MIXING AND COVERING IN THE SYMMETRIC GROUPS

UZI VISHNE

Abstract. We discuss mixing and covering theorems in the symmetric groups. We present an example of a covering without mixing, and study the conjugacy class $[2^{n/2}]$ of symmetric group S_n, which demonstrates mixing without covering. We derive some new character identities from computation of $[2^{n/2}]^2$,and also compute $[2^{n/2}]^3$, filling a hole between theorems of Brenner [3] and Dvir [6]. This computation also motivates a certain classification of 3-colored 3-regular graphs.

Appeared in *Journal of Algebra*, **205**(1), (1998), 119-140.

1. Preliminaries

Products of conjugacy classes in a group may be approached from two directions: covering, which is a set-theoretic notion, and mixing, which is related to distributions on the group.

Let G be a finite nonabelian simple group. For two conjugacy classes $C, D \subseteq G$, the set $CD = \{cd : \ c \in C, \ d \in D\}$ is a union of conjugacy classes. Define powers of classes by $C^1 = C$, $C^{n+1} = CC^n$. It is known [1, 1.1] that for any class $C \subseteq G$ there is a minimal number $\upsilon(C)$ such that $C^\upsilon = G$. A theorem of the form $C^\upsilon = G$ is called a **covering** theorem. Dvir [6] proves that for any class $C \subseteq A_n$ ($n \geq 6$), $\upsilon(C) \leq \frac{n}{2}$.

Since we will state some of the results in S_n and others in A_n, some remarks on the connection between the groups are in order. A conjugacy class C of S_n which is contained in A_n is **nonexceptional** if C is a also a conjugacy class in A_n, and **exceptional** otherwise. In the latter case the class is a union of two conjugacy classes in A_n. Exceptional classes have all cycles of different odd lengths. When we treat powers of a certain class $C \subseteq S_n$, we denote by A_n^* the subgroup A_n if $C \subseteq A_n$, and the complement $S_n - A_n$ otherwise. Thus $C \subseteq A_n^*$.

We now focus on classes with $\upsilon(C)$ small.

Date: December 29, 1996.

The author would like to thank Zvi Arad and Avital Frumkin for some helpful conversations.

The condition $v(C) = 2$ for $C \subset A_n$ was studied in [2]. Sample results are: $v([n]) = v([(\frac{n}{2})^2]) = 2$, $v([3^{n/3}]) > 2$. We will return to these examples later.

Brenner [3] proves the only known criteria for $C^4 = A_n$. Let $\mu(C)$ denote the number of cycles of an element of C.

Theorem 1.1 ([3]). *Let C be a nonexceptional class in A_n ($n \geq 5$). If $n - 2\mu(C) \geq -1$, then $C^4 = A_n$.*

Dvir [6, 9.3] proves that Brenner's condition is actually sufficient for $C^3 = A_n^*$, except for the case $C = [2^{n/2}]$. The third power of all nonexceptional classes with $n - 2\mu(C) \geq -1$ is thus known, except for $C = [2^{n/2}]$. We fill this gap in sections 4-6.

The second approach to products of conjugacy classes is related to the group algebra. For a conjugacy class $C \subseteq G$, denote by $\hat{C}$ the sum of elements of C in the group algebra $\mathbb{C}[G]$. The set $\{\hat{C}\}$ is a standard basis for the center $Cent(\mathbb{C}[G])$, and the multiplication may be computed via Burnside's formula

$$\hat{C}_1\hat{C}_2 = \frac{|C_1||C_2|}{|G|} \sum_{D \subseteq G} \left(\sum_{\chi} \frac{\chi(C_1)\chi(C_2)\chi(D^{-1})}{\chi(1)} \right) \hat{D}, \tag{1}$$

where the outer sum is over all the conjugacy classes and the inner one is over all irreducible characters. Using orthogonality of characters, this formula may be easily generalized to

$$\hat{C}_1 ... \hat{C}_m = \frac{|C_1| ... |C_m|}{|G|} \sum_{D \subseteq G} \left(\sum_{\chi} \frac{\chi(C_1) ... \chi(C_m)\chi(D^{-1})}{\chi(1)^{m-1}} \right) \hat{D}. \tag{2}$$

Questions about covering are concerned only with the non-zero coefficients in (2).

We call $x \in \mathbb{C}[G]$ a **distribution element**, if $x = \sum \alpha_g g$, where $\forall g : \alpha_g \geq 0$ and $\sum_{g \in G} \alpha_g = 1$. A distribution element induces a distribution on G, with $Prob(g) = \alpha_g$. If x,y are two distribution elements, then their product xy is a distribution element, inducing the convolution of the distributions induced by x and y.

The uniform element $U = \frac{1}{|G|} \sum g$ is a distribution element, with the property $Ux = x$ for any $x \in \mathbb{C}[G]$.

The difference $x - y$ is an element in the augmentation ideal $I_G = \{\sum \alpha_g g : \sum \alpha_g = 0\}$. Thus, a norm on I_G may be thought of as a distance measure between distributions.

