STATISTICAL GROUP THEORY

ELAN BECHOR

Abstract. This paper examines two major results concerning the symmetric group, S_n. The first result, Landau's theorem, gives an asymptotic formula for the maximum order of an element in S_n, and the second, Dixon's Theorem, settled an open conjecture concerning the probability that two randomly selected elements of S_n will generate A_n or S_n.

1. Introduction

The field of statistical group theory was born in the 1960s with the series of papers by Erdős and Turán that gave a statistical characterization of the symmetric group (see, for example, [5]). It is an easy exercise in induction to show that, for example, if and element of S_n is chosen uniformly at random, the length of the cycle containing 1 is distributed uniformly. On the other hand, the two authors show that the order of elements in S_n are asymptotically normally distributed. This paper will give two examples of proofs on the symmetric group: one "classical", the other statistical in the style of Erdős and Turán. Landau's theorem, proved in 1902, states that the maximum order of an element in S_n is asymptotic to $e^{\sqrt{n \log n}}$. Dixon's theorem states that as n goes to infinity, if two elements are selected from S_n uniformly at random, the probability that these two elements generate A_n or S_n approaches 1. Both proofs are interesting in that they use both combinatorial and number-theoretical techniques.

2. A Proof of Landau's Theorem

The order of an element x in a group is defined as the smallest non-negative integer n such that $x^n = 1$. It is not difficult to prove that for an element x in S_n with cycle lengths a_1, a_2, ..., a_k, the order of x is $\operatorname{lcm}(a_1, a_2, \ldots, a_k)$. Landau's Theorem, proved in 1902, states that the maximum order of an element in S_n is asymptotic to $e^{\sqrt{n \log n}}$. The proof in this paper follows that of Miller [6].

Definition 2.1. The Landau function $G(n)$ is defined as the maximum order of an element in S_n. Equivalently,

$$G(n) = \max\{\operatorname{lcm}(a_1, a_2, \ldots, a_k) : \sum a_i = n\}$$

Definition 2.2. If m is any natural number greater than 1 and has prime factorization $q_1^{e_1} q_2^{e_2} \ldots q_k^{e_k}$, define $S(m) = \sum_{i=1}^{k} q_i^{e_i}$

The following lemma will allow us to relate the sum of the prime factors of a given number to the Landau function.

Lemma 2.3. *If* $\operatorname{lcm}(a_1, a_2, \ldots, a_k) = m$*,* $S(m) \leq \sum_{i=1}^{k} a_i$

Date: 29 July 2008.

Proof. Given m, take $a_1, a_2, \dots, a_k$ with $\operatorname{lcm}(a_1, a_2, \dots, a_k) = m$ such that $\sum a_i$ is minimal. Each a_1 is greater than 1 since if $a_i = 1$ for any i, then a_i can be removed to get a smaller sum, contradicting minimality. Moreover, each a_i is a prime power. For if not, we may decompose a_i into integers b and c such that $a_i = bc$ and $\gcd(a, b) = 1$ where neither a nor b are 1. Assuming without loss of generality $c > b > 1$, we have that $b + c \leq b + c(b-1) = bc + (b - c) < bc$ and hence we can construct a new minimal set, $a_1,\ a_2, \dots, a_{i-1}, b, c, a_{i+1}, \dots, a_k$ with least common multiple m (since b and c were relatively prime).

Finally, the p_is must be distinct, since only the p_i with the largest exponent contributes to the least common multiple, so any smaller power may be removed to get a smaller sum, contradicting minimality. After these reductions, then, we have the $\operatorname{lcm}(p_1^{e_1}, p_2^{e_2}, \dots, p_k^{e_k}) = m$, so the set of a_i with minimal sum is exactly the prime factorization of m. This means that $S(m) = \sum_{i=1}^{k} a_i$ for the minimal case and hence that in general $S(m) \leq \sum_{i=1}^{k} a_i$. □

Hence we have the following two corollaries, which reduce calculating $G(n)$ to a purely number theoretic question.

