COMBINATORICA
Bolyai Society – Springer-Verlag

Combinatorica **32** (3) (2012) 309–323
DOI: 10.1007/s00493-012-2502-9

APPLICATIONS OF CHARACTER ESTIMATES TO STATISTICAL PROBLEMS FOR THE SYMMETRIC GROUP

JAN-CHRISTOPH SCHLAGE-PUCHTA

Received April 22, 2008
Revised August 12, 2011

Let $\pi, \sigma \in S_n$ be chosen at random. Using character estimates we show that in various aspects the elements $\pi\sigma^i$ behave like independent random variables. As application we show that almost surely the Cayley graph determined by π and σ has diameter $\mathcal{O}(n^3 \log n)$, and the directed Cayley-graph has almost surely diameter $\mathcal{O}(n^4 \log n)$. Further we describe an algorithm for the black-box-recognition of the symmetric group, and show that for each element τ moving a positive proportion of all points, the number of cycles of a random element σ and of $\tau\sigma$ are nearly independent.

Let π, σ be random elements in the symmetric group S_n. Netto's conjecture, which was proven by Dixon [8], states that with probability tending to 1 as n goes to infinity, the subgroup generated by π and σ is either A_n or S_n. Hence, almost always two random elements which are not both contained in A_n define a Cayley graph of S_n. Babai and Seress [1] showed that the diameter of this graph is always bounded above by $\exp((1+o(1))\sqrt{n \log n})$, moreover, Babai and Hetyei [3] showed that for almost all pairs π, σ the diameter is bounded by $\exp((1/2+o(1)) \log^2 n)$. They conjectured that in both cases the true order of magnitude is n^c. Later, Babai and Hayes [4] proved this conjecture by showing that the diameter of the Cayley graph is almost always $\mathcal{O}(n^{7+\epsilon})$. Moreover, Babai [5] showed that a polynomial bound for the diameter of the Cayley graph implies a polynomial bound for the directed Cayley graph, that is, the directed graph with edges passing from x to πx and σx. More precisely, he showed that if π, σ are permutations chosen at random, then almost surely every permutation can be written as a

Mathematics Subject Classification (2000): 05C25, 20B30, 60C05, 68W20

word of length $\mathcal{O}(n^{17+\epsilon})$. All these proofs are combinatorial in nature, here we give a proof based on character theory. We shall show the following.

Theorem 1. *Let π, σ be random elements in S_n, not both in A_n. Then with probability tending to 1, π and σ generate S_n, and the Cayley graph with respect to this system of generators has diameter $\leq n^3 \log n$. The directed Cayley graph has almost surely diameter $\leq 3n^4 \log n$.*

Note that the proof yields an algorithm to represent an element of S_n as a word in σ and τ, which in the directed case answers a question posed by Babai [5].

The proof will use character theory to show that with high probability there exists an element which can be written as a short word in π and σ and consists of a short cycle. To do so, we use a conjugacy class which has small character values, and allows one to reach a single small cycle easily. There is some freedom in the choice of this element, we will work with the class $\mathbf{c}$ of elements consisting of an $(n-2)$-cycle and a 2-cycle, if n is odd, and an $(n-3)$-cycle, a 2-cycle and a fixed point, if n is even. The main step in the proof of Theorem 1 is the following.

Proposition 1. *Let $\pi \in A_n$ and $\sigma \in S_n \setminus A_n$ be chosen at random, and let N be an integer satisfying $n < N < n^{1+1/64}$. Then the probability that there is some i in the range $1 \leq i \leq N$, such that $\pi\sigma^i \in \mathbf{c}$ is bounded below by $1 - c\frac{n}{N}$ for some absolute constant c. The same holds true if $\mathbf{c}$ is the conjugacy class consisting of n-cycles or of $n-1$-cycles.*

This result can be used to improve probabilistic algorithms. Instead of choosing n random permutations one can choose 2 random permutations σ, τ, and then use $\sigma, \sigma\tau, \sigma\tau^2 \ldots, \sigma\tau^n$ as pseudo-random elements. This may be an improvement, since in certain circumstances choosing random elements in a group is a difficult task in itself. As an example, we show the following.

Theorem 2. *Let G be a black box group isomorphic to A_n or S_n. Then for every $k < n^{1/64}$ there exists a Las Vegas algorithm giving an effective isomorphism with probability $1 - \mathcal{O}(k^{-1})$ which takes 2 random elements, and $kn \log n$ multiplications in G.*

Another application of our method concerns near-independence of permutations as defined in [4]. As an example, we show the following.

Theorem 3. *Let $\alpha > 0$ be given, and let $\tau \in S_n$ be a permutation moving at least αn points. Let $\sigma \in S_n$ be chosen at random. Then the number of*

cycles of σ and $\tau\sigma$ are nearly independent, more precisely, denoting by $c(\pi)$ the number of cycles of a permutation π, we have

$$\lim_{n\to\infty} \max_{\substack{\tau\in S_n \\ |\operatorname{supp}(\tau)|>\alpha n}} \max_{x,y} \left|P(c(\sigma)<x, c(\tau\sigma)<y) - P(c(\sigma)<x)P(c(\tau\sigma)<y)\right| = 0.$$

We remark that the cycle type of σ and $\tau\sigma$ are not independent, in fact, it is easy to see that the conditional expected number of fixed points of $\tau\sigma$ subject to the condition that σ has k fixed points is $k(1-\alpha)+\alpha$; and a similar result holds true for the number of ℓ-cycles for each fixed ℓ, however, we will see in the proof that longer cycles are independent in a very strong sense.

