

The proportion of derangements characterizes the symmetric and alternating groups

Bjorn Poonen¹ | Kaloyan Slavov²
¹Department of Mathematics,
Massachusetts Institute of Technology,
Cambridge, Massachusetts, USA

²Department of Mathematics, ETH
Zürich, Zurich, Switzerland

Correspondence

Kaloyan Slavov, Department of
Mathematics, ETH Zürich, Rämistrasse
101, 8006 Zürich, Switzerland.
Email: kaloyan.slavov@math.ethz.ch

Funding information

National Science Foundation,
Grant/Award Numbers: DMS-1601946,
DMS-2101040; Simons Foundation,
Grant/Award Numbers: #402472,
#550033; SNSF

Abstract

Let G be a subgroup of the symmetric group S_n . If the proportion of fixed-point-free elements in G (or a coset) equals the proportion of fixed-point-free elements in S_n , then $G = S_n$. The analogue for A_n holds if $n \geq 7$. We give an application to monodromy groups.

MSC (2020)

20B35 (primary), 11A63, 14E20, 14G15, 20B10 (secondary)

1 | INTRODUCTION

1.1 | Derangements in permutation groups

Motivated by an application to monodromy groups, we prove the following.

Theorem 1.1. *Let G be a subgroup of the symmetric group S_n for some $n \geq 1$. Let C be a coset of G in S_n . If*

$$\frac{|\{\sigma \in C : \sigma \text{ has no fixed points}\}|}{|C|} = \frac{|\{\sigma \in S_n : \sigma \text{ has no fixed points}\}|}{|S_n|}, \quad (1)$$

then $G = C = S_n$.

Elements of S_n with no fixed points are called derangements. Let D_n be the number of derangements in S_n . The right side of (1) is

$$\frac{D_n}{n!} = \sum_{i=0}^n \frac{(-1)^i}{i!};$$

see [10, Example 2.2.1], for instance. When the denominator of $D_n/n!$ in lowest terms is $n!$, the conclusion of Theorem 1.1 follows immediately, but controlling $\gcd(D_n, n!)$ in general is nontrivial. Our proof requires an irrationality measure for e , divisibility properties of D_n , and a bound on the orders of primitive permutation groups.

Remark 1.2. The proof shows also that for $n \geq 5$, if C is not necessarily a coset but just any subset of S_n having the same size as G , then (1) implies that G is A_n or S_n . In fact, we prove that if a subgroup G of S_n has order divisible by the denominator of $D_n/n!$, then G is A_n or S_n .

Remark 1.3. We also prove an analogue of Theorem 1.1 in which both appearances of S_n on the right side of (1) are replaced by the alternating group A_n for some $n \geq 7$; see Theorem 5.1. But there are counterexamples for smaller alternating groups. For example, the order 10 dihedral group in A_5 has the same proportion of derangements as A_5 , namely $4/10 = 24/60$.

1.2 | Application to monodromy

Let $\mathbb{F}_q$ be the finite field of q elements. Let $f(T) \in \mathbb{F}_q[T]$ be a polynomial of degree n . Birch and Swinnerton-Dyer [2] define what it means for f to be ‘general’ and estimate the proportion of field elements in the image of a general f :

$$\frac{|f(\mathbb{F}_q)|}{q} = 1 - \sum_{i=0}^n \frac{(-1)^i}{i!} + O_n(q^{-1/2}).$$

More generally, let $f: X \rightarrow Y$ be a degree n generically étale morphism of schemes of finite type over $\mathbb{F}_q$, with Y geometrically integral. The geometric and arithmetic monodromy groups G and A are subgroups of S_n fitting in an exact sequence

$$1 \longrightarrow G \longrightarrow A \longrightarrow \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q) \longrightarrow 1$$

for some $r \geq 1$; see [4, Section 4] for an exposition. Let C be the coset of G in A mapping to the Frobenius generator of $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. Let M be a bound on the geometric complexity of X and Y . Assume that $Y(\mathbb{F}_q) \neq \emptyset$, which is automatic if q is large relative to M . Then the Lang–Weil bound implies

$$\frac{|f(X(\mathbb{F}_q))|}{|Y(\mathbb{F}_q)|} = \frac{|\{\sigma \in C : \sigma \text{ has at least one fixed point}\}|}{|C|} + O_{n,M}(q^{-1/2}); \quad (2)$$

see [4, Theorem 3], for example. In particular, if $G = S_n$, then

$$\frac{|f(X(\mathbb{F}_q))|}{|Y(\mathbb{F}_q)|} = 1 - \sum_{i=0}^n \frac{(-1)^i}{i!} + O_{n,M}(q^{-1/2}). \quad (3)$$