Corollary 2.4. *S_n contains an element of order m if and only if $S(m) \leq n$*

Proof. If $S(m) \leq n$, then if m has prime decomposition $q_1^{e_1},\ \dots,\ q_k^{e_k}$, there is an element of S_n containing one cycle each of lengths $q_i^{e_i}$ for $i = 1,\ \dots,\ k$ with the remaining points fixed. On the other hand, if there is a partition of n with least common multiple of m, then by the previous lemma, $S(m) \leq n$. □

This gives us the following:

Corollary 2.5. $G(n) = \max\limits_{S(m)\leq n} m$

Definition 2.6. Define P to be the unique prime such that $\sum_{p<P} p \leq n$ while $\sum_{p\leq P} p > n$ and let $F(n) = \prod\limits_{p<P} p$.

$F(n)$ represents the order of an obvious candidate for $G(n)$, i.e. the one with disjoint cycles with lengths corresponding to the first $\pi(P-1)$ primes. The goal is to prove that $\log F(n) \sim \log G(n)$ and then to show that $\log F(n) \sim \sqrt{n \log n}$.

Lemma 2.7. *Let $q_1 < \dots < q_s$ be the primes dividing $G(n)$. Then $\sum_{i=1}^{s} \log q_i < 2 + \log F(n) + \log P$*

Proof. We note that

$$\sum_{j=1}^{s} q_j \leq S(G(n)) \leq n < \sum_{p\leq P} p.$$

Define $q_1, \dots, q_t$ to be the primes dividing $G(n)$ that do not exceed P, and p_1, $\dots$, p_r to be the odd primes not dividing $G(n)$ that do not exceed P. Then by subtracting $q_1 + \dots + q_t$ from above, we have

$$\sum_{i=t+1}^{s} q_i \leq 2 + \sum_{i=1}^{r} p_i$$

By definition, $q_j > P$ whenever $j > t$, and for all $i = 1,\ \dots,\ r$, $p_i < P$. We note that $\frac{\log x}{x}$ is a decreasing function, so that if $a \leq b$, $\frac{a}{\log a} \log b \leq b$ and $a \leq \frac{b}{\log b} \log a$.

Thus $\log q_i \leq q_i \frac{\log P}{P}$ and $p_i \leq \frac{P}{\log P} \log p_i$. Hence we have

$$\sum_{i=t}^{s} \log q_i \leq 2\frac{\log P}{P} + \sum_{i=1}^{r} \log p_i.$$

We then add $\sum_{i=1}^{t} \log q_i$ to both sides to get the conclusion. □

Lemma 2.8. *Let q be prime. If $e > 1$ and $q^e | G(n)$, then $q^e \leq 2P$ and $q \leq \sqrt{2P}$.*

Proof. Denote by Q the smallest prime not dividing $G(n)$. We actually show that $q^e \leq 2Q$. Suppose $q^e > 2Q$, and let N be the smallest integer such that $Q^N > q$. Since by definition $Q^{N-1} < q$, we have $q < Q^N < qQ$. Now let $m = \frac{Q^N}{q} G(n)$. Thus $m > G(n)$. Because q does not divide Q, m has the same prime factorization of $G(n)$ except that it includes a factor of Q^N and the exponent of q is $(e-1)$ instead of e. Thus we have the following equation for $S(m)$:

$$S(m) = S(G(n)) + (Q^N - q^e + q^{e-1}).$$

Note that it is sufficient to prove that $(Q^N - q^e + q^{e-1}) < 0$, since this would imply $S(m) \leq S(G(n)) \leq n$, while simultaneously $m > G(n)$. This would contradict 2.5. If $q < Q$, then $N = 1$ and $-q^e + q^{e-1} \leq -q^e/2 < -(2Q)/2 < -Q$, a contradiction. On the other hand, if $q > Q$, since $e > 1$, then

$$Q^N - q^e + q^{e-1} < qQ - q(q-1) \leq qQ - qQ = 0,$$

also a contradiction. Q cannot equal q, of course, since q divides $G(n)$ and Q does not. □

Remark 2.9. The lemma is interesting in that it shows the prime factors of $G(n)$ are bunched up; once one is skipped, the number of primes larger than Q dividing $G(n)$ is bounded by $\pi(2Q) - \pi(Q)$.