1. Proof of Theorem 1 and 2

In this section we deduce Theorem 1 and 2 from Proposition 1. The proof of the first part of Theorem 1 runs parallel to the proof given in [1]. Note first that the restriction $\pi\in A_n$ is of no relevance, for if both π and σ are contained in $S_n\setminus A_n$, we replace π by $\pi\sigma$. For an element $\tau\in S_n$, define $c(\tau)$, the cost of τ with respect to π and σ as the length of the shortest word in $\pi,\pi^{-1},\sigma,\sigma^{-1}$ representing τ, and $c^+(\tau)$, the positive cost, as the length of the shortest word representing τ using only π and σ. Applying the proposition with $N=\frac{1}{2}n\log n$ we find that almost surely there exists an element π consisting of one 2-cycle, one cycle of odd length, and possibly one fixed point. Taking this element to the power of $n-2$ or $n-3$, we obtain a transposition τ of positive cost $\le n^2\log n$. From this transposition we may pass to all transpositions in view of the following result, which is a slight improvement of a result proven by Babai and Seress [1].

Lemma 1. *Let $\pi_1,\dots,\pi_k$ be permutations generating a 2-transitive subgroup of S_n. Then there exists a set $R\subseteq S_n$, which acts 2-transitive, and consists of elements of cost n^2 with respect to the generating set $\{\pi_1,\dots,\pi_k\}$ at most.*

Proof. Define R_i to be the set of permutations of cost at most i, and define the set Ω_i and Ω as

$$\Omega_i := \{(1,2)^\pi : \pi\in R_i\} \subseteq \{(x,y): 1\le x,y\le n, x\ne y\} =: \Omega.$$

We have to show that $\Omega_{n^2}=\Omega$. Since $|\Omega|\le n^2$, it suffices to show that for each i either $\Omega_i=\Omega$, or $|\Omega_i|<|\Omega_{i+1}|$. Let i be an index such that $\Omega_i=\Omega_{i+1}$. Then we have

$$\Omega_{i+2} = \bigcup_{\nu=1}^{k} \{(i,j)^{\pi_\nu} : (i,j)\in\Omega_{i+1}\} = \bigcup_{\nu=1}^{k} \{(i,j)^{\pi_\nu} : (i,j)\in\Omega_i\} = \Omega_{i+1},$$

thus, the chain $\Omega_1 \subseteq \Omega_2 \subseteq \dots$ stabilizes at i. However, since $\langle \pi_1, \dots, \pi_k \rangle$ is 2-transitive, we have $\Omega_i = \Omega$ for i sufficiently large. Hence, our claim follows. ∎

Since two random permutations generate A_n or S_n with probability tending to 1, we may restrict ourselves to the case that π and σ generate a 2-transitive subgroup. In this case all transpositions can be reached by conjugating the one already obtained by elements of cost $\leq n^2$, and therefore have cost $\leq \frac{1}{2} n^2 \log n + n^2 \leq n^2 \log n$. Every permutation can be written as the product of $\leq n$ transpositions, and our claim follows.

For the second part of Theorem 1 we apply Proposition 1 to find an n-cycle α and an $n-1$-cycle β of positive cost $n \log n$ each. Since $\alpha^{-k} = \alpha^{n-k}$ and $\beta^{-k} = \beta^{n-k-1}$, conjugating by some power of α or β increases the positive cost of an element by $n^2 \log n$ at most. In particular, conjugating β by some power of α, we obtain the 2-transitive set

$$R = \{\alpha, \alpha^2, \dots, \alpha^{n-1}, \beta, \beta^\alpha, \dots, \beta^2, (\beta^2)^\alpha, \dots\},$$

such that each element in R has positive cost $\leq 2n^2 \log n$ and order at most n. Thus, conjugating by an element in R increases the positive cost by $2n^3 \log n$ at most, and we find that all transpositions have positive cost at most $3n^3 \log n$. Hence, the second part of Theorem 1 follows.

For Theorem 2 we follow an idea of Bratus and Pak [6]. To simplify notation, assume that n is odd and that G is isomorphic to S_n; the other cases are similar. Choose random elements $g, h \in G$, compute $x_i = gh^i$, and test whether these elements have order n or $2(n-2)$. Suppose that we found elements x, y of the desired order. If these elements are an n-cycle and an $n-2$-cycle together with a transposition, we may assume without loss that $x = (123 \dots n)$, and $t' = y^{n-2} = (1i)$. Now $[x, t'^k]$ has order 2, unless $k = i, n-i$. Replacing t' by either of t'^i or t'^{n-i} yields $x = (123 \dots n)$ and $t = (12)$, and we found an isomorphism. Thus, if x, y are of the right cycle type, we are done. The next results shows that the annoying case, where one of x, y has the correct order, but is not of the desired cycle type, is rare.

