ALTERNATING GROUPS AS PRODUCTS OF FOUR CONJUGACY CLASSES

MARTINO GARONZI AND ATTILA MARÓTI

ABSTRACT. Let G be the alternating group $\mathrm{Alt}(n)$ on n letters. We prove that for any $\varepsilon > 0$ there exists $N = N(\varepsilon) \in \mathbb{N}$ such that whenever $n \geq N$ and A, B, C, D are normal subsets of G each of size at least $|G|^{1/2+\varepsilon}$, then $ABCD = G$.

1. INTRODUCTION

Given two subsets A, B of a group G we denote by AB the set of products ab where $a \in A$, $b \in B$. A subset A of G is called normal if $gAg^{-1} = A$ for all $g \in G$. Clearly, a subset of G is normal if and only if it is a union of conjugacy classes. Observe that if A and B are normal sets, then $AB = BA$.

The covering number of a nontrivial conjugacy class C of a finite nonabelian simple group G is the minimum positive integer k such that $C^k = G$. Brenner [2] showed that almost all conjugacy classes of the alternating group $\mathrm{Alt}(n)$ have covering number at most 4, and observed that there are classes with covering number 4, for example the class of fixed-point-free involutions (see the penultimate paragraph of the Introduction).

Larsen and Shalev [5, Theorem 1.13] proved that an element g of the symmetric group $\mathrm{Sym}(n)$ satisfies $(g^{\mathrm{Sym}(n)})^2 = \mathrm{Alt}(n)$ with probability tending to 1 as $n \to \infty$. (Here and throughout the paper x^G denotes the conjugacy class of an element x in a finite group G.) For a related result see [5, Theorem 1.20]. Larsen and Shalev also proved [5, Theorem 1.14] that if n is sufficiently large, then any element $g \in \mathrm{Sym}(n)$ with at most $n/5$ fixed points satisfies $(g^{\mathrm{Sym}(n)})^4 = \mathrm{Alt}(n)$.

In this paper we take a different approach, considering the product of possibly distinct normal sets. Larsen, Shalev and Tiep [6] proved that if $\varepsilon > 0$ is a constant, then for sufficiently large n the following holds: whenever A, B are two normal subsets of $G = \mathrm{Alt}(n)$ of size larger than $\varepsilon|G|$, then AB contains every nontrivial element of G, and they proved that the same holds for simple groups of Lie type of bounded rank. In this context, a subset is large if it has size at least the size

of G multiplied by a universal positive constant (less than 1). Observe that using their result it is easy to see that, if A, B, C are large normal subsets of G, then $ABC = G$. We are interested in studying largeness related to the size of G raised to a constant γ.

Let $G = \text{Alt}(n)$ be the alternating group on n letters. In [7, Theorem 1.3] it is proved that there exists γ with $0 < \gamma < 1$ such that whenever 8 normal subsets of G have size at least $|G|^\gamma$, their product is G. It was asked if the same holds with less than 8 normal sets. In this paper we prove that the result holds for 4 normal sets and that if γ is close to $1/2$, then this is best possible.

Theorem 1.1. *For any $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that whenever $n > N$ and A, B, C, D are normal subsets of $G = \text{Alt}(n)$ such that all of the numbers $|A||B|$, $|A||C|$, $|A||D|$, $|B||C|$, $|B||D|$, $|C||D|$ are at least $|G|^{1+\varepsilon}$, then $ABCD = G$.*

In particular Theorem 1.1 applies to the case in which the four normal subsets have size not less than $|G|^{1/2+\varepsilon}$, improving [7, Theorem 1.3] in the case of alternating groups. The question of whether there exists γ with $\gamma < 1$ such that, whenever A, B, C are normal subsets of $G = \text{Alt}(n)$ with $|A|, |B|, |C| \geq |G|^\gamma$, then $ABC = G$ is still open, however Theorem 1.1 goes in this direction, since one of the four classes is allowed to be very small. If we interpret largeness in the sense of Larsen, Shalev and Tiep, then the product of any three large normal sets equals G, as seen above.