We prove a *converse*, that an estimate as in (3) on the proportion of points in the image implies that the geometric monodromy group of f is the full symmetric group S_n :

Corollary 1.4. *Given n and M , there exists an effectively computable constant $c = c(n, M)$ such that for any $f : X \rightarrow Y$ as above, with $\deg f = n$ and the complexities of X and Y bounded by M , if*

$$\frac{|f(X(\mathbb{F}_q))|}{|Y(\mathbb{F}_q)|} = 1 - \sum_{i=0}^n \frac{(-1)^i}{i!} + \epsilon, \quad \text{where } |\epsilon| < \frac{1}{n!} - cq^{-1/2},$$

then $G = S_n$.

Proof. Combine (2) and Theorem 1.1. □

Remark 1.5. We originally proved Corollary 1.4 in order to prove a version of [8, Theorem 1.9], about specialization of monodromy groups, but later we found a more natural argument.

1.3 | Structure of the paper

The proof of Theorem 1.1 occupies the rest of the paper, which is divided in sections according to the properties of G . Throughout, we assume that G , C , and n are such that (1) holds. The cases with $n \leq 4$ can be checked directly, so assume that $n \geq 5$ and $G \neq S_n$.

2 | PRIMITIVE PERMUTATION GROUPS

The proportion of derangements in A_n is given by the inclusion–exclusion formula; it differs from $D_n/n!$ by the nonzero quantity $\pm(n-1)/n!$. The proportion for S_n is the average of the proportions for A_n and $S_n - A_n$, so the proportion for $S_n - A_n$ also differs from $D_n/n!$. Thus $G \neq A_n$.

Suppose that G is primitive, $n \geq 5$, and $G \neq A_n, S_n$. The main theorem in [9]¹ gives $|G| < 4^n$. On the other hand, $D_n/n!$ is close to $1/e$ and hence cannot equal a rational number with small denominator; this will show that $|G|$ is at least about $\sqrt{n!}$. These will give a contradiction for large n . We now make this precise.

Let $a = |\{\sigma \in C : \sigma \text{ has no fixed points}\}|$ and $b = |C| = |G|$, so $a \leq b = |G| < 4^n$. Then

$$\left| \frac{a}{b} - \frac{1}{e} \right| = \left| \frac{D_n}{n!} - \frac{1}{e} \right| < \frac{1}{(n+1)!}.$$

No rational number with numerator ≤ 4 is within $1/6!$ of $1/e$, so $a \geq 5$. By the main result of [7] (see also [1]),

$$\left| e - \frac{b}{a} \right| > \frac{\log \log a}{3a^2 \log a}.$$

¹ This is independent of the classification of finite simple groups. Using the classification, [6] gives better bounds.

Combining the two displayed inequalities yields

$$\frac{1}{(n+1)!} > \left| \frac{a}{b} - \frac{1}{e} \right| = \frac{a}{be} \left| e - \frac{b}{a} \right| > \frac{1}{be} \cdot \frac{\log \log a}{3a \log a} > \frac{\log \log 4^n}{3e(4^n)^2 \log 4^n}; \quad (4)$$

the last step uses that $a, b < 4^n$ and that $\frac{\log \log x}{x \log x}$ is decreasing for $x \geq 5$. Inequality (4) implies $n \leq 41$.

Let d_n be the denominator of the rational number $\frac{D_n}{n!} = \frac{a}{b}$. Then $d_n \mid b$, so $d_n \leq b < 4^n$. For $11 < n \leq 41$, the inequality $d_n < 4^n$ fails. For $n \leq 11$, a Magma computation [5] shows that there are no degree n primitive subgroups $G \neq A_n, S_n$ for which $d_n \mid b$.

3 | IMPRIMITIVE BUT TRANSITIVE PERMUTATION GROUPS

Suppose that G is imprimitive but transitive. Then G preserves a partition of $\{1, \dots, n\}$ into l subsets of equal size k , for some $k, l \geq 2$ with $kl = n$. The subgroup of S_n preserving such a partition has order $(k!)^l l!$ (it is a wreath product $S_k \wr S_l$). Thus $|G|$ divides $(k!)^l l!$.