Theorem 2.10. $\log F(n) \sim \log G(n)$.

Proof. Split up the factorization of $G(n)$ into primes with exponent 1 and primes which appear with exponent greater than 1. The latter set contains at most $\sqrt{2P}$ primes, for otherwise we would have at least one prime factor greater than $\sqrt{2P}$ raised to a power of two or greater, contradicting Lemma 2.8. Thus

$$\log F(n) \leq \log G(n) \leq 2 + \log F(n) + \log P + \sqrt{2P} \log 2P.$$

It thus suffices to prove that $\log F(n) > cP$ for some constant c. For this it is sufficient to show that $A(x) = \sum_{p \leq x} \log p \sim x$. Abel's summation formula says that if $a(x)$ is the indicator function of the primes,

$$A(x) = \sum_{j=1}^{x} a(j) \log j = \pi(x)\log(x) - \pi(1)\log(1) - \int_2^x \frac{\pi(x)}{x}.$$

By the prime number theorem, then, we have that

$$\frac{A(x)}{x} = 1 + \frac{1}{x}\left[\int_2^{\sqrt{x}} \frac{\pi(x)}{x} + \int_{\sqrt{x}}^{x} \frac{\pi(x)}{x}\right] \sim 1 + \frac{1}{x}\left[\int_2^{\sqrt{x}} \frac{1}{\log x} + \int_{\sqrt{x}}^{x} \frac{1}{\log x}\right].$$

The theorem is proved with simple bounds on the last term above. □

Theorem 2.11. $\displaystyle\sum_{p < \sqrt{n \log n}} p \sim n.$

Proof. We will need a statement equivalent to the proof of the Prime Number Theorem (whose equivalence we will not prove but can be found in [6]). In particular, if we define

$$A\left(x\right) = \sum p \leq xp,$$

then we have

$$A(x) \sim \frac{x^2}{2\log x}.$$

The proof is immediate when one substitutes $\sqrt{n \log n}$ for x. □

Corollary 2.12. $G(n) \sim e^{\sqrt{n \log n}}$.

Proof. By Theorem 2.11, we have that $\log F(n) \sim \sqrt{n \log n}$. Hence $F(n) \sim e^{\sqrt{n \log n}}$. By Theorem 2.10, $G(n) \sim e^{\sqrt{n \log n}}$. □

3. Dixon's Theorem

We will now prove Dixon's theorem, which settled affirmatively a 70-year-old conjecture that as n tends to infinity, the probability that randomly selected pairs of elements of S_n generate either A_n or S_n tends to 1. The theorem employs some algebraic machinery, combinatorial analysis, and some of the results of Erdős and Turán. We begin with some standard definitions about group actions that will help classify the subgroups of S_n that candidate pairs will generate.

Definition 3.1. The *orbit* of an element $a \in A$ under the action of a group G is the set $\{a^g : g \in G\}$.

Definition 3.2. A subset of $S \subseteq \{1, 2, \dots, n\}$ is called a *block* if for any element $g \in G$, $S^g \cap S = \emptyset$.

Definition 3.3. A subgroup $G \leq S_n$ is called *transitive* if it has one orbit.

Definition 3.4. A subgroup $G \leq S_n$ is called *primitive* if it is transitive and has no non-trivial blocks, where singletons and the whole set are considered trivial.

Definition 3.5. t_n and p_n are defined as the proportion of the $(n!)^2$ pairs of elements in S_n that generate a transitive group and primitive group, respectively.

The idea of the proof is to show that p_n is nearly 1, while at the same time using primitivity as part of a sufficient condition for generating A_n and S_n.