Lemma 2. *In S_n there are $\mathcal{O}(n^{-3} \cdot n!)$ elements of order n which are not n-cycles, or elements of order $2(n-2)$ which do not consist of an $n-2$-cycle and a transposition.*

Proof. We only prove the statement for elements of order n. An element of order n has cycle lengths dividing n. We split the set of elements of order n, which are not n-cycles, into 3 classes: Those with at least 3 cycles of length $> n/120$, those with at most 2 cycles of length $> n/120$, but at least 12 cycles of length $> \sqrt{n}$, and the rest. The number of permutations having n_i cycles

of length k_i is $n!\prod \frac{1}{n_i^{k_i}k_i!}$. Hence, the number of elements having 3 given cycle lengths $>n/120$ is at most $120^3 n^{-3} n!$, since the number of divisors of n which are less than 120 is bounded, the number of elements of the first class is of the right order. For elements in the second class we consider the 12 largest cycle lengths. For each fixed choice, the number of permutations realizing this choice is at most $n^{-6}n!$, and since n has $\mathcal{O}(n^{1/4})$ divisors, choosing 12 of them gives a factor $<n^3$, hence, the number of permutations in the second class is also of the right order. Finally, if a permutation of order n has at most 2 cycles of length $> n/120$, these cycles cannot be both of length $n/2$, since then the order would be $n/2$. Hence, the number of points in cycles of length $>n/100$ is at most $n/2+n/3=5n/6$. Thus, a permutation in the third class has at least $n/6-12n/120=n/15$ points in cycles of length $<\sqrt{n}$. Since there are at most $\mathcal{O}(n^{1/4})$ different cycle lengths, there exists a cycle length which is populated by $\gg n^{1/4}$ cycles. Hence, the number of permutations in the third class is at most $\frac{n!}{[cn^{1/4}]!}$, which is far smaller than necessary. ∎

It remains to check whether x and y have indeed the correct cycle structure, that is, we need an algorithm, which, given two elements $x,t \in S_n$, where x has order n and t has order 2, decides using $\mathcal{O}(n\log n)$ multiplications whether the pair (x,t) is in fact conjugate to $((12\dots n),(12))$. To do so, we follow an idea of Bratus and Pak [6]. Represent $n-2$ as the sum of distinct odd primes $p_1+\dots+p_k=n-2$. Then we can write the permutation $(12\dots p_1)(p_1+1\dots p_1+p_2)\dots(p_1+\dots+p_{k-1}+1\dots n-2)(n-1n)$ as a word in (12) and $(12\dots n)$ of length $\ll k\log n$, thus, we can form from x and t an element, which has order $2p_1\cdots p_k$, provided that x and t have the right cycle structure. We now check whether the order of this element is correct, and if this is the case, we take the $p_1\cdots p_k$-th power of this element, thus, we obtain an element which is necessarily a transposition, and, if our conjecture on x and t is true, is $(n-1n)$. Now conjugating by x^2 yields an element which is necessarily a transposition and should equal t, thus, we can now decide whether t is in fact a trasposition, and we may assume without loss that $t=(12)$. Let $\ell_1,\dots,\ell_k$ be the cycle lengths of x, where ℓ_1 is the length of the cycle containing 1, and ℓ_2 is the length of the cycle containing 2, unless 1 and 2 are in the same cycle. We now check whether tx has the expected order $n-1$, and claim that this already implies that x is an n-cycle. Suppose that x is not an n-cycle, but that 1 and 2 are in the same cycle of x. Then tx has cycles of length $a,b,\ell_2,\dots,\ell_k$, where $a+b=\ell_1$, and the fact that the order of tx is $n-1$ shows that the least common multiple of $a,b,\ell_2,\dots,\ell_k$ is $n-1$ and therefore coprime to n, hence, $\ell_2=\dots=\ell_k=1$. But then the order

of x is $\ell_1 = n$, and we have shown that x is an n-cycle. If on the other hand 1 and 2 are contained in different cycles of x, then tx has cycles of length $\ell_1 + \ell_2, \ell_3, \dots, \ell_k$, thus, we again find that $\ell_3 = \cdots = \ell_k = 1$, and therefore ℓ_1 and ℓ_2 have sum $n-1$ and least common multiple n. If ℓ_1 and ℓ_2 have a common factor, this factor would divide both n and $n-1$, which is impossible, thus, we have $\ell_1 + \ell_2 = n-1$, and $\ell_1 \ell_2 = n$, which is impossible for $n \geq 7$. Hence, if our test was positive, then x is in fact an n-cycle. Moreover, tx has two cycles of length ℓ_1, ℓ_2, where ℓ_1 and ℓ_2 have least common multiple $n-1$ and sum n, thus, ℓ_1 and ℓ_2 are coprime, and satisfy $\ell_1 + \ell_2 = n$, $\ell_1 \ell_2 = n-1$, which implies that one of ℓ_1, ℓ_2 equals 1. However, this implies that x maps 1 to 2, that is, the pair (x,t) is indeed conjugate to $((12\dots,n),(12))$.

2. Proof of Proposition 1

The remainder of this article is devoted to the proof of proposition 1. We will only give the proof for n even, the computations for n odd are slightly easier.

Fix N in the interval $[n, n^2]$. Then, for $\pi, \sigma \in S_n$, define

$$r(\pi,\sigma) = \#\{1 \leq i \leq N \colon \pi\sigma^i \in \mathbf{c}\}.$$

Note that $\mathbf{c} \subset S_n \setminus A_n$, hence, even values of i never lead to solutions, whereas for a fixed odd integer i and a fixed permutation σ, there are precisely $|\mathbf{c}|$ choices for π, and we obtain

$$\sum_{\substack{\pi \in A_n \\ \sigma \in S_n \setminus A_n}} r(\pi,\sigma) = \left[\frac{N+1}{2}\right] \frac{n!}{2} |\mathbf{c}| = \big(1 + \mathcal{O}(n^{-1})\big) \frac{n!^2 N}{8n}.$$