Theorem 1.1 is best possible in the following sense. Let n be a multiple of 4, let $G = \text{Alt}(n)$ and let x be a fixed-point-free involution in G. Let C be the conjugacy class of x in G. Then, using the fact that $(n/3)^n \leq n! \leq (n/2)^n$ whenever $n \geq 6$, which can be easily deduced from Stirling's inequalities, one may see that if n is sufficiently large, then $|C| = (n-1)!! = (n-1)(n-3)\cdots 3 \cdot 1 \geq (2/3)^n |G|^{1/2}$. This implies that $|C|$ is arbitrarily close to $|G|^{1/2}$ in the sense that for every $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that $|C| \geq |G|^{1/2-\varepsilon}$ for every $n \geq N$. However, as shown by Brenner in [2, Lemma 3.06], $C^3 \neq G$ and $C^4 = G$. See also [9].

The paper is organized as follows. In Section 2 we introduce a useful tool by Dvir and Rodgers used to decide whether a product of two conjugacy classes of $\text{Sym}(n)$ contains the n-cycles, for n odd, and the $(n-1)$-cycles, for n even, based on the number of disjoint cycles of an element in each class (Theorem 2.1). We then relate this to our context (Lemma 2.3). In Section 3 we recall known facts about character sums and how to apply them to products of conjugacy classes. In Section 4 we recall how to compute character values for the symmetric and alternating groups. In Section 5 we finish the proof of Theorem 1.1.

2. The δ of a conjugacy class

Given a conjugacy class C of $\text{Alt}(n)$ or $\text{Sym}(n)$, let $\delta(C) := n - t$, where t is the number of disjoint cycles of an element of C. Dvir [3] proved a fact reformulated by Rodgers [8, Theorem 1.1(iii)], which we will state here a particular case of. Denote the set of all n-cycles in $\text{Sym}(n)$ by O_n, and denote the set of all $(n-1)$-cycles in $\text{Sym}(n)$ by O_{n-1}. Observe that if C is a conjugacy class of $\text{Sym}(n)$ contained in $\text{Alt}(n)$ then $\delta(C)$ is even.

Theorem 2.1. *Let A, B be two conjugacy classes of $\text{Sym}(n)$ contained in $\text{Alt}(n)$.*

(1) *If n is odd and $\delta(A) + \delta(B) > n - 1$, then $O_n \subseteq AB$.*
(2) *If n is even and $\delta(A) + \delta(B) > n$, then $O_{n-1} \subseteq AB$.*

Using Dvir's results, Rodgers proved the following [8, Lemma 2.2]:

Lemma 2.2. $O_n^2 = O_{n-1}^2 = \mathrm{Alt}(n)$ *for every n.*

Let $G = \mathrm{Alt}(n)$. In order to apply Theorem 2.1 in our context, we need to translate the condition $|C| \geq |G|^\gamma$, for a conjugacy class C of G and a constant γ, into a lower bound for $\delta(C)$. This is precisely what we do in the following lemma.

Lemma 2.3. *For every γ and ε with $0 < \gamma < 1$ and $0 < \varepsilon < 1$ there exists $N \in \mathbb{N}$ such that for every $n \geq N$, whenever $x \in G = \mathrm{Alt}(n)$ satisfies $|x^G| \geq |G|^\gamma$, then $\delta(x^G) > (\gamma - \varepsilon)n$.*

Proof. Let γ and ε be arbitrary positive real numbers less than 1. Choose ε_1 with $0 < \varepsilon_1 < \varepsilon/(1 - \gamma + \varepsilon)$, and observe that $\varepsilon_1 < 1$. Let $x \in G = \mathrm{Alt}(n)$ be such that $|x^G| \geq |G|^\gamma$. Let r_i be the number of i-cycles in the cycle structure of x for $i = 1, \ldots, t$, where t is a fixed positive integer such that

$$\frac{1}{2}\varepsilon_1(1 - \gamma + \varepsilon) < \frac{1}{t + 1} < \varepsilon_1(1 - \gamma + \varepsilon).$$

Set $s := \sum_{i=1}^{t} r_i$. The number of disjoint cycles of x is at most $n/(t + 1) + s$, thus

$$\delta(x^G) \geq n - \frac{n}{t + 1} - s > n - \varepsilon_1(1 - \gamma + \varepsilon)n - s.$$

In order to prove the lemma, it is sufficient to show that $s < n(1 - \varepsilon_1)(1 - \gamma + \varepsilon)$ for every sufficiently large n.