Lemma 3.6. *We have the recursive formula* $n = \sum_{i=1}^{n} \binom{n}{i}^{-1} it_i$

Proof. Choose any partition of $\{1, 2, \dots, n\}$, say, $A_1, A_2, \dots, A_k$. Then the number of pairs of elements (x, y) that have exactly A_1, A_2, $\dots$, A_k as fixed blocks in the subgroup $\langle x, y\rangle$ is

$$\prod_{i=1}^{n} (k_i!)^2 t_{k_i}$$

where $k_i = |A_i|$. We next observe that the number of partitions of $\{1,\ 2,\ \dots\ ,\ n\}$ that have j_i parts of size i is

$$v_{j_1,j_2,\dots,j_n} = \prod_{i=1}^{n} \frac{n!}{(i!)^{j_i} j_i!}.$$

This, of course, comes from the multinomial coefficient with k_i indices of i, further divided by $\prod_{i=1}^{n} j_i!$ because subsets of the same size are not distinguished. Thus by summing over all n-tuples $(j_1, j_2, \ldots, j_n)$ such that $\sum_{i=1}^{n} i j_i = n$, we arrive at the identity:

$$(n!)^2 = \sum v_{j_1,j_2,\ldots,j_n} \prod_{i=1}^{n} ((i!)^2 t_i)^{j_i}$$

Substituting for $v_{j_1,j_2,\ldots,j_n}$ we get

$$n! = \sum \prod_{i=1}^{n} \frac{(i!t_i)^{j_i}}{j_i!}.$$

Next, we multiply each side by X^n and formally sum over all nonnegative integers n, giving the following formal identities:

$$\sum_{n=0}^{\infty} n! X^n = \sum_{n=0}^{\infty} \left[\sum \prod_{i=1}^{n} \frac{(i!t_i)^{k_i}}{k_i!} \right] X^n = \prod_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{(i!t_i X^i)^j}{j!} = \exp\left(\sum_{i=0}^{\infty} i! t_i X^i \right).$$

The second equality can be justified as follows: the series on the right will contribute 1 to the coefficient of X^n if and only if it is the product of coefficients whose power terms where the ns are the k_is. We recall that $(e^{f(x)})' = f'(x) e^{f(x)}$, and hence we have:

$$\sum_{n=0}^{\infty} n! n X^{n-1} = \sum_{i=1}^{\infty} i! i t_i X^{i-1} \sum_{k=0}^{\infty} k! X^k.$$

Thus by taking the formal product of the two series on the right and equating the $(n-1)$st coefficients, we get

$$n = \sum_{i=1}^{n} \binom{n}{i}^{-1} i t_i$$

as desired. □

Lemma 3.7. *We have the relation* $t_n = 1 - \frac{1}{n} + O(n^{-2})$

Proof. Define $r_n = n(1 - t_n)$ and $c_n = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} i$. Then

$$r_n = n(1-t_n) = \sum_{i=1}^{n} \binom{n}{i}^{-1} i - \sum_{i=1}^{n} \binom{n}{i}^{-1} i(1-t_i) = c_n - \sum_{i=1}^{n} \binom{n}{i}^{-1} r_i$$

Since $\binom{n}{i} = \binom{n}{n-i}$, we may write $c_n = \sum_{i=1}^{n-1} \binom{n}{i}^{-1} i = n \sum_{i=1}^{n-1} \binom{n}{i}^{-1}$. Since also $\binom{n}{3} \leq \binom{n}{c}$, $c \leq n-3$ and $\binom{n}{3} = O(n^3)$, we have the following upper bound:

$$c_n \leq n \sum_{i=1}^{n-1} \binom{n}{3}^{-1} = O(n^{-1})$$

Since $r_i \geq 0$, $r_n \leq c_n$ by definition. Hence

$$t_n = 1 - \frac{r_n}{n} \geq 1 - \frac{c_n}{n}$$

which goes to 1 as n goes to infinity. □

Definition 3.8. An *imprimitive* group is a transitive group which is not primitive. The proportion of pairs of elements in S_n which generate an imprimitive group is denoted by i_n.