Note, that as $N/n \to \infty$, the expected value of $r(\pi,\sigma)$ tends to infinity. Hence, to show that $r(\pi,\sigma) > 0$ almost always, it suffices to show that the variance is not too large. We have

$$\begin{aligned}
\sum_{\substack{\pi \in A_n \\ \sigma \in S_n \setminus A_n}} r(\pi,\sigma)^2 &= \#\big\{(\pi,\sigma,i,j) \colon \pi\sigma^i, \pi\sigma^j \in \mathbf{c}\big\} \\
&= \sum_{\substack{\pi \in A_n \\ \sigma \in S_n \setminus A_n}} r(\pi,\sigma) + 2\#\{(\pi,\sigma,i,j) \colon 1 \leq i < j \leq N, \pi\sigma^i, \pi\sigma^j \in \mathbf{c}\} \\
&= 2\#\big\{(\pi,\sigma,i,j) \colon 1 \leq i < j \leq N, \pi\sigma^i, \pi\sigma^j \in \mathbf{c}\big\} + \mathcal{O}\left(\frac{N}{n} n!^2\right).
\end{aligned}$$

We now claim the following, the proof of which is postponed.

Lemma 3. *As $n\to\infty$, the estimate*

$$\#\big\{(\pi,\sigma,i,j)\colon 1\le i<j\le N, \pi\sigma^i,\pi\sigma^j\in\mathbf{c}\big\}=\big(1+\mathcal{O}(n/N)\big)\frac{N^2}{32n^2}n!^2$$

holds true uniformly in the range $n<N<n^2$.

We can now compute the variance of $r(\sigma,\pi)$.

$$\begin{aligned}\sum_{\pi\in A_n}\sum_{\sigma\in S_n\setminus A_n}\big(r(\sigma,\pi)-N/(2n)\big)^2&=\sum_{\pi\in A_n}\sum_{\sigma\in S_n\setminus A_n}r(\sigma,\pi)^2+\frac{N^2}{16n^2}n!^2\\&\quad-\frac{N}{n}\sum_{\pi\in A_n}\sum_{\sigma\in S_n\setminus A_n}r(\sigma,\pi)\\&\ll\left(\frac{n}{N}+\frac{1}{n}\right)\frac{N^2}{n^2}n!^2.\end{aligned}$$

Hence, for $n<N<n^2$ we obtain

$$\#\big\{(\pi,\sigma)\colon\pi\in A_n,\sigma\in S_n\setminus A_n, r(\sigma,\pi)=0\big\}\ll\frac{\left(\frac{n}{N}+\frac{1}{n}\right)\frac{N^2}{n^2}n!^2}{N^2/n^2}\le\frac{n}{N}n!^2,$$

which implies our claim.

It remains to prove Lemma 3. To do so note that $\pi\sigma^i\in\mathbf{c}\subseteq S_n\setminus A_n$ implies that i is odd. Hence we have

$$\begin{aligned}&\#\big\{(\pi,\sigma,i,j)\colon 1\le i<j\le N,\pi\sigma^i,\pi\sigma^j\in\mathbf{c}\big\}\\&=\sum_{\substack{\nu\le N\\2\mid\nu}}\left\lfloor\frac{N-\nu+1}{2}\right\rfloor\sum_{x,y\in\mathbf{c}}\#\{\sigma\in S_n\setminus A_n\colon\sigma^\nu=xy^{-1}\}\\&=\big(1+\mathcal{O}(N^{-1})\big)\sum_{\substack{\nu\le N\\2\mid\nu}}\frac{N-\nu}{2}\sum_{\tau\in S_n}\#\{\sigma\in S_n\setminus A_n\colon\sigma^\nu=\tau\}\#\{x,y\in\mathbf{c}\colon xy^{-1}=\tau\}.\end{aligned}$$

The inner sum in the last expression is the inner product of the root number function

$$r_\nu^*(\tau)=\#\{\sigma\in S_n\setminus A_n\colon\sigma^\nu=\tau\}$$

and the representation function

$$N_{\mathbf{c}}(\tau)=\#\{x,y\in\mathbf{c}\colon xy^{-1}=\tau\}.$$

Both of these functions can be expressed as sums over irreducible characters. Here, the coefficient of χ in r_ν is given as

$$\langle r_\nu^*, \chi\rangle = \frac{1}{n!}\sum_{\tau\in S_n} r_\nu^*(\tau)\chi(\tau) = \frac{1}{n!}\sum_{\pi\in S_n\setminus A_n}\chi(\sigma^\nu).$$

The coefficient of χ in $N_{\mathbf{c}}$ is equal to $\frac{\chi(\mathbf{c})^2}{n!\chi(1)}$ (confer, e.g. [7, Prop. 9.33], where we write $\chi(\mathbf{c})$ to denote $\chi(\pi)$ for some $\pi\in\mathbf{c}$). Hence, using orthogonality relations, we obtain

$$\begin{aligned}(1)\quad &\#\big\{(\pi,\sigma,i,j)\colon 1\le i<j\le N, \pi\sigma^i,\pi\sigma^j\in\mathbf{c}\big\}\\ &\qquad = \big(1+\mathcal{O}(N^{-1})\big)\frac{|\mathbf{c}|^2}{n!}\sum_{\substack{\nu\le N\\ 2|\nu}}\frac{N-\nu}{2}\sum_{\sigma\in S_n\setminus A_n}\sum_{\chi\in\mathrm{Irr}(S_n)}\frac{\chi(\sigma^\nu)\chi(\mathbf{c})^2}{\chi(1)}.\end{aligned}$$

In this expression we shall compute the contribution of the linear characters explicitly, and show that the remaining characters give terms which can be absorbed into the error term.