Definition 1.2 (normalized l^2 norm on G). *For $x = \sum \alpha_g g \in I_G$, define $\|x\|^2 = |G| \cdot \sum \alpha_g^2$.*

Multiplying the standard l^2 norm by $|G|$ has the following reasoning. Suppose x is uniform on a p-portion of the group. Then the distance from the uniform distribution $\|x - U\|^2 = \frac{1-p}{p}$ is independent of $|G|$, as seems suited.

See [4, pp. 24-25] for a short survey on distance measures between distributions.

Fix a conjugacy class C, and consider the process of sampling $c_1, ..., c_\kappa$ from C at random, and computing the product $c_1...c_\kappa$. The resulting distribution is described by the distribution element $(\frac{\hat{C}}{|C|})^\kappa$. A theorem which connects $(\frac{\hat{C}}{|C|})^\kappa$ to the uniform distribution U is called a **mixing** theorem.

It can be seen that $\|(\frac{\hat{C}}{|C|})^\kappa - U\|^2 \to 0$ as $\kappa \to \infty$.

But good mixing can occur even for constant κ. To describe this more accurately, let G_n be a sequence of groups (usually $|G_n| \to \infty$), and Let $C_n \subseteq G_n$ be a sequence of conjugacy classes. (We allow C_n to be classes in supergroups $G'_n \supseteq G_n$, *e.g.* $S_n \supseteq A_n$). We say that κ is the **mixing time** for $\{C_n\}$ if it is minimal for $\|(\frac{\hat{C}_n}{|C_n|})^\kappa - U_n\| \to 0$ as $n \to \infty$. A typical sequence would be $G_n = A_n$, and C_n some conjugacy class of S_n defined by a generic rule. For example, the classes of transpositions $C_n = [2, 1^{n-2}]$ were studied in depth by Diaconis and Shahshahani [5]. The mixing time of classes sequences is known in only a few cases. See [8, chap. 2] for details.

Lulov, in [8], considers the classes $[r^{n/r}]$, and proves that the mixing time for this sequence of classes is $\kappa = 2$ for $r \geq 3$, and $\kappa = 3$ for $r = 2$.

The theme of this paper is a comparison between covering and mixing theorems for sequences of classes. If a random process (such as multiplying elements sampled from a conjugacy class) can reach any element of the group, we may wonder if the process is uniform. On the other hand, it is interesting to understand almost-uniform distributions with probability-zero elements.

We can compare Lulov's mixing results to what is known about covering properties of the classes $[r^{n/r}]$. Note that the size of these classes is increasing with r, so it is natural to expect $\upsilon_r = \upsilon([r^{n/r}])$ and κ_r, the mixing time of $[r^{n/r}]$, to decrease with r. According to [8] and [2], we have:

$$\upsilon_2 = 4, \upsilon_3 > 2, \upsilon_4 = \upsilon_{\frac{n}{2}} = \upsilon_n = 2$$

$$\kappa_2 = 3, \kappa_3 = \kappa_4 = ... = \kappa_n = 2$$

Conjecture 1.3. *$\upsilon_3 = 3$, $\upsilon_5 = \upsilon_6 = ... = \upsilon_{\frac{n}{3}} = 2$*

This paper is organized as follows. In section 2 we give an example of a sequence of products with the covering property, but with no mixing. In section 3 we compute $\widehat{[2^{n/2}]}^2$, deriving some new character identities. We consider the behavior of the cycles number under this distribution, and compare it to the cycles number under the uniform distribution. We also reprove that $[2^{n/2}]^4 = A_n$. In sections 4–6 we describe the classes contained in $[2^{n/2}]^3$: In section 4 we show that almost all classes are contained in $[2^{n/2}]^3$, using technical lemmas that are proved in section 5. In section 6 we show that the classes omitted in section 4 are indeed not contained in $[2^{n/2}]^3$. Chapter 7 is devoted to graph-theoretic applications.

2. Covering without mixing

Sequences of classes which have no finite mixing time are easy to find. For example, this is the case with bounded-support sequences, such as $C_n = [2, 1^{n-2}]$. But this type of non-mixing is easily explained by the fact that bounded-support sequences cannot cover either (since for large n almost all points do not move).

In this section we give an example with best cover but worst mix. More precisely, we present a sequence $\{C_n\}$ of classes all with $\upsilon(C_n) = 2$, such that $\|(\frac{\hat{C}_n}{|C_n|})^\kappa - U\| \not\to 0$ for any κ.

If $x = \sum_g \alpha_g g$ is a distribution element, then $\chi(x) = \sum_g \alpha_g \chi(g)$ may be thought of as the expectation of $\chi(g)$ where g's distribution is determined by x. We start with a general result connecting the norm on I_G to expectancies of the irreducible characters. This result could be derived from the Plancharel identity too. Recall the basic orthogonality relations,

$$\sum_{C \subset G} |C| \psi_1(C) \psi_2(C) = |G| \delta_{\psi_1, \psi_2} \tag{3}$$

$$\sum_{\chi} \chi(C) \chi(D^{-1}) = \frac{|G|}{|C|} \delta_{C,D} \tag{4}$$

By $\chi(C)$ we mean $\chi(c)$ for any $c \in C$.