Observe that we may assume that s is not bounded above by a fixed universal constant. In particular we assume that $s > 3t$.

By plugging $x_1 = \ldots = x_t = 1$ into the well-known identity of multinomial coefficients

$$(x_1 + \cdots + x_t)^s = \sum_{k_1 + \ldots + k_t = s} \frac{s!}{k_1! \cdots k_t!} \prod_{i=1}^{t} x_i^{k_i},$$

we obtain $s!/t^s \leq \prod_{i=1}^{t} r_i!$.

An easy application of Stirling's inequality gives $s! \geq (s/3)^s$. Since $\gamma > 0$ and $|x^G| \geq |G|^\gamma$, x is not the identity and so $\prod_{i=1}^{t} r_i! \leq |C_G(x)| \leq |G|^{1-\gamma}$. We obtain

$$(s/3t)^s \leq s!/t^s \leq \prod_{i=1}^{t} r_i! \leq |C_G(x)| \leq (n!/2)^{1-\gamma} < n^{n(1-\gamma)}.$$

Taking natural logarithms we obtain $s \log(s/3t) < n(1 - \gamma)\log(n)$. Since $s > 3t$, we obtain

$$s < n(1 - \gamma)\frac{\log(n)}{\log(s/3t)}.$$

Let

$$\mathcal{A} := \{(n, s) \in \mathbb{N} \times \mathbb{N} \; : \; \exists x \in G \; : \; |x^G| \geq |G|^\gamma \text{ and } s \geq n(1 - \varepsilon_1)(1 - \gamma + \varepsilon)\}.$$

In order to prove the result, it is enough to show that $\mathcal{A}$ is finite. Assume by contradiction that $\mathcal{A}$ is infinite. Observe that, if $(n, s) \in \mathcal{A}$, then

$$\frac{\log(n)}{\log(s/3t)} = \frac{\log(n)}{\log(s) - \log(3t)} \leq \frac{\log(n)}{\log(n) + \log((1 - \varepsilon_1)(1 - \gamma + \varepsilon)) - \log(3t)}.$$

It follows that $\log(n)/\log(s/3t)$ tends to 1 as $(n, s) \in \mathcal{A}$ and n goes to infinity, since ε_1, γ, ε and t are fixed.

Since $\frac{\varepsilon(1-\varepsilon_1)}{1-\gamma} > \frac{\varepsilon}{1-\gamma+\varepsilon} > \varepsilon_1$, there exists ε_2 such that $0 < \varepsilon_2 < \frac{\varepsilon(1-\varepsilon_1)}{1-\gamma} - \varepsilon_1$. If $(n, s) \in \mathcal{A}$ and n is sufficiently large, we have $\log(n)/\log(s/3t) \leq 1 + \varepsilon_2$, therefore

$$s < n(1 - \gamma)(1 + \varepsilon_2) < n(1 - \gamma)\left(1 + \frac{\varepsilon(1 - \varepsilon_1)}{1 - \gamma} - \varepsilon_1\right) = n(1 - \varepsilon_1)(1 - \gamma + \varepsilon).$$

This contradicts the fact that $(n, s) \in \mathcal{A}$. □

3. Background on character sums

Let $\mathrm{Irr}(G)$ denote the set of irreducible complex characters of a finite group G.