Proposition 3.9. *There are at most $(m!)^2 t_m (d!)^{2m}$ pairs $(x, y) \in S_n \times S_n$ that generate an imprimitive group with m blocks.*

Proof. As in the first part of the proof, there are exactly $(m!)^2 t_m$ pairs of elements which generate a group that has m blocks of equal size of d. Each element x and y acts transitively on these blocks, so the action of x or y on a single block determines the action of x or y on the whole set. This gives at most $(d!)^{2m}$ possible choices (with each factor $d!$ coming from the internal variation within each block). □

Lemma 3.10. *The proportion of pairs of (x, y) that generate an imprimitive group in S_n is at most $n2^{-\frac{n}{4}}$.*

Proof. There are $\frac{n!}{(d!)^m m!}$ ways to partition $\{1, 2, \ldots, n\}$ into m blocks of size d. Each imprimitive group has some block structure, even if it is not unique, so summing over each pair m, d such that $md = n$, we have at most $\frac{n!(m!)^2 t_m (d!)^{2m}}{(d!)^m m!}$ pairs of generators, and hence we have:

$$i_n \leq \sum_{md=n} \frac{(m!)^2 t_m (d!)^{2m}}{n!(d!)^m m!} \leq \sum_{md=n} \frac{m!(d!)^m}{n!}$$

We need the identity

$$\prod_{i=1}^{m} i \binom{id}{d}^{-1} = \prod_{i=1}^{m} \frac{(id-d)!d!i}{(id)!} = \frac{m!(d!)^m}{n!}.$$

We also note that

$$\frac{(id-d)!d!i}{(id)!} = \prod_{j=1}^{d-1} \frac{d-j}{id-j}.$$

Since each $\frac{d-j}{id-j} \leq \frac{1}{i}$, this product is bounded above by

$$\leq \prod_{i=1}^{m} i^{-(d-1)} = (m!)^{-(d-1)}.$$

Since we require $m \geq 2$ and $d \geq 2$, we have $m! \geq 2^{\frac{m}{2}}$ and $-(d-1) \leq \frac{d}{2}$. Hence $\frac{m!(d!)^m}{n!} \leq (2^{\frac{m}{2}})^{-\frac{d}{2}} = 2^{-\frac{n}{4}}$. So we arrive at:

$$i_n \leq \sum_{md=n} 2^{-\frac{n}{4}} \leq n2^{-\frac{n}{4}} = O(n^{-2}).$$

□

We have shown that almost all pairs of elements generate a primitive group. This is very useful when combined with Jordan's Theorem, which gives a sufficient condition for a subgroup to generate A_n or S_n.

Theorem 3.11. *(Jordan, 1893). A primitive subgroup of S_n is equal to either A_n or S_n whenever it contains at least one permutation which is a q-cycle for some prime $q \leq n - 3$.*

Proof. Throughout the proof we will make use of a few lemmas whose proofs are elementary and can be found in [7]. To begin, we must give a multidimensional analogue to transitivity:

Definition 3.12. A subgroup $G \leq S_n$ is called k-fold transitive if for every pair of ordered k-tuples S and B, there exists $g \in G$ such that $S^g = B$.

Suppose that some element $g \in G$ is a q-cycle; without loss of generality g $= (123 \ldots q)$. Throughout the proof we use the following notation: $\Omega = \{1, 2, \ldots, n\}$, $\Gamma = \{1, 2, \ldots, q\}$, and $\Delta = \{q+1, \ldots, n\}$, where of course $|\Delta| \geq 3$ by hypothesis. For any set A, we also denote the pointwise stabiliser of A by G_A. Observe that $\langle g \rangle$, having order q, is a Sylow subgroup of G_Δ, which has order dividing $q!$. It is not hard to see that G_Δ is primitive on Γ. Thus we can apply the following lemma from [7]:

Lemma 3.13. *If G is primitive on $\{1, 2, \ldots, n\}$ and G_Δ is primitive on Γ, where $1 < |\Gamma| = m < n$, then G is $(n - m + 1)$-fold transitive and primitive on Ω.*

We next use the following lemma, which can also be found in [7]:

Lemma 3.14. *Let G be k-fold transitive on Ω, and a subgroup $U \leq G_\Gamma$ be a subgroup such that for any V such that U is conjugate to V in G, U is conjugate to V in G_Γ. Then the normalizer $N = N(U)$ is k-fold transitive on the set of points left fixed by U.*

Since $\langle g \rangle$ is a Sylow subgroup, it satisfies the hypotheses of the lemma and hence the normalizer N of $\langle g \rangle$ is k-fold transitive on G_Δ. If G^S denotes the action of G on the subset S, then this amounts to $N^\Delta = S^\Delta$, since k-fold transitivity on a set of cardinality k generates the entire S^Δ. The following stronger fact is also true:

Lemma 3.15. *If $\alpha \in \Gamma$, $N_\alpha^\Delta = S^\Delta$.*

Proof. By the work above, $N^\Delta = S^\Delta$, so for any k-tuple $\tau \in S^\Delta$, there exists $\sigma \in N^\Delta$ such that $\sigma = \tau$ on Δ. But if we take the composition $g^c\sigma$ for some appropriate exponent c, then $g^c\sigma(\alpha) = \alpha$, where still $g^c\sigma = \tau$ on Δ, since g^c leaves these points fixed. □

The next fact about N_α^Γ will give us a complete characterization of the commutator subgroup of N_α:

Lemma 3.16. *N_α^Γ is abelian.*

Proof.

$$N_\alpha^\Gamma = \{\sigma \in S_n : \sigma(\alpha) = \alpha, \sigma|_\Delta = id, \sigma \langle g \rangle \sigma^{-1} = \langle g \rangle\}$$

In particular, the first and third condition give exactly one $\sigma \in S_n$ for each $g \in \langle g \rangle$ such that $\sigma \langle g \rangle \sigma^{-1} = \langle g \rangle$. This is because for each $g^c \in \langle g \rangle$, we require $(\sigma(1)\sigma(c)\sigma(2c+1) \ldots \alpha\sigma(\alpha + c) \ldots) \in \sigma \langle g \rangle \sigma^{-1}$. Since the elements in the cycle must be equally spaced, together these uniquely determine some element in S_n. N_α^Γ is isomorphic to some subgroup of the automorphisms of $\langle g \rangle$; in other words,

$$N_\alpha^\Gamma \cong T \leq \mathrm{Aut}(\langle g \rangle).$$

Since $\mathrm{Aut}(\langle g \rangle)$ is abelian, the result follows. □

We just need one more well-known fact [3], namely that

Lemma 3.17. *Any primitive group G containing a 3-cycle is the alternating group or the symmetric group.*

Proof. Denote by Λ the largest subset of Ω such that $\mathrm{Alt}(\Lambda) \leq G$, where $\mathrm{Alt}(\Lambda)$ denotes the subgroup of A_Ω which leaves points outside of Λ fixed. Such a set is non-empty since G contains a 3-cycle. For the sake of contradiction, assume $\Lambda \neq \Omega$. Λ is not a block, so for some $g \in G$, $\Lambda \cap \Lambda^g \neq \emptyset$ or Λ. Suppose this intersection consists of at most one point for each g. Call this point a and let the original 3-cycle be (abc). We note that since $g\operatorname{Alt}(\Lambda)g^{-1} = \operatorname{Alt}(\Lambda^g) \leq G$, some other 3-cycle (ade) is in G as well. It's easily checked that