Theorem 2.1. *Let x be a central distribution element on a group G. Then*

$$\|x - U\|^2 = \sum_{\chi \neq 1} |\chi(x)|^2.$$

Proof. Write $x = \sum_C \alpha_C \hat{C}$. By (4),

$$\sum_\chi \chi(x)\chi(D^{-1}) = \sum_C |C|\alpha_C \sum_\chi \chi(C)\chi(D^{-1}) = |G|\alpha_D,$$

so $\alpha_D = \frac{1}{|G|}\sum_\chi \chi(x)\chi(D^{-1})$. Now compute

$$\|x\|^2 = |G|\sum_C |C|\alpha_C^2 = \frac{1}{|G|}\sum_{\psi_1,\psi_2} \psi_1(x)\psi_2(x)\sum_C \psi_1(C^{-1})\psi_2(C^{-1}) =$$

$$= \sum_{\psi_1,\psi_2} \psi_1(x)\psi_2(x)\delta_{\overline{\psi_1},\psi_2} = \sum_\chi |\chi(x)|^2.$$

□

Corollary 2.2. *If $\|x - U\| \to 0$, then $\chi(x) \to 0$ for all $\chi \neq 1$.*

Consider the process of multiplying random elements sampled from the classes $C_1, ..., C_\kappa$. We now compute $\chi(p)$ for the corresponding distribution element p.

Theorem 2.3. *Let $C_1, ..., C_\kappa$ be conjugacy classes, χ an irreducible character. Then*

$$\chi\left(\frac{\hat{C}_1\hat{C}_2...\hat{C}_\kappa}{|C_1||C_2|...|C_\kappa|}\right) = \frac{\chi(C_1)\chi(C_2)...\chi(C_\kappa)}{\chi(1)^{\kappa-1}}$$

Proof.

$$\begin{aligned}\chi\left(\frac{\hat{C}_1\hat{C}_2...\hat{C}_\kappa}{|C_1||C_2|...|C_\kappa|}\right) &= \chi\left(\frac{1}{|G|}\sum_D\sum_\psi \frac{\psi(C_1)...\psi(C_\kappa)\psi(D^{-1})}{\psi(1)^{\kappa-1}}\hat{D}\right)\\ &= \frac{1}{|G|}\sum_\psi \frac{\psi(C_1)...\psi(C_\kappa)}{\psi(1)^{\kappa-1}}\sum_D |D|\psi(D^{-1})\chi(D)\\ &= \frac{\chi(C_1)...\chi(C_\kappa)}{\chi(1)^{\kappa-1}}.\end{aligned}$$

□

Note the case $\kappa = 1$, where 2.3 is the obvious $\chi(\frac{\hat{C}}{|C|}) = \chi(C)$.

We apply 2.3 to the symmetric group, with the character χ_0 induced by the standard representation. Recall that $\chi_0(\sigma)$ equals the number of fixed points of σ, minus 1.

Theorem 2.4. *Let $\{C_n \subset S_n\}$. If $\{C_n\}$ has a finite mixing time, then $\frac{\chi_0(C_n)}{n^{1-\epsilon}} \to 0$ for some $\epsilon > 0$.*

In particular, if $\chi_0(C_n) \geq \delta n$ for some $\delta > 0$, then $\{C_n\}$ has no finite mixing time.

Proof. Let κ be the mixing time for $\{C_n\}$, that is, $\|(\frac{\hat{C}_n}{|C_n|})^\kappa - U_n\| \to 0$, and take $\epsilon = \frac{1}{\kappa}$. Using 2.2 and 2.3 we have

$$\frac{\chi_0(C_n)}{\chi_0(1)^{1-\epsilon}} = \sqrt[\kappa]{\frac{\chi_0(C_n)^\kappa}{\chi_0(1)^{\kappa-1}}} = \sqrt[\kappa]{\chi_0\left((\frac{\hat{C}_n}{|C_n|})^\kappa\right)} \to 0.$$

□

A similar lower bound for the mixing time in the variation norm $\|\sum_g \alpha_g g\|_1 = sup_{A\subseteq G}|\sum_{g\in A}\alpha_g|$ was obtained in [10, 3.1], where character bounds are used to give an upper bound for the mixing time as well.

Note that by the "upper bound lemma" of [5], $\|x\|_1 \leq \|x\|$.

As for the promised covering-but-not-mixing sequence, take $C_n = [3^n, 1^n] \subset A_{4n}$.

By [2, 6.12] $C_n^2 = A_{4n}$, while by 2.4 C_n has no finite mixing.

3. The second and forth powers of $[2^{n/2}]$

In this section we compute $\widehat{[2^{n/2}]}^2$ and $[2^{n/2}]^4$. We assume throughout that *n is an even number.*

To get some feeling of the size of $[2^{n/2}]$ we start with a numerical fact.