For a prime p , let ν_p denote the p -adic valuation. Since $\frac{a}{|G|} = \frac{D_n}{n!}$, every prime $p \nmid D_n$ satisfies $\nu_p(n!) \leq \nu_p(|G|) \leq \nu_p((k!)^l l!) \leq \nu_p(n!)$. Thus for every prime $p \nmid D_n$, the inequality $\nu_p((k!)^l l!) \leq \nu_p(n!)$ is an equality. The third of the three following lemmas will prove that this is impossible for $n \geq 5$.

Lemma 3.1. *Let $k, l \geq 2$ and let p be a prime. The inequality*

$$\nu_p((k!)^l l!) \leq \nu_p((kl)!) \quad (5)$$

is an equality if and only if at least one of the following holds:

- k is a power of p ;
- there are no carry operations in the l -term addition $k + \dots + k$ when k is written in base p (in particular, $l < p$).

Proof. Let $s_p(k)$ denote the sum of the p -adic digits of a positive integer k ; then $\nu_p(k!) = \frac{k - s_p(k)}{p-1}$. Thus equality in (5) is equivalent to equality in

$$l + s_p(kl) \leq ls_p(k) + s_p(l). \quad (6)$$

We always have

$$l + s_p(kl) \leq l + s_p(k)s_p(l) \leq ls_p(k) + s_p(l); \quad (7)$$

the first follows from $s_p(kl) \leq s_p(k)s_p(l)$, and the second is simply

$$(s_p(k) - 1)(l - s_p(l)) \geq 0.$$

Thus equality in (6) is equivalent to equality in both inequalities of (7).

The second inequality of (7) is an equality if and only if either k is a power of p or $l < p$; in each case, we must check when equality holds in the first inequality (7), that is, when $s_p(kl) = s_p(k)s_p(l)$. If k is a power of p , then it holds. If $l < p$, then it holds if and only if $s_p(kl) = ls_p(k)$, which holds if and only if there are no carry operations in the l -term addition $k + \dots + k$ when k is written in base p . $\square$

The following lemma will help us produce primes p not dividing D_n .

Lemma 3.2. *For $0 \leq m \leq n$, we have $D_n \equiv (-1)^{n-m} D_m \pmod{n-m}$. In particular,*

$$D_n \equiv \pm 1 \pmod{n} \quad (8)$$

$$D_n \equiv \pm 1 \pmod{n-2} \quad (9)$$

$$D_n \equiv \pm 2 \pmod{n-3}. \quad (10)$$

Proof. Reduce each term in D_n modulo $n-m$; most of them are 0. $\square$

Lemma 3.3. *Let $k, l \geq 2$. Set $n = kl$ and assume $n > 4$. Then there exists a prime $p \nmid D_n$ such that*

$$v_p((k!)^l l!) < v_p(n!).$$

Proof. **Case 1. $l \geq 3$ and $n-2$ is not a power of 2.**

Let $p \geq 3$ be a prime with $p \mid n-2$. By (9), $p \nmid D_n$, so $v_p((k!)^l l!) = v_p(n!)$. Apply Lemma 3.1. If k is a power of p , then p divides k , which divides n , so $p \mid n - (n-2) = 2$, contradicting $p \geq 3$. Otherwise, there are no carry operations in the l -term addition $k + \dots + k$ in base p . This is impossible because the last digit of n is 2 (since $p \mid n-2$ and $p \geq 3$) and $l \geq 3$.

Case 2. $l = 2$.

Then $2 \mid n$. By (8), $2 \nmid D_n$. By Lemma 3.1, k is a power of 2 (since $l < 2$ is violated). Thus $n = 2k$ is a power of 2.

Since $n \geq 5$, there exists a prime $p \mid n-3$. Since n is a power of 2, this implies $p \geq 5$. By (10), $p \nmid D_n$. Apply Lemma 3.1. Note that k is not a power of p , since k is a power of 2 and $p \neq 2$. Therefore, there are no carry operations in $k + k = n$, so the last digit of n is even. But $p \mid n-3$ and $p \geq 5$, so the last digit of n is 3.

Case 3. $l = 3$ and $n-2$ is a power of 2.

Then $3 \mid n$. By (8), $3 \nmid D_n$. By Lemma 3.1, k must be a power of 3 (since $l < 3$ is violated). Then $n = 3k$ is a power of 3, contradicting the fact that n is even.