$$(abc)\,(ade)\,(abc)^{-1}\,(ade)^{-1} = (abd)\,.$$

Now suppose that the intersection $\Lambda \cap \Lambda^g$ consists of two points or more points, including a and b, for some $g \in G$, choose $d \in \Lambda^g - \Lambda$. We know there is such a point since G is primitive. Since $\operatorname{Alt}(\Lambda^g) \leq G$, G contains the 3-cycle (abd). Now suppose $\operatorname{Alt}(\Phi) = \Lambda \cup \{d\}$. We wish to show $\operatorname{Alt}(\Phi) \leq G$, which will give the desired contradiction. To do this, note that we only need to show that for all elements $\sigma \in \operatorname{Alt}(\Phi)$ such that $\sigma(d) \neq d$, we have $\sigma \in G$. Of course, if without loss of generality $a = \sigma(d) \neq d$ but $\sigma \in \operatorname{Alt}(\Phi)$, then $\sigma(d) \in \Lambda$. But then we have some $\tau \in \operatorname{Alt}(\Delta)$ such that $\tau(\sigma(d)) = b$, so $\pi = \tau\sigma \in \operatorname{Alt}(\Delta)$. However, then we have both $(abd)\,\pi\sigma$ and $(abd)\,\pi$ in G since the former fixes d. Then clearly $\sigma \in G$. □

Note that the commutator of a direct product follows a rather nice rule:

$$[N_\alpha, N_\alpha] = \left[N_\alpha^\Delta, N_\alpha^\Delta\right] \times \left[N_\alpha^\Gamma, N_\alpha^\Gamma\right] = \left[S^\Delta, S^\Delta\right] = A^\Delta$$

Thus G contains a 3-cycle, since a subgroup of a subgroup of G contains a 3-cycle, and we apply Lemma 3.17. This completes the proof of Jordan's theorem. □

Definition 3.18. For a prime q satisfying $(\log n)^2 \leq q \leq n-3$, define $T_n = \bigcup_q \{\sigma \in S_n | \sigma$ contains a q-cycle and its other cycle lengths are relatively prime to $q\}$.

Corollary 3.19. *Suppose there is some $z \in T_n$ with order h, where h is divisible by q. Since* $\operatorname{ord}(z^{\frac{h}{q}}) = \frac{h}{\gcd(\frac{h}{q},h)} = q$*, then any primitive group G containing z generates A_n or S_n by Jordan's theorem.*

We shall prove that the proportion of T_n in S_n is at least $1 - \frac{4}{3\log\log n}$ to prove Dixon's theorem. Three more lemmas will finish the proof. The first is an asymptotic estimate for $\sum_p \frac{1}{p}$ that I wrote. Two come from Erdős' and Turán's seminal paper from 1967 [5].

Lemma 3.20. *For prime $p \leq n$, $\sum_p \frac{1}{p} \sim \log\log n$.*

Proof. We write $\sum_p \frac{1}{p} = \sum_{1\leq x\leq n} a(x)\frac{1}{x}$, where $a(n)$ is the indicator function of the primes. Now, $\sum_{i=0}^n a(i) = \pi(n)$, so by Abel's summation formula,

$$\sum_p \frac{1}{p} = \pi(x)\frac{1}{x} + \int_2^x \frac{\pi(x)}{x^2}.$$

The estimate $\pi(x) \sim \frac{x}{\log x}$ of the Prime Number Theorem proves the lemma.

□

Lemma 3.21. *Let $1 \leq a_1 \leq a_2 \leq \cdots \leq a_n \leq n$. Then the proportion d_n of elements in S_n without any cycles of length $a_1, a_2, \ldots, a_n$ is at most $(\sum_{i=1}^n \frac{1}{a_i})^{-1}$.*

Lemma 3.22. *The proportion of elements in S_{n-q} with order relatively prime to q is bounded below by $e^{-\frac{1}{\log n}}$ for sufficiently large n.*

Proof. It is clear that if we take the product over all positive integers such that p does not divide v and for any $|z| < 1$,

$$\prod_v \sum_{n=0}^{\infty} \left(\frac{z^v}{v}\right)^n \frac{1}{n!} = \prod_v \exp\left(\frac{z^v}{v}\right)$$

the *nth* coefficient gives the number of ways to sum to n using no multiple of p. But in taking this product, we are merely excluding multiples of p, so

$$\prod_v \exp(\frac{z^v}{v}) = \exp(\sum_{v=0}^{\infty} \frac{z^v}{v} - \sum_{v=0}^{\infty} \frac{z^{pv}}{pv}).$$