First, we compute the contribution of the linear characters. Since ν is even, we have $\chi(\sigma^\nu)\chi(\mathbf{c})^2=\chi(1)=1$ for both the trivial character and the sign character, and the contribution of the linear characters to the two inner sums equals $n!$, and the whole contribution becomes

$$\big(1+\mathcal{O}(N^{-1})\big)|\mathbf{c}|^2\sum_{\substack{\nu\le N\\ 2|\nu}}\frac{N-\nu}{2} = \big(1+\mathcal{O}(n^{-1})\big)\frac{n!^2N^2}{32n^2},$$

which is the expected main term with an error of admissible magnitude.

To bound the contribution of non-linear characters to the right-hand side of (1), we will repeatedly use the following estimate (cf. [10, Theorem 1]).

Lemma 4. *Let χ be an irreducible character of S_n, n be sufficiently large, and σ be an element with k fixed points. Then we have*

$$|\chi(\sigma)|\le\chi(1)^{1-\frac{\log(n/k)}{32\log n}}.$$

We assume that the reader is familiar with the correspondance between irreducible characters of S_n and partitions of n. Due to the special structure of $\mathbf{c}$, the only characters with $\chi(\mathbf{c})\neq 0$ correspond to partitions which have at most 3 cells outside the first row and the first column. [1] By first removing

[1] By explicitly enumerating these permutations we could avoid the use of Lemma 4 and remain completely elementary. However, doing so would dramatically increase the amount of computations needed, and in the last section we need this bound anyway.

a rim hook of length $n-3$, we find that we always have $|\chi(\mathbf{c})| \le 1$, that is, the bound to be established is

$$\sum_{\substack{\nu \le N \\ 2|\nu}} \sum_{\sigma \in S_n \setminus A_n} \sum_{\substack{\chi \in \mathrm{Irr}(S_n) \\ \chi(\mathbf{c}) \neq 0}} \frac{\chi(\sigma^\nu)}{\chi(1)} \ll n \cdot n!. \tag{2}$$

The trivial bound $|\chi(\sigma)| \le \chi(1)$ together with the fact that $\chi(\mathbf{c}) = 0$ for all but $2(n-3)$ characters yields an upper bound $nN \cdot n!$, which is too large for our purpose by a factor of N; we shall save this factor by different methods for different ranges of the summation parameters.

More precisely, we split the summation over ν and σ in (1) into subsums depending on the number of fixed points of σ^ν. Denote by $f(\pi)$ the number of fixed points of π, and set $k = f(\sigma^\nu)$.

Consider first pairs (σ, ν) with $k \le \sqrt{n}$. Using Lemma 4 we find that for ν fixed the sum over all permutations σ is at most

$$n! \sum_{\substack{\chi:\, \chi(1) \neq 1 \\ \chi(\mathbf{c}) \neq 0}} \frac{\chi(\sigma^\nu)}{\chi(1)} \le n! \sum_{\substack{\chi:\, \chi(1) \neq 1 \\ \chi(\mathbf{c}) \neq 0}} \chi(1)^{-1/64} \ll n! \cdot n^{-1/64},$$

where we used the fact that $\chi(\mathbf{c}) = 0$ for all but $2(n-3)$ characters, and that for each A, there are $\mathcal{O}(A)$ characters satisfying both $\chi(1) < n^A$ and $\chi(\mathbf{c}) \neq 0$. We obtain a contribution $N \cdot n^{-1/64} n!$, which is sufficiently small, since by assumption $N < n^{1+1/64}$.

Next, consider the case $\sqrt{n} \le k \le 2n/3$. Then, using Lemma 4, we obtain

$$\sum_{\substack{\chi:\, \chi(1) \neq 1 \\ \chi(\mathbf{c}) \neq 0}} \frac{\chi(\sigma^\nu)}{\chi(1)} \le \sum_{\substack{\chi:\, \chi(1) \neq 1 \\ \chi(\mathbf{c}) \neq 0}} \chi(1)^{-1/(80 \log n)} \ll 1,$$

that is,

$$\sum_{\substack{\sigma \in S_n \setminus A_n \\ f(\sigma^\nu) \ge \sqrt{n}}} \sum_{\chi \in \mathrm{Irr}(S_n)} \frac{\chi(\sigma^\nu)\chi(\mathbf{c})^2}{\chi(1)} \ll \#\{\sigma \in S_n \colon f(\sigma^\nu) \ge \sqrt{n}\}.$$

Hence, to show that elements of this form are negligible, it suffices to show that there are at most $\mathcal{O}(n^{-1/64} n!)$ elements $\sigma \in S_n$ such that σ^ν has more then $\sqrt{n}$ fixed points. To do so, we need the following result on the statistics of cycles of permutation, which is due to Erdős and Turán [9].

Lemma 5. *Let n be an integer.*

1. *Let $k_1,\dots,k_\ell$ be positive integers. Then the number of permutations $\pi\in S_n$ which have cycles of length k_i for each i is $\mathcal{O}(\frac{n!}{k_1k_2\cdots k_\ell})$.*
2. *The number of permutations $\pi\in S_n$ which contain k cycles of the same length is $\mathcal{O}(\frac{n!}{k!})$.*

In particular, when counting permutations σ such that $f(\sigma^\nu)>\sqrt{n}$, we may neglect permutations containing cycles of any given length with multiplicity $\geq\log n$. Let σ be a permutation with $f(\sigma^\nu)>\sqrt{n}$, which does not contain more than $\log n$ cycles of the same length. Since ν has at most $\mathcal{O}(n^\epsilon)$ divisors, we find that there is some divisor $t>n^{1/3}$ of d, such that σ contains a cycle of length t. For each divisor, the number of such permutations is $\mathcal{O}(n^{-1/3}\cdot n!)$, hence, summing over all divisors of ν we obtain $\mathcal{O}(n^{-1/4}\cdot n!)$ permutations of this type, which is sufficiently small.