Remark 3.1. $|[2^{n/2}]| = \frac{n!}{2^{\frac{n}{2}}(\frac{n}{2})!}$, *so* $\frac{|[2^{n/2}]|^2}{|S_n|} = 2^{-n}\binom{n}{n/2} \approx \sqrt{\frac{2}{\pi n}}$.

If $\lambda = [1^{a_1}, 2^{a_2}, ...] \subseteq S_{\frac{n}{2}}$ is a conjugacy class, denote by $2\lambda = [1^{2a_1}, 2^{2a_2}, ...] \subseteq S_n$ the "double" conjugacy class.

Theorem 3.2. $[2^{n/2}]^2$ *equals the union of classes of the form* 2λ, $\lambda \subseteq S_{\frac{n}{2}}$.

We actually prove a more exact statement. Recall that $Cent_G(C)$ is the centralizer of an element from C in the group G. The choice of element is irrelevant for the size of the centralizer.

Theorem 3.3. $\widehat{[2^{n/2}]}^2 = \sum_{\lambda\subseteq S_{n/2}} 2^{-\mu(\lambda)} \frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|}\widehat{2\lambda}$.

Proof. Denote $C = [2^{n/2}]$. Let $\mathcal{G}_2$ denote the collection of all (loopless) 2-colored 2-regular graphs on n points. Name the two colors "red" and "blue". We establish one correspondence between $C \times C$ and $\mathcal{G}_2$, and another between $\mathcal{G}_2$ and the union of the classes 2λ of S_n, $\lambda \subseteq S_{\frac{n}{2}}$.

Let $\sigma_1, \sigma_2 \in [2^{n/2}]$. Construct a 2-colored graph on n points, by connecting the couples $i, \sigma_1(i)$ with red edges, and the couples $i, \sigma_2(i)$ with blue edges. The resulting graph is 2-regular since vertex i is connected only to the two vertices $\sigma_1(i)$,$\sigma_2(i)$. Obviously this map $C \times C \to \mathcal{G}_2$ is bijective.

Now define a map from $\mathcal{G}_2$ to $\bigcup(2\lambda)$, as follows. Let $g \in \mathcal{G}_2$ be a graph. Clearly g is the union of even-length cycles. Map g to the product $\sigma_1\sigma_2$ for the corresponding $(\sigma_1, \sigma_2) \in C \times C$. Fix a cycle of length $2m$, and number the points from 0 to $2m-1$, such that $0 \leftrightarrow 1$ is a blue edge. Then $\sigma_1\sigma_2$ shifts $k \mapsto k+2$ for even k, and $k \mapsto k-2$ for odd k. As a permutation, it has two cycles of length m in the action on $\{0, ..., 2m-1\}$. This is true for any cycle of g, so $\sigma_1\sigma_2 \in 2\lambda$ for some $\lambda \subseteq S_{\frac{n}{2}}$. This proves $\widehat{[2^{n/2}]}^2 = \sum_{\lambda \subseteq S_{\frac{n}{2}}} \alpha_\lambda \widehat{2\lambda}$ (which is theorem 3.2).

To compute the coefficients, fix some $\sigma \in 2\lambda = [n_1^{2\alpha_1}, ..., n_t^{2\alpha_t}]$. We count the graphs $g \in \mathcal{G}_2$ that correspond to σ. For any i, the $2\alpha_i$ cycles of length n_i of σ can be coupled in $\frac{(2\alpha_i)!}{2^{\alpha_i}\alpha_i!}$ ways. In any couple, the two cycles may be attached in n_i ways, and this attachment determines a cycle of length $2n_i$ in a graph. Multiplying the numbers of ways to get graphs we get $\prod_{i=1}^{t} \frac{(2\alpha_i)!}{2^{\alpha_i}\alpha_i!} n_i^{\alpha_i}$, which is the number of ways $\sigma \in 2\lambda$ can be expressed as a multiplication $\sigma_1\sigma_2$, $\sigma_1, \sigma_2 \in [2^{n/2}]$. So this is the coefficient of $\widehat{2\lambda}$.

To finish we note that $|Cent_{S_n}(2\lambda)| = \prod(2\alpha_i)! n_i^{2\alpha_i}$ and $|Cent_{S_{\frac{n}{2}}}(\lambda)| = \prod \alpha_i! n_i^{\alpha_i}$, so $2^{-\mu(\lambda)} \frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|} = 2^{-\sum \alpha_i} \frac{\prod(2\alpha_i)! n_i^{2\alpha_i}}{\prod \alpha_i! n_i^{\alpha_i}} = \prod \frac{(2\alpha_i)!}{2^{\alpha_i}\alpha_i!} n_i^{\alpha_i}$. □