Case 4. $l > 3$ and $n-2$ is a power of 2.

In particular, $n = kl > 6$. Then $n-3$ is not a power of 3, because otherwise we would have a solution to $3^u = 2^v - 1$ with $u > 1$, whereas the only solution in positive integers is $(u, v) = (1, 2)$ (proof: $3 \mid 2^v - 1$, so v is even, so $2^{v/2} - 1$ and $2^{v/2} + 1$ are powers of 3 that differ by 2, so they are 1 and 3).

Let $p \neq 3$ be a prime divisor of $n-3$. Then $p \geq 5$. Apply (10) and Lemma 3.1. If k is a power of p , then $p \mid n$, so $p \mid n - (n-3) = 3$, contradicting $p \neq 3$. Therefore, there are no carry operations

in the l -term addition $k + \dots + k$. This is impossible, since the last digit of kl is 3 (since $p \mid n - 3$ and $p \geq 5$) and $l > 3$. $\square$

4 | INTRANSITIVE PERMUTATION GROUPS

Suppose that G is intransitive. Then G embeds in $S_u \times S_v \subset S_n$ for some $u, v \geq 1$ with $u + v = n$.

Consider a prime $p \mid n$. By (8), $p \nmid D_n$. Then, analogously to the second paragraph of Section 3, $\nu_p(n!) \leq \nu_p(|G|) \leq \nu_p(u!v!) \leq \nu_p(n!)$, so $\nu_p(u!) + \nu_p(v!) = \nu_p(n!)$; equivalently, $s_p(u) + s_p(v) = s_p(n)$. So there are no carry operations in $u + v$. Let $e = \nu_p(n)$, so the last e base p digits of n are zero; then the same holds for u and v . In other words, $p^e \mid u, v$ as well. Since this holds for each $p \mid n$, we conclude that $n \mid u, v$. This contradicts $0 < u, v < n$.

This completes the proof of Theorem 1.1.

5 | ALTERNATING GROUP

Theorem 5.1. *Let G be a subgroup of the symmetric group S_n for some $n \geq 7$. Let C be a coset of G in S_n having the same proportion of fixed-point-free elements as A_n . Then $G = A_n$.*

Remark 5.2. For $n \leq 6$, the subgroups of S_n other than A_n for which some coset has the same proportion as A_n , up to conjugacy, are:

- the order 4 subgroup of S_4 generated by (1423) and (12)(34);
- the order 4 subgroup of S_4 generated by (34) and (12)(34);
- the order 8 subgroup of S_4 ;
- the subgroups of S_5 of order 5, 10, or 20;
- the order 36 subgroup of S_6 generated by (1623)(45), (12)(36), (124)(365), and (142)(365);
- the order 36 subgroup of S_6 generated by (13)(25)(46), (14)(36), (154)(236), and (145)(236).

The proof of Theorem 5.1 follows the proof of Theorem 1.1; we highlight only the differences. The proportion of fixed-point-free elements in A_n is $E_n/n!$, where $E_n := D_n + (-1)^{n-1}(n-1)$.

5.1 | Primitive permutation groups

Suppose $G \neq A_n$. The first paragraph of Section 2 shows that $G \neq S_n$. For $7 \leq n \leq 13$, we use Magma to check Theorem 5.1 for each primitive subgroup of S_n . So assume $n \geq 14$. Define a and b as in Section 2. We have

$$\left| \frac{a}{b} - \frac{1}{e} \right| = \left| \frac{E_n}{n!} - \frac{1}{e} \right| \leq \left| \frac{E_n - D_n}{n!} \right| + \left| \frac{D_n}{n!} - \frac{1}{e} \right| < \frac{n-1}{n!} + \frac{1}{(n+1)!} = \frac{n^2}{(n+1)!}.$$

No a/b with $a < 5$ is within $15^2/16!$ of $1/e$, so $a \geq 5$. Inequality (4) with $1/(n+1)!$ replaced by $n^2/(n+1)!$ implies $n \leq 49$.

Let e_n be the denominator of $E_n/n!$, so e_n divides $|G|$, which is less than 4^n . But for $13 < n \leq 49$, the inequality $e_n < 4^n$ fails.

5.2 | Imprimitive permutation groups that preserve a partition into blocks of equal size

To rule out imprimitive permutation groups that preserve a partition into l blocks of size k , we argue as in Section 3, but with Lemma 3.3 replaced by the following.