We find that for each value of ν the contribution of the range $\sqrt{n}<k<\frac{2n}{3}$ is bounded above by $n^{-1/3}\cdot n!$, yielding a total contribution $Nn^{-1/3}n$, which is sufficiently small.

Now, consider permutations σ such that the number of fixed points of σ lies between $2n/3$ and $n-\sqrt{n}$. The number of permutations σ such that there are two or more cycles of length $\geq n^{2/3}$ which are annihilated by ν is bounded above by

$$\sum_{\substack{t_1,t_2\mid\nu\\ t_1,t_2>n^{2/3}}}\frac{n!}{t_1t_2}\leq\frac{n!}{n^{4/3-\epsilon}},$$

that is, the contribution of permutations can be neglected using the trivial estimate $|\chi(\sigma^\nu)|\leq\chi(1)$. Similarly, if σ is a permutation such that σ^ν has $n/6$ fixed points lying in cycles of length $\leq n^{2/3}$ of σ, some cycle length is repeated $\gg n^{1/4}$ times, and there are less than $n^{-2}\cdot n!$ permutations with this property, which give a negligible contribution as well. Hence, we may suppose that σ has one cycle of length t, where $n/2\leq t\leq n$ is a divisor of ν. The number of such divisors is bounded above by $2\nu/n\leq 2N/n$, that is, the number of permutations σ with this property is bounded above by $\frac{4N}{n^2}n!$. To estimate the character sum, we use the trivial bound $|\chi(\sigma)|\leq\chi(1)$ for characters corresponding to partitions with $\lambda_1\geq n-n^{2/3}$ or $\lambda_1'\geq n-n^{2/3}$. The number of characters with this property and $\chi(\mathbf{c})\neq 0$ is $\mathcal{O}(n^{2/3})$, hence, the sum over these characters and permutations σ under consideration is of size $\frac{N}{n^{4/3}}n!$, yielding a total contribution $N^2n^{-4/3}n!<n^{3/4}n!$, which is acceptable. For the remaining characters we again use Lemma 4 together with the estimate $\chi(1)>\binom{n-n^{2/3}}{n^{2/3}}>e^{n^{2/3}}$ to obtain

$$\sum_\chi{}^*\frac{\chi(\sigma)}{\chi(1)}\leq\sum_\chi{}^*\chi(1)^{-\frac{1}{33\sqrt{n\log n}}}\ll ne^{-\frac{n^{1/6}}{33\log n}}\ll e^{-n^{1/7}},$$

which gives a contribution $Ne^{-n^{1/7}}n!$, which is far smaller than necessary.

Finally, consider permutations σ such that σ^ν has more than $n-\sqrt{n}$ fixed points. Then by the same argument as above, we deduce that we may restrict our attention to the case that σ has a cycle of length t for some divisor t of ν in the range $n-2\sqrt{n}\le t\le n$. For fixed t, the number of permutations σ with this property is $\le \frac{2n!}{n}$, and the number of possible ν is $\frac{N}{t}\le 2n^{1/64}$. The trivial bound $|\chi(\sigma^\nu)|\le\chi(1)$ implies that the sum over χ in (2) is $\le 2n$, thus, we find that for fixed t the contribution to the right hand side of (2) is bounded above by $n^{1/64}n!$. There are $2\sqrt{n}$ possible values of t, hence, the contribution of this range is less than $n^{2/3}n!$.

Collecting the various contributions we find that

$$\frac{|\mathbf{c}|^2}{n!}\sum_{\substack{\nu\le N\\ 2|\nu}}\frac{N-\nu}{2}\sum_{\sigma\in S_n\setminus A_n}\sum_{\chi\in\mathrm{Irr}(S_n)}\frac{\chi(\sigma^\nu)\chi(\mathbf{c})^2}{\chi(1)}=\Big(1+\mathcal{O}(n/N)\Big)\frac{N^2\cdot n!^2}{32n^2},$$

which proves Lemma 3, and therefore Proposition 1.

Note that we did not use that π and σ generate S_n, hence, our method also gives a new proof of Netto's conjecture. In fact, the argument applies to all classes $\mathbf{c}$ which consist of elements with one cycle of length very close to n. Suppose that $\pi,\sigma\in S_n$ are chosen at random, and that not both of them are contained in A_n. Then we deduce, that with probability $1-\mathcal{O}(n^{-1/64})$, $\langle\pi,\sigma\rangle$ contains an n-cycle, an $(n-1)$-cycle, and a transposition, that is, $\langle\pi,\sigma\rangle=S_n$. To deal with $\pi,\sigma\in A_n$, one can use for n odd an n-cycle, an $(n-2)$ cycle and the product of an $(n-4)$-cycle with a 3-cycle; for n even one obtains an $(n-1)$-cycle, an $(n-3)$-cycle and the product of an $(n-3)$-cycle with a 3-cycle. The exponent $\frac{1}{64}$ can be improved, however, doing so would require to consider characters χ with $\chi(1)$ small seperately, which would lead to rather lengthy computations; moreover, our method cannot detect whether $\langle\sigma,\pi\rangle$ is transitive or not, thus, the best we could achieve would be an error term $\mathcal{O}(n^{-1})$, which is worse than the best known result $1-\frac{2}{n}+\mathcal{O}(n^{-2})$ obtained by Babai [2].