Example 3.4. *We demonstrate the theorem in the case $n = 8$. $S_{\frac{n}{2}} = S_4$ has the five classes $[4], [3,1], [2^2], [2,1^2], [1^4]$, and*

$$\begin{aligned}
\widehat{[2^4]}^2 &= \frac{1}{2}\frac{|Cent_{S_8}([4^2])|}{|Cent_{S_4}([4])|}\widehat{[4^2]} + \frac{1}{4}\frac{|Cent_{S_8}([3^2,1^2])|}{|Cent_{S_4}([3,1])|}\widehat{[3^2,1^2]} + \\
&+ \frac{1}{4}\frac{|Cent_{S_8}([2^4])|}{|Cent_{S_4}([2^2])|}\widehat{[2^4]} + \frac{1}{8}\frac{|Cent_{S_8}([2^2,1^4])|}{|Cent_{S_4}([2,1^2])|}\widehat{[2^2,1^4]} + \\
&+ \frac{1}{16}\frac{|Cent_{S_8}([1^8])|}{|Cent_{S_4}([1^4])|}\widehat{[1^8]} = \\
&= 4\widehat{[4^2]} + 3\widehat{[3^2,1^2]} + 12\widehat{[2^4]} + 6\widehat{[2^2,1^4]} + 105\widehat{[1^8]}.
\end{aligned}$$

Counting elements in both sides of the equation in theorem 3.3, we get the following nice result.

Corollary 3.5. $\sum_{\lambda \subseteq S_n} 2^{-\mu(\lambda)}|\lambda| = \frac{(2n)!}{2^{2n}n!}$.

Proof. For convenience, we prove this identity for $\frac{n}{2}$ instead of n. Using $|Cent_G(C)| = \frac{|G|}{|C|}$ for $G = S_n$ and for $G = S_{\frac{n}{2}}$ we get

$$\begin{aligned}\frac{n!^2}{2^n(\frac{n}{2})!^2} &= |[2^{n/2}]|^2 = \sum_{\lambda\subseteq S_{n/2}} 2^{-\mu(\lambda)}\frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|}|2\lambda| = \\ &= \sum_{\lambda\subseteq S_{n/2}} 2^{-\mu(\lambda)}\frac{n!/|2\lambda|}{(\frac{n}{2})!/|\lambda|}|2\lambda| = \frac{n!}{(\frac{n}{2})!}\sum_{\lambda\subseteq S_{n/2}} 2^{-\mu(\lambda)}|\lambda|.\end{aligned}$$

□

This last corollary, as well as the obvious $\sum_{\lambda\subseteq S_n}|\lambda| = n!$, are the instances $\alpha = \frac{1}{2}$ and $\alpha = 1$ of the following.

Proposition 3.6 ([9, 4.3(8)])**.** *For any α,*
$\sum_{\lambda\subseteq S_n}\alpha^{\mu(\lambda)}|\lambda| = \sum_{\sigma\in S_n}\alpha^{\mu(\sigma)} = \alpha(\alpha+1)(\alpha+2)...(\alpha+(n-1))$.

Comparing theorem 3.3 to Burnside's formula produces an interesting character identity. The coefficient of $\widehat{2\lambda}$ in $\widehat{[2^{n/2}]}^2$, which is by Burnside $\frac{|[2^{n/2}]|^2}{|S_n|}\sum_\chi \frac{\chi([2^{n/2}])^2\chi(2\lambda)}{\chi([1^n])}$, was computed in theorem 3.3. We get

Corollary 3.7. *For any class $\lambda \subseteq S_{\frac{n}{2}}$,*

$$\sum_\chi \frac{\chi([2^{n/2}])^2\chi(2\lambda)}{\chi([1^n])} = 2^{n-\mu(\lambda)}\frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|}\frac{1}{\binom{n}{n/2}}.$$

Example 3.8.

- *Take $\lambda = [\frac{n}{2}]$, the class of maximal length cycles in $S_{\frac{n}{2}}$. Then $\sum_\chi \frac{\chi([2^{n/2}])^2\chi([(\frac{n}{2})^2])}{\chi([1^n])} = \frac{2^{n-1}n}{\binom{n}{n/2}}$.*
- *Assume $\frac{n}{2}$ is even, and take $\lambda = [2^{n/4}] \subseteq S_{\frac{n}{2}}$. Then $2\lambda = [2^{n/2}]$ and $\sum_\chi \frac{\chi([2^{n/2}])^3}{\chi([1^n])} = 2^n\frac{\binom{n/2}{n/4}}{\binom{n}{n/2}}(\frac{n}{4})!$. For example, $\sum_\chi \frac{\chi([2^4])^3}{\chi([1^8])} = 2^8\frac{\binom{4}{2}}{\binom{8}{4}}2! = \frac{3\cdot 2^9}{5\cdot 7}$. If $\frac{n}{2}$ if odd, then $[2^{n/2}]$ is an odd class and $\sum_\chi(\frac{\chi([2^{n/2}])^3}{\chi([1^n])}) = 0$*

A hook formula for $|\chi([2^{n/2}])|$, for any character χ (and more generally for $|\chi([r^{n/r}])|$ for any r dividing n), was recently given by Fomin

and Lulov [7]. They also give the bound $|\chi([2^{n/2}])| < c \cdot n^{\frac{1}{4}}\sqrt{\chi([1^n])}$ for $c = (\frac{\pi}{2})^{1/4} + \xi$.