If A, B are conjugacy classes of G we are interested to know which conjugacy classes the normal set AB contains. Fix $a \in A$, $b \in B$, $g \in G$. Then [1, page 43] gives

$$|\{(x, y) \in A \times B \ : \ xy = g\}| = \frac{|A||B|}{|G|}\left(\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(a)\chi(b)\overline{\chi(g)}}{\chi(1)}\right).$$

It follows that the conjugacy class of g in G is contained in the normal set AB if and only if

$$(1) \qquad\qquad \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(a)\chi(b)\overline{\chi(g)}}{\chi(1)} \neq 0.$$

Assume G is the alternating group $\mathrm{Alt}(n)$. The strategy to show that condition (1) holds will often be the following: first, we separate the contribution of the trivial character in the sum, which is 1, then we show that the remaining part tends to 0 when n tends to infinity. This implies that in this case condition (1) holds when n is sufficiently large.

4. Background on characters of $\mathrm{Alt}(n)$

In this section we review some basic facts about the characters of the alternating and symmetric groups. Everything here may be found in [4, Chapter 2].

A partition $\lambda = (\lambda_1, \dots, \lambda_t)$ of n is a sequence of positive integers $\lambda_1 \geq \dots \geq \lambda_t$ such that $\lambda_1 + \dots + \lambda_t = n$. The partitions of n correspond bijectively to the cycle structures of the elements of $\mathrm{Sym}(n)$ and to the Young diagrams of size n. Each partition λ of n determines uniquely a complex irreducible character χ_λ of $\mathrm{Sym}(n)$, and these are precisely the complex irreducible characters of $\mathrm{Sym}(n)$. We will use the well-known Murnaghan-Nakayama rule to compute character values, and the well-known hook length formula to compute character degrees.

We define l to be n if n is odd and $n-1$ if n is even. An l-hook will be a hook of length l. An immediate consequence of the Murnaghan-Nakayama rule is the following. Assume that λ is a partition of n and $g \in \mathrm{Sym}(n)$ is an l-cycle. If λ contains an l-hook then $\chi_\lambda(g) = (-1)^k$ where k is the leg length of the unique l-hook of λ. If λ does not contain an l-hook, then $\chi_\lambda(g) = 0$.

Before describing the irreducible complex characters of $\mathrm{Alt}(n)$ we introduce a notation. The conjugacy class of an element g of $\mathrm{Alt}(n)$ may or may not be equal to its conjugacy class in $\mathrm{Sym}(n)$. If it is (resp. if it is not), we call g a non-exceptional (resp. exceptional) element, the conjugacy class of g a non-exceptional (resp. exceptional) class and the cycle type of g a non-exceptional (resp. exceptional) cycle type. Since partitions of n correspond bijectively to cycle types, we may also talk about exceptional and non-exceptional partitions. Recall that an element of $\mathrm{Alt}(n)$ is exceptional if and only if the lengths of the cycles in its disjoint cycle decomposition are odd and pairwise distinct (including 1-cycles), and that the conjugacy class in $\mathrm{Sym}(n)$ of an exceptional element is the union of precisely two conjugacy classes of $\mathrm{Alt}(n)$ of equal size. An important example of an exceptional element is given by any l-cycle, where l is defined in the previous paragraph.

The irreducible complex characters of $\mathrm{Alt}(n)$ are described as follows. Let λ be a partition of n. Denote by λ' the partition adjoint to λ, obtained by reflecting its Young diagram through the main diagonal. The partition λ is said to be self-adjoint if $\lambda = \lambda'$. If $\lambda \neq \lambda'$, then the restriction of the character χ_λ to $\mathrm{Alt}(n)$ is an irreducible character of $\mathrm{Alt}(n)$, which we denote by ψ_λ. Clearly, $\psi_\lambda = \psi_{\lambda'}$ in this case. If $\lambda = \lambda'$, then the restriction of the character χ_λ to $\mathrm{Alt}(n)$ is the sum of two irreducible characters ψ_λ^+, ψ_λ^- of $\mathrm{Alt}(n)$. Every irreducible complex character of $\mathrm{Alt}(n)$ is of the form ψ_λ where λ is a non-self-adjoint partition or $\psi_\lambda^\pm$ where λ is a self-adjoint partition.