Lemma 5.3. *Let $k, l \geq 2$. Set $n = kl$ and assume $n > 6$. Then there exists a prime $p \nmid E_n$ such that*

$$\nu_p((k!)^l l!) < \nu_p(n!).$$

Proof of Lemma 5.3. For each integer $n \in (6, 30]$, we check directly that there exists a prime $p \in (n/2, n]$ such that $p \nmid E_n$. Assume from now on that $n > 30$.

Suppose the statement is false. Then whenever a prime p satisfies $p \nmid E_n$, (5) is an equality and Lemma 3.1 applies.

By using $D_n \equiv (-1)^{n-s} D_s \pmod{n-s}$ and $E_n = D_n + (-1)^{n-1}(n-1)$, we obtain

$$E_n \equiv 2(-1)^n \pmod{n} \tag{11}$$

$$E_n \equiv 4(-1)^{n-1} \pmod{n-3} \tag{12}$$

$$E_n \equiv 6(-1)^n \pmod{n-4} \tag{13}$$

$$E_n \equiv (-1)^{n-1} 2^4 \times 3 \pmod{n-5} \tag{14}$$

Case 1. $n - 4$ is a power of 2.

Then $n - 3$ is not a power of 3 because otherwise, we have a solution to $3^u - 1 = 2^v$ with $u \geq 3$; working modulo 4 shows that u is even, and factoring the left side leads to a contradiction. Let $p \neq 3$ be a prime with $p \mid n - 3$. Since $n - 3$ is odd, $p \geq 5$. By (12), $p \nmid E_n$, so we have one of the conclusions of Lemma 3.1.

If k is a power of p , then $p \mid k \mid n$, which, combined with $p \mid n - 3$ gives $p = 3$, a contradiction.

Suppose that there is no carry in $k + \dots + k$ (l terms). This sum has last digit 3 in base p , so $l = 3$, so $3 \mid n$, and hence $3 \nmid E_n$ by (11). Apply Lemma 3.1 for the prime 3. Since $l < 3$ is violated, we deduce that k is a power of 3. Then $n = kl$ is also a power of 3, but this contradicts the fact that n is even.

Case 2. $n - 3$ is a power of 2 and $l \neq 2, 4$.

Then $n - 4$ is odd and is not a power of 3. Let $p \neq 3$ be a prime with $p \mid n - 4$. Then $p \geq 5$, so $p \nmid E_n$ by (13). If k is a power of p , then $p \mid k \mid n$, which contradicts $p \mid n - 4$ since $p \geq 5$. If there are no carry operations in the l -term addition $k + \dots + k$ (which has last digit 4 in base p), then $l = 2$ or $l = 4$, contrary to assumption.

Case 3. $l = 3$.

Then $3 \mid n$, hence $3 \nmid E_n$ by (11). Apply Lemma 3.1 for the prime 3. Since $3 < l$ is violated, k is a power of 3. Then $n = kl$ is also a power of 3. Then $n - 4$ is odd and not divisible by 3. Let q be a prime with $q \mid n - 4$. Then $q \geq 5$, and hence $q \nmid E_n$ by (13). Since k is a power of 3, it is not a power of q . So there is no carry in $k + k + k$ in base q . But this sum has last digit 4 in base q , which is a contradiction.

Case 4. $l \neq 2, 4$.

By the previous cases, we may assume in addition that $n - 4$ and $n - 3$ are not powers of 2 and $l \neq 3$.

Let $p \neq 2$ be a prime with $p \mid n - 3$. Then $p \nmid E_n$ by (12). Since the l -term addition $k + \dots + k$ has last digit 3 and $l \neq 3$, there is some carry. Therefore k is a power of p . Then $p \mid k \mid n$, which, combined with $p \mid n - 3$, gives $p = 3$. In particular, $3 \mid n$.

Let $q \neq 2$ be a prime with $q \mid n - 4$. Since $3 \mid n$, we have $q \neq 3$ so $q \geq 5$. By (13), $q \nmid E_n$. If k is a power of q , then $q \mid n$, hence $q \mid 4$ — contradiction. Therefore there is no carry in the l -term addition $k + \dots + k$ in base q . This sum has last digit 4 and $l \neq 2, 4$, so this case is impossible.

Case 5. $l = 2$ or $l = 4$.

Then n is even, so $n - 3$ and $n - 5$ are odd.

Subcase 5.1: $n - 3$ is not a power of 3.