Let U be the uniform distribution on S_n, and denote $e_n(\alpha) = E_U(\alpha^{\mu(\sigma)})$, the expectancy of $\alpha^{\mu(\sigma)}$ where σ is uniformly distributed.

Theorem 3.6 is equivalent to the statement $e_n(\alpha) = \binom{\alpha+n-1}{n}$.

Using 3.3 we can give a similar result for the distribution p^2, where $p = \frac{\widehat{[2^{n/2}]}}{|[2^{n/2}]|}$ is the uniform distribution on $[2^{n/2}]$.

Proposition 3.9. $E_{p^2}(\alpha^{\mu(\sigma)}) = 2^n(\frac{n}{2})!e_{\frac{n}{2}}(\frac{\alpha^2}{2})$.

Proof. If $q = \sum \alpha_\sigma \sigma$ is a distribution element and f is a function defined on the group, then the expectancy $E_q(f)$ is $\sum \alpha_\sigma f(\sigma)$. If $q = \sum \alpha_\lambda \hat{\lambda}$ is uniform on conjugacy classes and f is a class function, then $E_q(f) = \sum \alpha_\lambda |\lambda| f(\lambda)$. By theorem 3.3

$$p^2 = \frac{\widehat{[2^{n/2}]}^2}{|[2^{n/2}]|^2} = \frac{1}{|[2^{n/2}]|^2} \sum_{\lambda \subseteq S_{\frac{n}{2}}} 2^{-\mu(\lambda)} \frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|} \widehat{2\lambda}$$

so, as in the proof of corollary 3.5,

$$\begin{aligned} E_{p^2}(\alpha^{\mu(\sigma)}) &= \frac{1}{|[2^{n/2}]|^2} \sum_{\lambda \subseteq S_{n/2}} 2^{-\mu(\lambda)} \frac{|Cent_{S_n}(2\lambda)|}{|Cent_{S_{n/2}}(\lambda)|} \cdot |2\lambda| \alpha^{2\mu(\lambda)} = \\ &= \frac{2^n(\frac{n}{2})!}{n!} \sum_{\lambda \subseteq S_{n/2}} |\lambda| (\frac{\alpha^2}{2})^{\mu(\lambda)} = 2^n \left(\frac{n}{2}\right)! e_{\frac{n}{2}} \left(\frac{\alpha^2}{2}\right). \end{aligned}$$

□

Expectancy over p^2 can be used to give another proof for Lulov's result [8, 6.2], that the mixing time of $[2^{n/2}]$ is greater than 2: $E_{p^2}((-1)^{\mu(\sigma)}) = 1$, while $E_U((-1)^{\mu(\sigma)}) = 0$. (This is also obvious from 3.1).

A related result is the following ([2, 5.02]): Let $C \subset A_m$. Then for large enough n, $v(C \oplus [2^n]) > 2$.

We end this section with

Theorem 3.10. $[2^{n/2}]^4 = A_n$.

Proof. Denote by N the set on which A_n acts. Let $\sigma \in A_n$, then σ must have an even number of cycles of even length. Likewise, since n is even, the number of odd-length cycles is also even. It follows that one can write $N = N_1 \cup ... \cup N_t$, a disjoint partition, with $|N_i|$ even and σ restricted to n_i the product of two cycles.

We show that $\sigma' = (x_1 \ ... \ x_k)(y_{k+1} \ ... \ y_{2m}) \in [2^m]^4$. Indeed,

$$(x_1 y_{k+1})(y_m y_{2m}) \cdot (x_1 x_2 ... x_k y_{k+1} ... y_{m-1} y_{2m})(y_m y_{m+1} ... y_{2m-1}) =$$

$$= (y_{k+1} ... y_{m-1} y_m y_{m+1} ... y_{2m})(x_1 ... x_k) = \sigma',$$

the permutations we used belong to $[2^2, 1^{2m-4}], [m^2] \subseteq [2^m]^2$.
With this we finish the proof, since $[2^m] \oplus [2^{m'}] \subseteq [2^{m+m'}]$. □

Note that 3.10 is a special case of Brenner's theorem mentioned in the introduction.

4. $[2^{n/2}]^3$

Let $\mathcal{S}$ denote the collection of all conjugacy classes in all the symmetric groups S_n. Define a **direct sum** operation on $\mathcal{S}$ by $[1^{a_1}, ..., k^{a_k}] \oplus [1^{b_1}, ..., k^{b_k}] = [1^{a_1+b_1}, ..., k^{a_k+b_k}]$. Under this operation $\mathcal{S}$ becomes an ($\mathbb{N}$-graded) semigroup with cancellation. We define a **division** relation, $C|D$ iff there exist $E \in \mathcal{S}$ such that $D = C \oplus E$. This (unique) E is denoted $C^{-1}D$.

From now on A_n^* is the coset of A_n in S_n that contains $[2^{n/2}]$.

We mark some important subsets of $\mathcal{S}$. Write $\mathcal{A}^*$ for the collection of classes in all A_n^*, even n, and $\mathcal{F}$ for the union of all $[2^{n/2}]^3$. Note that $\mathcal{F} \subseteq \mathcal{A}^*$ are subsemigroups of $\mathcal{S}$.