Given a self-adjoint partition λ of n, denote by $h(\lambda)$ the partition whose parts are the lengths of those hooks of λ whose heads are in the main diagonal. Observe that $h(\lambda)$ is an exceptional partition. For example, if λ is a self-adjoint hook, then $h(\lambda)$ is the partition (n).

Let λ be a partition of n and let $x \in \mathrm{Alt}(n)$. If $\lambda \neq \lambda'$, then $\psi_\lambda(x) = \chi_\lambda(x)$. If $\lambda = \lambda'$ and the cycle type of x is not $h(\lambda)$, then $\psi_\lambda^\pm(x) = \chi_\lambda(x)/2$. If $\lambda = \lambda'$ and the cycle type of x is $h(\lambda)$, then x is an exceptional element, hence there exists $y \in \mathrm{Sym}(n)$ which is conjugate to x in $\mathrm{Sym}(n)$ but not in $\mathrm{Alt}(n)$. Let h_{ii}^λ be the length of the hook in λ with head in position (i,i). We have

$$\psi_\lambda^\pm(x) = \frac{1}{2}\left(\chi_\lambda(x) \pm \sqrt{\chi_\lambda(x)\prod_i h_{ii}^\lambda}\right), \quad \psi_\lambda^\pm(y) = \frac{1}{2}\left(\chi_\lambda(y) \mp \sqrt{\chi_\lambda(y)\prod_i h_{ii}^\lambda}\right).$$

An important consequence for us is the following. Let l be n if n is odd and $n-1$ if n is even and let x be an l-cycle. Let λ be a partition of n. If λ does not contain an l-hook, then $\psi_\lambda(x) = 0$. Assume λ contains an l-hook. Observe that in this case λ contains a unique l-hook. If $\lambda \neq \lambda'$, then $\psi_\lambda(x) = \chi_\lambda(x) = (-1)^k$ where k is the leg length of the l-hook contained in λ. If $\lambda = \lambda'$, then $|\psi_\lambda^\pm(x)| \leq \sqrt{n}$.

5. Proof of Theorem 1.1

In this section we prove Theorem 1.1. First we need a list of technical lemmas.

The following is a special case of [5, Theorem 1.2].

Theorem 5.1 (Larsen, Shalev)**.** *If $\sigma \in \mathrm{Sym}(n)$ has at most $n^{o(1)}$ cycles of length at most 5, then $|\chi(\sigma)| \leq \chi(1)^{1/5+o(1)}$ for every complex irreducible character χ of $\mathrm{Sym}(n)$.*

This theorem will be applied in the special case when σ is an exceptional element in $\mathrm{Sym}(n)$, and $\chi = \chi_\lambda$, where λ is a partition containing an n-hook for n odd and an $(n-1)$-hook for n even.

Let l be n if n is odd and $n-1$ if n is even.

Lemma 5.2. *Let $n \geq 9$ and let $G = \mathrm{Alt}(n)$. Let $\psi \in \mathrm{Irr}(G)$ be a nontrivial character associated to a partition λ of n containing an l-hook. Either $\psi(1) \geq n(n-3)/2$ or n is odd, ψ is equal to the restriction of χ_λ to G where $\lambda = (n-1,1)$ and $\psi(1) = n-1$. Moreover if $\lambda = \lambda'$, then $\psi(1) \geq 2^{n-2}/n^2$.*

Proof. Since ψ is nontrivial, both λ and λ' are different from (n). Let $\lambda = \lambda'$. The hook length formula implies

$$
\psi(1) = \begin{cases} \frac{1}{2}\binom{n}{n/2}\frac{(n/2-1)^2}{n-1} & \text{if } n \text{ is even,} \\[2ex] \frac{1}{2}\binom{n-1}{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}
$$