3. Proof of Theorem 3

If π is chosen at random, then with probability tending to 1, π has less than $\log^2 n$ cycles. The Murnaghan-Nakayama-rule immediately implies that $|\chi(\pi)|<n^{\log^2 n}$ with probability tending to 1 for all irreducible characters χ.

Hence, our claim follows, once we have shown the following.

Proposition 2. *Let $\mathbf{c} \subseteq S_n$ be a conjugacy class consisting of elements with less than $\log^2 n$ cycles, and let τ be an element moving at least αn points. Then the number of cycles of $\tau\sigma$ is asymptotically normal distributed with mean and variance $\log n$.*

Since almost all permutations have less than $7 \log\log n$ cycles of length $\leq \log^5 n$ or $\geq n/\log n$, we may replace the number of cycles by the number of cycles of length in the interval $[\log^5 n, n/\log n]$. Moreover, it suffices to count cycles of distinct length only, hence, by the method of moments, we have to show that for fixed k, the probability that $\tau\sigma$ contains a cycle of length ℓ_i, $1 \leq i \leq k$, is $\frac{1+o(1)}{\ell_1 \cdots \ell_k}$, where the o-Symbol is uniform in all choices $\log^5 n < \ell_1 < \cdots < \ell_k < \frac{n}{\log n}$. Let $\mathbf{1}_{\vec{\ell}}$ be the characteristic function of the set of permutations satisfying this condition. Clearly, $\mathbf{1}_{\vec{\ell}}$ is a class function, hence, we begin by expressing this function as a linear combination of characters.

Lemma 6. *Define $m_{\vec{\ell}}(\chi) = \ell_1 \cdots \ell_k \langle \mathbf{1}_{\vec{\ell}}, \chi \rangle$, and let λ be the partition associated to χ. Suppose that $n > 2(\ell_1 + \cdots + \ell_k)$*

1. *If $m_{\vec{\ell}}(\chi) \neq 0$, then one can clip off rim hooks of length $\ell_1, \ldots, \ell_k$ from λ to obtain the trivial partition $(n - \ell_1 - \cdots - \ell_k)$.*
2. *If $n - \ell_1 < \lambda_1 < n$, then $m_{\vec{\ell}}(\chi) = 0$*
3. *We have always $|m_{\vec{\ell}}(\chi)| < n^k$.*

Proof. Let μ be a partition of $n - \ell_1 - \cdots - \ell_k$, such that $\mu_i \leq \lambda_i$ for all i, that is, the Ferrer's diagram of μ is contained in the Ferrer's diagram of λ. Denote by $N(\lambda, \mu)$ the number of ways to obtain μ from λ by removing rim hooks of length $\ell_1, \ldots, \ell_k$, $N^*(\lambda, \mu)$ be the sum with signs according to the Murnaghan-Nakayama-rule. Let π be a permutation containing cycles of length $\ell_1, \ldots, \ell_k$, and let π^* be the permutation with these cycles removed. Then we have

$$\chi_\lambda(\pi) = \sum_\mu N^*(\lambda, \mu) \chi_\mu(\pi^*),$$

thus

$$\begin{aligned} m_{\vec{\ell}}(\chi) &= \frac{\ell_1 \cdots \ell_k}{n!} \sum_{\pi \in S_n} \mathbf{1}_{\vec{\ell}}(\pi) \chi(\pi) \\ &= \frac{\ell_1 \cdots \ell_k}{n!} \sum_{\substack{\pi \in S_n \\ \mathbf{1}_{\vec{\ell}}(\pi) = 1}} N^*(\lambda, \mu) \chi_\mu(\pi^*) \\ &= \frac{1}{(n - \ell_1 - \cdots - \ell_k)!} \sum_\mu N^*(\lambda, \mu) \sum_{\pi^* \in S_{n - \ell_1 - \cdots - \ell_k}} \chi_\mu(\pi^*) \end{aligned}$$

By orthogonality, the inner sum is 0, unless μ is the trivial partition $\mu_0 = (n-\ell_1-\cdots-\ell_k)$, and we obtain

$$|m_{\vec{\ell}}(\chi)| = \left|\sum_{\mu} N^*(\lambda,\mu_0)\right| \le \sum_{\mu} N(\lambda,\mu_0).$$

In particular, if $N(\lambda,\mu_0)=0$, we have $m_{\vec{\ell}}(\chi)=0$, which implies the first claim. If $\lambda_1 > n-\ell_1$, we cannot remove a rim hook of length ℓ_i without taking boxes from the first row, since the number of boxes outside the first row is smaller than the number of boxes to be removed. On the other hand, if $\lambda_1 > n-\ell_1$, then after removing $\ell_1+\ldots+\ell_k$ boxes from the first row, the first row is still longer than the second one, that is, we did not remove any boxes outside the first row at all. Hence, $N(\lambda,\mu_0)$ is only non-zero, if λ is trivial, proving our second claim. For the last claim note that $|N^*(\lambda,\mu)| \le N(\lambda,\mu)$, hence, $m_{\vec{\ell}}(\chi)$ is bounded above by the number of ways to remove k rim hooks from λ. Every rim hook is defined by its upper-rightmost box, hence, there are at most n rim hooks, and the third claim is proven as well. ∎