Denote by $\mathcal{E}$ the collection of classes

$$\mathcal{E} = \{[3^5, 1], [3, 1^{1+4k}], [4, 3, 1^{3+4k}], [5, 1^{3+4k}], [3, 2, 1^{1+4k}], [3, 2^k, 1], [5, 3, 2^k] : k \geq 0\}.$$

It is easy to check that $\mathcal{E} \subseteq \mathcal{A}^*$. Denote by $\mathcal{E}_n$ the set of members of $\mathcal{E}$ which are classes in S_n. Note that $\mathcal{E}_n$ contains 4 classes for $n \geq 8$, $n \neq 16$, while $|\mathcal{E}_{16}| = 5$, $\mathcal{E}_6 = \{[3, 2, 1]\}$, $\mathcal{E}_4 = \{[3, 1]\}$ and $\mathcal{E}_2$ is empty.

We will show $\mathcal{F} = \mathcal{A} - \mathcal{E}$, that is,

Theorem 4.1. *Let n be even, $C \subseteq A_n^*$. Then $C \subseteq [2^{n/2}]^3$ iff $C \notin \mathcal{E}_n$.*

In this section we prove that $\mathcal{A} - \mathcal{E} \subseteq \mathcal{F}$.

We now introduce a certain equivalence relation on the set of natural numbers. This relation induces an epimorphism from $\mathcal{S}$ to a semigroup $\hat{\mathcal{S}}$, which will be useful in the sequel.

Denote $\Pi = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}, \hat{7}, \hat{9}\}$, where $\hat{1} = \{1\}$, $\hat{2} = \{2\}$, $\hat{3} = \{3\}$, $\hat{4} = \{k \equiv 4 \pmod 4 : k \geq 4\}$, $\hat{5} = \{5\}$, $\hat{6} = \{k \equiv 6 \pmod 4 : k \geq 6\}$, $\hat{7} = \{k \equiv 7 \pmod 4 : k \geq 7\}$, $\hat{9} = \{k \equiv 9 \pmod 4 : k \geq 9\}$. Π is a partition of $\mathbb{N}$.

We use the standard notation for conjugacy classes of S_n, with members of Π instead of numbers. If $a_1, ..., a_t \in \Pi$, $[a_1, ..., a_t] = \{[n_1, ..., n_t] :$

$n_i \in a_i\}$. If P is such set of classes, write $n_x = n_x(P)$ for the number of appearances of $\hat{x}$ in P. Of course, the numbers $n_x(P)$ determine P.

Denote by $\hat{\mathcal{S}}$ the collection of classes $[a_1, ..., a_t]$, $a_i \in \Pi$. $\hat{\mathcal{S}}$ is a partition of $\mathcal{S}$, and the map from $C \in \mathcal{S}$ to the corresponding class in $\hat{\mathcal{S}}$ is a semigroup epimorphism. $\hat{\mathcal{S}}$ is a semigroup with cancellation too, and the division relation may be defined on $\hat{\mathcal{S}}$ as well.

Let $P \in \hat{\mathcal{S}}$. Then

$$n_1 + n_3 + n_5 + n_7 + n_9 \equiv 0 \pmod 2 \tag{5}$$

since classes in P act on an even number of points, and

$$(n_1 + n_5 + n_9) - (n_3 + n_7) \equiv 2n_4 \pmod 4 \tag{6}$$

since a class $C \in P$, $C \subset A_n^*$, have the same sign as $[2^{n/2}]$.

In section 5 we prove several results of the form "$P \subseteq \mathcal{F}$" for $P \in \hat{\mathcal{S}}$. We use these results to prove the following lemmas.

Lemma 4.2. *Let $P \in \hat{\mathcal{S}}$, and assume $n_3(P)$ is odd. Then one of the following holds.*

(a) There exist $P_0|P$, $P_0 \subseteq \mathcal{F}$, such that $n_3(P_0^{-1}P)$ is even, and, moreover, $P_0^{-1}P \neq [\hat{5}, \hat{1}^m]$ $(m \geq 1)$, **or**

(b) $n_6 = n_7 = n_9 = 0$, and also $n_1 + n_5 = 1$ or $n_3 = 1$.

Proof. First assume $n_6 + n_7 + n_9 > 0$.