It follows that $\psi(1) \geq n(n-3)/2$ for $n \geq 9$. In any case $\psi(1) \geq 2^{n-2}/n^2$. Now let $\lambda \neq \lambda'$. Let $k \geq 1$ be the leg length of the unique l-hook contained in λ. We will use the hook length formula to compute $\psi(1)$. If n is odd, then $\psi(1) = \binom{n-1}{k}$. This is either $n-1$ or at least $\binom{n-1}{2}$. Let n be even. Without loss of generality, k satisfies $1 \leq k \leq n/2 - 1$ and

$$
\psi(1) = d(n,k) := \binom{n}{k+1}\frac{k(n-k-2)}{n-1}.
$$

We claim that $d(n,k) \geq \binom{n-1}{2}$. Observe that if $k \geq 3$ we have $k(n-k-2) \geq n-3$ whenever $n \geq 6$, hence $d(n,k) \geq d(n,1)$, and if $n \geq 8$ then

$$
d(n,1) \leq d(n,2) \leq d(n,3).
$$

This implies that if $n \geq 8$ then, for any k between 1 and $n/2-1$, we have $d(n,k) \geq d(n,1) = n(n-3)/2$. $\qquad\square$

Denote the set of all l-cycles in $\mathrm{Sym}(n)$ by O_l.

Lemma 5.3. *Let A and B be conjugacy classes of $G = \mathrm{Alt}(n)$, and let n be sufficiently large.*

(1) If A and B are exceptional classes, then AB contains O_l.
(2) If A and B are classes of l-cycles, then AB contains every exceptional class.
(3) If A is a class of l-cycles, then $O_l A = G$.
(4) The product of any three classes of l-cycles equals G.

Proof. We prove part (1). Assume A and B are exceptional classes of G and let D be the conjugacy class in G of an l-cycle. Let $x \in A$, $y \in B$, and $g \in D$. Let $\psi \in \mathrm{Irr}(G)$ be arbitrary, and let λ be the partition of n associated to ψ. Then $\psi(g) = 0$, unless the Young diagram of λ contains an l-hook, by Section 4. Therefore, it is enough to show that (cf. Section 3) the rational number

$$\Sigma := \sum_\psi \frac{\psi(x)\psi(y)\overline{\psi(g)}}{\psi(1)}$$

tends to 0 as n tends to infinity, where the sum is over the nontrivial irreducible characters of G corresponding to partitions containing an l-hook. Let z be any of x, y, or g. For such characters ψ we have $|\psi(z)| \leq |\chi_\lambda(z)|$, unless λ is self-adjoint and z is an l-cycle. Let λ be self-adjoint, and assume z is an l-cycle. We have $|\psi(z)| \leq \sqrt{n}$, which is at most $\psi(1)^{o(1)}$ as $n \to \infty$ by Lemma 5.2. Since x, y, g are exceptional elements, we obtain the following by Theorem 5.1 and Lemma 5.2 for n sufficiently large.

$$|\Sigma| \leq \sum_\psi \left| \frac{\psi(x)\psi(y)\overline{\psi(g)}}{\psi(1)} \right| = \sum_\psi \frac{|\psi(x)||\psi(y)||\psi(g)|}{\psi(1)} \leq \sum_\psi \psi(1)^{-3/5+o(1)}$$

$$\leq (n-1)^{-3/5+o(1)} + n \left(\frac{n(n-3)}{2} \right)^{-3/5+o(1)},$$

where the sums are over the nontrivial irreducible characters ψ of G associated to partitions containing an l-hook. Therefore $|\Sigma|$ tends to 0 as $n \to \infty$.

We prove part (2). Assume A, B are classes of l-cycles and C is any exceptional class. We need to show that $C \subseteq AB$. Since the conjugacy class B^{-1} of the inverse of an element of B is an exceptional class, $A \subseteq CB^{-1}$ by part (1). Fix $a \in A$. There exist $b \in B$, $c \in C$ such that $a = cb^{-1}$, so that $c = ab \in AB$. Since C is the conjugacy class of c and AB is a normal set, $C \subseteq AB$ follows.

We prove part (3). Let A be a class of l-cycles. Then, since $O_l O_l = G$ (by Lemma 2.2), $O_l A$ contains a representative of every conjugacy class of $\mathrm{Sym}(n)$, therefore $O_l A$ contains every non-exceptional class. On the other hand, O_l contains a class of G consisting of l-cycles, hence $O_l A$ also contains every exceptional class by part (2). It follows that $O_l A = G$.