Let $p \neq 3$ be a prime such that $p \mid n - 3$. Then $p \geq 5$ and $p \nmid E_n$ by (12). If k is a power of p , then $p \mid k \mid n$, giving $p = 3$, which is a contradiction. However, there is carry in the l -term addition $k + \dots + k$ because the sum has last digit 3, and l is 2 or 4.

Subcase 5.2: $n - 3$ is a power of 3 but $n - 5$ is not a power of 5.

Let $p \neq 5$ be a prime with $p \mid n - 5$. Then $p \geq 7$ and we apply the argument of subcase 5.1: an l -term sum $k + \dots + k$ cannot have last digit 5 in base p .

Subcase 5.3: $n - 3 = 3^a$ and $n - 5 = 5^b$ for some $a, b \geq 1$.

Then $3^a - 5^b = 2$, so $a = 3$ and $b = 2$ by [3, Theorem 4.06]. This contradicts $n > 30$. $\square$

5.3 | Intransitive subgroups

As in Section 4, G embeds in $S_u \times S_v \subset S_n$ for some $u, v \geq 1$ with $u + v = n$. Write $n = 2^s m$, where $s \geq 0$ and $2 \nmid m$. The argument in Section 4 for odd p with E_n in place of D_n and (11) in place of (8) implies $m \mid u, v$. Thus $s \geq 1$.

If $s = 1$, then $n = 2m$, so $u = v$. This case is covered in Section 5.2.

Suppose that $s \geq 2$. Then $4 \mid n$, so (11) implies that $E_n/2$ is odd. Using $\frac{a}{|G|} = \frac{E_n/2}{n!/2}$, we obtain $\nu_2(n!/2) \leq \nu_2(|G|) \leq \nu_2(u!v!) \leq \nu_2(n!)$. If the last inequality is an equality, then the same argument used in Section 4 shows that $\nu_2(u) = \nu_2(v) = \nu_2(n)$; combining this with $m \mid u, v$ shows that $n \mid u, v$, a contradiction. Therefore the first two inequalities must be equalities, so $\nu_2(u!v!) = \nu_2(n!) - 1$; equivalently, $s_2(u) + s_2(v) = s_2(n) + 1$. This means there is exactly one carry operation in $u + v$ in base 2. This is possible only when $2^{s-1} \mid u, v$. Also, $m \mid u, v$, so $n/2 \mid u, v$, so again $u = v$, and this case is covered in Section 5.2.

ACKNOWLEDGEMENTS

We thank Andrew Sutherland for useful discussions concerning Section 2 and specifically for drawing our attention to [7]. We thank Michael Bennett and Samir Siksek for suggesting references for the solution of $3^a - 5^b = 2$. We also thank the referees for comments.

B.P. was supported in part by National Science Foundation grants DMS-1601946 and DMS-2101040 and Simons Foundation grants #402472 and #550033. K.S. was supported by NCCR SwissMAP of the SNSF.

Open access funding provided by Eidgenössische Technische Hochschule Zurich.

JOURNAL INFORMATION

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. H. Alzer, *On rational approximation to e* , J. Number Theory **68** (1998), no. 1, 57–62. MR1492888.
2. B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. **5** (1959), 417–423. MR113844.
3. J. L. Brenner and L. L. Foster, *Exponential Diophantine equations*, Pacific J. Math. **101** (1982), no. 2, 263–301. MR675401.
4. A. Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, Int. Math. Res. Not. **2021** (2021), no. 14, 10409–10441. MR4285725.
5. 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. Computational algebra and number theory (London, 1993). Magma is available at <http://magma.maths.usyd.edu.au/magma/>. MR1484478.
6. A. Maróti, *On the orders of primitive groups*, J. Algebra **258** (2002), no. 2, 631–640. MR1943938.
7. T. Okano, *A note on the rational approximations to e* , Tokyo J. Math. **15** (1992), no. 1, 129–133. MR1164191.
8. B. Poonen and K. Slavov, *The exceptional locus in the Bertini irreducibility theorem for a morphism*, Int. Math. Res. Not. **2022** (2022), no. 6, 4503–4513. MR4391895.
9. C. E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bull. Lond. Math. Soc. **12** (1980), no. 4, 303–307. MR576980.
10. R. P. Stanley, *Enumerative combinatorics. Volume 1*, 2nd ed., Cambridge Stud. Adv. Math., vol. 49, Cambridge Univ. Press, Cambridge, 2012. MR2868112.