But using the facts that $-\log(1-z) = \sum_{v=0}^{\infty} \frac{z^v}{v}$ and $-\frac{\log(1-z^p)}{p} = \sum_{v=0}^{\infty} \frac{z^{pv}}{pv}$, we simplify this to

$$\frac{(1-z^p)^{\frac{1}{p}}}{1-z} = (\frac{\sum_{i=0}^{p-1} z^i}{(1-z)^{p-1}})^{\frac{1}{p}} = (\sum_{i=0}^{p-1} z^i)(1-z^p)^{-\frac{p-1}{p}}.$$

Using the representation $(1-z^p)^{-\frac{p-1}{p}} = 1 + \sum_{m=1}^{\infty} z^{mp} \prod_{k=1}^{m}(1-\frac{1}{kp})$, we actually get the exact formula,

$$d_n = \prod_{i=1}^{m} \frac{qi-1}{qi}$$

where $m = \left\lfloor \frac{n-q}{q} \right\rfloor$. It is not difficult to show that, since $q \geq (\log n)^2$,

$$\prod_{i=1}^{m} \frac{qi-1}{qi} \sim \exp(-\frac{\log n - \log q}{q}) \geq \exp(-\frac{\log n}{q}) \geq \exp(-\frac{1}{\log n})$$

□

We now have all the tools to prove Dixon's celebrated result.

Theorem 3.23. *(Dixon, 1969.) The proportion of pairs of elements in S_n which generate either A_n or S_n is at least $1 - \frac{2}{(\log\log n)^2}$.*

Proof. Let u_n be the proportion of elements in S_n which lie in T_n. Combining the previous two lemmas, we see that for q prime, $(\log n)^2 \leq q \leq n-3$, and n sufficiently large,

$$u_n \geq (1 - (\sum_q \frac{1}{q})^{-1})e^{-\frac{1}{\log n}}$$

By the estimate on the sum of prime reciprocals, for sufficiently large n

$$\sum_q \frac{1}{q} \sim \log\log(n-3) - \log\log(\log n)^2 > \frac{4}{5}\log\log n.$$

In the previous part of the proof, we showed that the proportion of elements which generate a primitive group, $p_n \geq 1 - \frac{2}{n}$ for large enough n. Thus the proportion of pairs of elements which generate A_n or S_n is at least

$$p_n - (1-u_n)^2 \geq (1-\frac{2}{n}) - \frac{16}{9(\log\log n)^2} \geq 1 - \frac{2}{(\log\log n)^2}.$$

□

Remark 3.24. Since publishing his paper in 1969, Dixon has sharpened his result with respect to the rate at which the probability approaches one. In fact, he finds an asymptotic formula [4]:

$$1 - \frac{1}{n} - \frac{1}{n^2} - \frac{4}{n^3} - \frac{23}{n^4} - \dots$$

This result is an improvement on Babai's 1989 theorem [1] which also gave a linear error term. Both of these papers use the classification of finite simple groups.

References

[1] Babai, László. The probability of generating a symmetric group. *Journal of Combinatorial Theory.* 1989.

[2] Dixon, John. The probability of generating the symmetric group. *Math. Z.* 1969.

[3] Dixon, John. *Permutation Groups.* Springer. 1996.

[4] Dixon, John. Asymptotics of generating the symmetric and alternating groups. http://www.math.carleton.ca/∼jdixon/Generating-An.pdf. 2005.

[5] Erdős, Paul. On some problems of a statistical group-theory II. *Acta Mathematica.* 1967.

[6] Miller, William. The maximum order of an element of a finite symmetric group. *The American Mathematical Monthly.* 1987.

[7] Wielandt, Helmut. *Finite Permutation Groups.* Academic Press. 1964.