We prove part (4). Let A, B, C be classes of l-cycles. Then AB contains O_l by part (1), so $ABC = G$ by part (3). $\qquad\square$

Lemma 5.4. *Let A, B be conjugacy classes of $G = \mathrm{Alt}(n)$. If neither A nor B is contained in O_l and AB contains an l-cycle, then AB contains O_l.*

Proof. Let $x \in A$, $y \in B$. Choose two nonconjugate l-cycles d_1, d_2 of G such that $d_1 \in AB$. We need to show that d_2 belongs to AB. Let

$$a_i := \sum_{\psi \in \mathrm{Irr}(G)} \frac{\psi(x)\psi(y)\overline{\psi(d_i)}}{\psi(1)}.$$

As explained in Section 3, the fact that $d_1 \in AB$ is equivalent to saying that $a_1 \neq 0$. We need to show that $a_2 \neq 0$. We will show that $a_1 = a_2$.

Section 4 implies that in the formula that defines a_i the summation can be done only over those ψ which are labelled by partitions containing an l-hook. If λ is not a self-adjoint partition containing an l-hook, then there is precisely one irreducible character ψ of G associated to λ and the corresponding summand is the same in a_1 and in a_2. Assume now that $\lambda = \lambda_0$ is the unique self-adjoint partition of n containing an l-hook, so that the restriction of χ_{λ_0} to G is a sum of two irreducible characters $\psi_{\lambda_0}^+$ and $\psi_{\lambda_0}^-$. Since $x, y, 1$ are not of cycle type $h(\lambda_0)$, we have $\psi_{\lambda_0}^+(x) = \psi_{\lambda_0}^-(x)$, $\psi_{\lambda_0}^+(y) = \psi_{\lambda_0}^-(y)$ and $\psi_{\lambda_0}^+(1) = \psi_{\lambda_0}^-(1)$. It follows that

$$a_1 - a_2 = \frac{\psi_{\lambda_0}^+(x)\psi_{\lambda_0}^+(y)}{\psi_{\lambda_0}^+(1)} \cdot \left(\overline{\psi_{\lambda_0}^+(d_1)} + \overline{\psi_{\lambda_0}^-(d_1)} - \overline{\psi_{\lambda_0}^+(d_2)} - \overline{\psi_{\lambda_0}^-(d_2)} \right).$$

The second factor equals $\overline{\chi_{\lambda_0}(d_1) - \chi_{\lambda_0}(d_2)}$, which is equal to 0 since d_1 and d_2 are conjugate in $\mathrm{Sym}(n)$. $\square$

Lemma 5.5. *Let $\varepsilon > 0$. There exists $N \in \mathbb{N}$ such that the following holds for every $n \geq N$: whenever A and B are conjugacy classes of $G = \mathrm{Alt}(n)$ not contained in O_l and $|A||B| \geq |G|^{1+\varepsilon}$, then $AB \supseteq O_l$.*

Proof. If both A and B are exceptional, then the result follows from Lemma 5.3(1). Assume without loss of generality that A is non-exceptional. Let B' be the conjugacy class of $\mathrm{Sym}(n)$ containing B. We claim that $AB' \supseteq O_l$. Write $|A| = |G|^{\gamma_1}$, $|B| = |G|^{\gamma_2}$, so that $0 < \gamma_i < 1$ for $i = 1, 2$ and $\gamma_1 + \gamma_2 \geq 1 + \varepsilon$. Lemma 2.3 implies that if n is large enough, then $\delta(A) > n(\gamma_1 - \varepsilon/2)$ and $\delta(B) > n(\gamma_2 - \varepsilon/2)$, therefore

$$\delta(A) + \delta(B') = \delta(A) + \delta(B) > n(\gamma_1 + \gamma_2 - \varepsilon/2 - \varepsilon/2) \geq n(1 + \varepsilon - \varepsilon) = n,$$

which implies that AB' contains O_l by Theorem 2.1. We may assume that B' properly contains B, that is, B is an exceptional class. Since AB' contains O_l, the normal set AB contains an l-cycle, hence AB contains O_l by Lemma 5.4. $\square$

