \rangle$.

**Proposition 5.** *There is a constant* $c > 0$ *such that*

$$\text{Prob}\left(|G| < \exp\left(c(n \log n)^{1/2}\right)\right) \leq \exp\left(-c(n \log n)^{1/2}\right).$$

*Proof.* Consider the elements of $G$ of the form $\bar{u}$ with $u \in \{x, y\}^*$ and $\ell(u) < r$ (for some $r$). The number of such $u$ is $1 + 2 + \cdots + 2^{r-1} = 2^r - 1$. Applying the previous proposition, the probability that any two such $\bar{u}$ and $\bar{u}'$ are equal is bounded by

$$4^r(4r/n)^{\lfloor n/4r \rfloor} \leq \exp(c_1 r - c_2(n/r)\log(n/r)))$$

for some constants $c_1, c_2 > 0$. Choosing $r = c_3(n \log n)^{1/2}$ for a small enough constant $c_3 > 0$, we obtain a bound of the required form. Failing this event, $|G| \geq 2^r - 1$, so the result is proved. ■

A beautiful recent result of Sun and Wilmes [12, 13] (building on seminal work of Babai [1]) classifies primitive coherent configurations with more than $\exp(Cn^{1/3}(\log n)^{7/3})$ automorphisms. A corollary is a CFSG-free determination of the uniprimitive subgroups of $S_n$ of order greater than the same bound. Much stronger bounds for the order of 2-transitive groups have been known for a long time [2, 11]. Thus we know there are at most two conjugacy classes of primitive maximal subgroups $M < S_n$ apart from $A_n$ such that $|M| > \exp\left(Cn^{1/3}(\log n)^{7/3}\right)$, and each satisfies $|M| = \exp\left(O\left(n^{1/2} \log n\right)\right)$. Since the number of pairs of permutations lying in a common conjugate of a maximal subgroup $M$ is at most $1/[S_n : M]$, Theorem 1 follows.

*Remark* 6. This proof was essentially anticipated in [3, Remark 1].

FUNDING INFORMATION
SE is supported by the Royal Society.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

**ORCID**

*Sean Eberhard* https://orcid.org/0000-0003-3347-0976

## REFERENCES

1. L. Babai, *On the order of uniprimitive permutation groups*, Ann. Math. **113** (1981), no. 3, 553–568. MR621016.
2. L. Babai, *On the order of doubly transitive permutation groups*, Invent. Math. **65** (1981), no. 3, 473–484. MR643565.
3. L. Babai, *The probability of generating the symmetric group*, J. Comb. Theory Ser. A **52** (1989), no. 1, 148–153. MR1008166.
4. A. Broder and E. Shamir, "*On the second eigenvalue of random regular graphs*," 28th Annu. Symp. Found. Comput. Sci. (sfcs 1987), IEEE, Piscataway, NJ, 1987, pp. 286–294.
5. J. D. Dixon, *Asymptotics of generating the symmetric and alternating groups*, Electron. J. Comb. **12** (2005), R56. MR2180793.
6. S. Eberhard. The trivial lower bound for the girth of $S_n$. arXiv preprint arXiv:1706.09972, June 2017.
7. S. Eberhard and U. Jezernik, *Babai's conjecture for high-rank classical groups with random generators*, Invent. Math. **227** (2022), no. 1, 149–210. MR4359476.
8. S. Eberhard and S.-C. Virchow, *The probability of generating the symmetric group*, Combinatorica **39** (2019), no. 2, 273–288. MR3962902.
9. A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virág, *On the girth of random Cayley graphs*, Random Struct. Algoritm. **35** (2009), no. 1, 100–117. MR2532876.
10. OEIS Foundation Inc. *The on-line Encyclopedia of integer sequences*. 2023 http://oeis.org.
11. L. Pyber, *On the orders of doubly transitive permutation groups, elementary estimates*, J. Comb. Theory Ser. A **62** (1993), no. 2, 361–366. MR1207742.
12. X. Sun and J. Wilmes, "*Faster canonical forms for primitive coherent configurations: Extended abstract*," Proc. 47th Annu. ACM Symp. Theory Comput., ACM, New York, 2015, pp. 693–702.
13. X. Sun and J. Wilmes. Structure and automorphisms of primitive coherent configurations. arXiv preprint arXiv: 1510.02195, October 2015.

**How to cite this article:** S. Eberhard, *Dixon's asymptotic without the classification of finite simple groups*, Random Struct. Alg. (2023), 1–4. https://doi.org/10.1002/rsa.21205