Now we compute the probability P that $\tau\sigma$ has cycles of length $\ell_1,\ldots,\ell_k$. To simplify computations it is convenient to pass from τ to the conjugacy class $[\tau]$ of τ, clearly, this does not affect the final result. We have

$$\begin{aligned}
P &= \frac{1}{|\mathbf{c}|}\sum_{\sigma\in\mathbf{c}} \mathbf{1}_{\vec{\ell}}(\tau\sigma)\\
&= \frac{1}{\ell_1\cdots\ell_k|\mathbf{c}|}\sum_{\sigma\in\mathbf{c}}\sum_{\chi} m_{\vec{\ell}}(\chi)\chi(\tau\sigma)\\
&= \frac{1}{\ell_1\cdots\ell_k|\mathbf{c}||[\tau]|}\sum_{\substack{\sigma\in\mathbf{c}\\ \tau'\in[\tau]}}\sum_{\chi} m_{\vec{\ell}}(\chi)\chi(\tau\sigma)\\
&= \frac{1}{\ell_1\cdots\ell_k n!}\sum_{\pi\in S_n}\sum_{\chi_1} m_{\vec{\ell}}(\chi)\chi_1(\pi)\sum_{\chi_2}\frac{\chi_2(\sigma)\chi_2(\tau)\chi_2(\pi)}{\chi_2(1)}.
\end{aligned}$$

The sum over π vanishes, unless $\chi_1=\chi_2$, in which case it becomes $n!$. Hence, applying Lemma 6, we obtain

$$P = \frac{1}{\ell_1\cdots\ell_k}\left(1+\mathcal{O}\left(n^k\cdot\sum_{\substack{\lambda\\ n-\frac{2n}{\log n}<\lambda_1<n-\log^5 n}}\frac{\chi_\lambda(\sigma)\chi_\lambda(\tau)}{\chi_\lambda(1)}\right)\right).$$

Now we estimate $\chi_\lambda(\tau)$ using Lemma 4, and $\chi_\lambda(\sigma)$ by $n^{\log^2 n}$, since σ was chosen to have at most $\log^2 n$ cycles. We find that the error term is at most

$$n^{2\log^2 n} \sum_{n-\frac{2n}{\log n}<\lambda_1<n-\log^5 n} \chi_\lambda(1)^{-\frac{\alpha}{32\log n}}$$

For $A < n/3$, the number of characters with $\lambda_1 = n - A$ equals the number of partitions of A, and for each such λ we have $\chi_\lambda(1) > \binom{n-A}{A}$, since when decomposing λ, we may choose which boxes to take from outside the first row. Hence, the error term is bounded above by

$$n^{2\log^2 n} \sum_{\log^5 n<A<\frac{n}{\log n}} e^{c\sqrt{A}} \binom{n-A}{A}^{-\frac{\alpha}{32\log n}} \ll n^{2\log^2 n} \sum_{\log^5 n<A<\frac{n}{\log n}} e^{-\frac{\alpha A}{32\log n}}.$$

Clearly, the summands are decreasing in A, which implies that the whole sum is of order $ne^{-\frac{\alpha\log^4 n}{32}}$, and we find that the probability for $\tau\sigma$ to have cycles of length $\ell_1, \dots, \ell_k$ equals

$$\frac{1}{\ell_1 \cdots \ell_k}\left(1 + \mathcal{O}\left(e^{-\frac{\alpha\log^4 n}{40}}\right)\right).$$

Defining the random variables ξ_i to be the number of cycles of length i, where $\log^5 n < i < \frac{n}{\log n}$, we find that for each fixed k the k-th moment of the sum of the ξ_i is asymptotically equal to the k-th moment of independent random variables with the same mean, hence, the distribution of the sum converges to a normal distribution. Since the contribution of very small or very large cycles is almost always of smaller order of magnitude, Theorem 3 follows.

References

[1] L. Babai, Á. Seress: On the diameter of Cayley graphs of the symmetric group, *J. Combin. Theory Ser. A* **49** (1988), 175–179.

[2] L. Babai: The probability of generating the symmetric group, *J. Combin. Theory Ser. A* **52** (1989), 148–153.

[3] L. Babai, G. L. Hetyei: On the diameter of random Cayley graphs of the symmetric group, *Combin. Probab. Comput.* **1** (1992), 201–208.

[4] L. Babai, T. P. Hayes: Near-independence of permutations and an almost sure polynomial bound on the diameter of the symmetric group, In *Proceedings of the Sixteenth Annual ACM-SIAM Symposium on Discrete Algorithms,* 1057–1066, ACM, New York, 2005.

[5] L. Babai: On the diameter of Eulerian orientations of graphs, In *Proceedings of the Seventeenth Annual ACM-SIAM Symposium on Discrete Algorithms,* 822–831, ACM, New York, 2006.
[6] S. Bratus, I. Pak: Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's conjecture, *J. Symbolic Comput.* **29** (2000), 33–57.
[7] C. Curtis, I. Reiner: *Methods of Representation theory* I, Wiley Interscience, New York, 1990.
[8] J. D. Dixon: The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.
[9] P. Erdős, P. Turán: On some problems of a statistical group-theory II, *Acta math. Acad. Sci. Hungar.* **18** (1967), 151–163.
[10] T. W. Müller, J.-C. Schlage-Puchta: Character theory of symmetric groups, subgroup growth of Fuchsian groups, and random walks, *Adv. Math.* **213** (2007), 919–982.

Jan-Christoph Schlage-Puchta

Mathematisches Institut
Eckerstr. 1
79104 Freiburg
Germany
jcsp@cage.ugent.be