Lemma 5.6. *Theorem 1.1 holds in the case when A, B, C, D are conjugacy classes.*

Proof. Let l be n if n is odd and $n-1$ if n is even. If at least three of the classes A, B, C, D consist of l-cycles, then the result follows from Lemma 5.3(4). Therefore we may assume that A and B are not classes of l-cycles, so that $O_l \subseteq AB$ by Lemma 5.5. If any of C, D is a class of l-cycles, then the result follows from Lemma 5.3(3) and if C and D are not classes of l-cycles, then the result follows from Lemma 5.5 and Lemma 2.2. $\square$

Proof of Theorem 1.1. Let $|A| = |G|^a$, $|B| = |G|^b$, $|C| = |G|^c$, $|D| = |G|^d$. For any $\gamma > 0$ there exists $N = N(\gamma) \in \mathbb{N}$ such that whenever $n > N$, any normal subset S of G of size at least $|G|^\gamma$ contains a conjugacy class of G of size at least $|G|^{\gamma - \varepsilon/3}$ by [7, Lemma 4.2]. Applying this for $n > \max\{N(a), N(b), N(c), N(d)\}$ and for $(S, \gamma) = (A, a), (B, b), (C, c), (D, d)$ we obtain that there exist conjugacy classes A_0, B_0, C_0, D_0 of G contained in A, B, C, D respectively, such that $|A_0| \geq |G|^{a - \varepsilon/3}$, $|B_0| \geq |G|^{b - \varepsilon/3}$, $|C_0| \geq |G|^{c - \varepsilon/3}$ and $|D_0| \geq |G|^{d - \varepsilon/3}$. The hypotheses of Theorem 1.1 hold for A_0, B_0, C_0, D_0 with the constant $\varepsilon/3$. Hence $ABCD \supseteq A_0 B_0 C_0 D_0 = G$ by Lemma 5.6. $\square$

References

[1] Z. Arad, M. Herzog, J. Stavi, Powers and products of conjugacy classes in groups. Products of conjugacy classes in groups, 6–51, *Lecture Notes in Math.*, 1112, Springer, Berlin, 1985.

[2] J. L. Brenner, Covering theorems for finasigs VIII - Almost all conjugacy classes in A_n have exponent ≤ 4. *J. Austral. Math. Soc.* 25 (Series A) (1978), 210–214.

[3] Y. Dvir, Covering properties of permutation groups. Products of conjugacy classes in groups, 197–221, *Lecture Notes in Math.*, 1112, Springer, Berlin, 1985.

[4] G. James, A. Kerber, The representation theory of the symmetric group. *Encyclopedia of Mathematics and its Applications*, 16. Addison-Wesley Publishing Co., Reading, Mass., 1981.

[5] M. Larsen, A. Shalev, Characters of symmetric groups: sharp bounds and applications. *Invent. Math.* **174** (2008), no. 3, 645–687.

[6] M. Larsen, A. Shalev, P. H. Tiep, Products of normal subsets and derangements. Arxiv:2003.12882.

[7] A. Maróti, L. Pyber, A generalization of the diameter bound of Liebeck and Shalev for finite simple groups. Arxiv:2003.14270.

[8] D. M. Rodgers, Generating and covering the alternating or symmetric group. *Comm. Algebra* **30** (2002), no. 1, 425–435.

[9] U. Vishne, Mixing and covering in the symmetric groups. *J. Algebra* **205** (1998), 119–140.

(Martino Garonzi) DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE DE BRASÍLIA, CAMPUS UNIVERSITÁRIO DARCY RIBEIRO, BRASÍLIA-DF, 70910-900, BRAZIL

Email address: `mgaronzi@gmail.com`

(Attila Maróti) ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, REÁLTANODA UTCA 13-15, H-1053, BUDAPEST, HUNGARY

Email address: `maroti.attila@renyi.hu`