- $n_9 > 0$:
  - $P = [\hat{9}, \hat{5}, \hat{3}, \hat{1}^m]$, $m \geq 1$: $m \geq 3$ by (6), so take $P_0 = [\hat{9}, \hat{5}, \hat{3}, \hat{1}^3]$ $(\in \mathcal{F}$ by 5.9).
  - Otherwise: Take $P_0 = [\hat{9}, \hat{3}]$ (by 5.4).
- $n_9 = 0, n_7 > 0$:
  - $n_1, n_5 \geq 1$:
    - $P = [\hat{7}, \hat{5}^2, \hat{3}, \hat{1}^m]$, $m \geq 2$: Take $P_0 = [\hat{7}, \hat{3}, \hat{1}^2]$ (5.9).
    - Otherwise: Take $P_0 = [\hat{7}, \hat{5}, \hat{3}, \hat{1}]$ (5.9).
  - $n_5 = 0$ or $n_1 = 0$:
    - $n_4 > 0$: Take $P_0 = [\hat{7}, \hat{4}, \hat{3}]$ (5.6).
    - $n_4 = 0$:
      - $n_1 + n_5 \geq 2$: Take P_0 one of $[\hat{7}, \hat{5}^2, \hat{3}]$,$[\hat{7}, \hat{3}, \hat{1}^2]$ (5.9).
      - Otherwise: by (6), $n_3 + n_7 \geq 4$, and n_3 is odd by assumption. Take P_0 one of $[\hat{7}, \hat{3}^3]$ or $P_0 = [\hat{7}^3, \hat{3}]$ (5.5).
- $n_7 = n_9 = 0, n_6 > 0$:
  - $n_5 = 1$ or $n_1 = 0$: $n_1 + n_5$ is odd by (6), so in any case $P_0 = [\hat{6}, \hat{5}, \hat{3}]$ divides P. $P_0 \in \mathcal{F}$ by 5.9.

– Otherwise: Take $P_0 = [\hat{6}, \hat{3}, \hat{1}]$ (5.9).

We may now assume $n_6 = n_7 = n_9 = 0$. Assume (b) does not hold, that is $n_3 \geq 3$ and $n_1 + n_5 \geq 3$.

- $n_5 \leq 3$: take $P_0 = [\hat{5}^{n_5}, \hat{3}^3, \hat{1}^{3-n_5}]$ (5.10).
- $n_5 = 4$: $n_1 \geq 1$ (since $n_1 + n_5$ is odd), so take $P_0 = [\hat{5}^2, \hat{3}^3, \hat{1}]$ (5.10).
- $n_5 > 4$: take $P_0 = [\hat{5}^3, \hat{3}^3]$ (5.10).

□

Lemma 4.3. *Assume $P \neq [5, 1^m]$ ($m \geq 1$), and $n_3(P)$ is even. If $n_5(P)$ is odd, than there exist $P_0|P$, $P_0 \subseteq \mathcal{F}$, such that $n_3(P_0^{-1}P)$ and $n_5(P_0^{-1}P)$ are both even.*

Proof. Separate to cases.

- $n_7 > 0$: Take $P_0 = [\hat{7}, \hat{5}] (\in \mathcal{F}$ by 5.4). We may now assume $n_7 = 0$, so $n_1 + n_9$ is odd.
- $n_3 > 0$: Then $n_3 \geq 2$, so take $P_0 = [\hat{5}, \hat{3}^2, \hat{1}]$ (5.10) or $P_0 = [\hat{9}, \hat{5}, \hat{3}^2]$ (5.9). Assume $n_3 = 0$.
- $n_5 \geq 3$: Take $P_0 = [\hat{5}^3, \hat{1}]$ or $P_0 = [\hat{9}, \hat{5}^3]$ (by 5.5). Assume $n_5 = 1$.
- $n_4 > 0$: Take $P_0 = [\hat{5}, \hat{4}, \hat{1}]$ or $P_0 = [\hat{9}, \hat{5}, \hat{4}]$ (5.6). Assume $n_4 = 0$.
- $n_9 > 0$: By (6) $n_1 + n_9 \geq 3$, so take $P_0 = [\hat{9}, \hat{5}, \hat{1}^2]$, $P_0 = [\hat{9}^2, \hat{5}, \hat{1}]$ or $P_0 = [\hat{9}^3, \hat{5}]$ (5.5). Assume $n_9 = 0$.

Since $P \neq [\hat{5}, \hat{1}^m]$, $n_2 + n_6 > 0$, so take $P_0 = [\hat{5}, \hat{2}, \hat{1}^3]$ (5.10) or $P_0 = [\hat{6}, \hat{5}, \hat{1}^3]$ (5.9). □

Lemma 4.4. *Assume $n_3(P)$ and $n_5(P)$ are even. Then $P \subseteq \mathcal{F}$.*

Proof. We show that there exist $P_0|P$ such that $P_0 \subseteq \mathcal{F}$, and $n_3(P_0^{-1}P)$, $n_5(P_0^{-1}P)$ are even. The proof is then finished by induction on $n_1 + \ldots + n_9$.

Assume, on the contrary, that no such P_0 exist. Then each of the following holds.

- n_7 is even, for if n_7 is odd than by (5) $n_1 + n_9$ is also odd, so take $P_0 = [\hat{7}, \hat{1}]$ or $P_0 = [\hat{9}, \hat{7}]$ (5.4).
  By (5) $n_1 + n_9$ must now be even too.
- $n_1 + n_5 + n_9 \leq 2$, by 5.5 and the assumption that n_5 is even.
- $n_3 + n_7 \leq 2$, by 5.5.
- $n_2 = n_6 = 0$ by 5.2.
- $n_4 \leq 1$ by taking $P_0 = [\hat{4}^2]$ (5.3).

- $n_4 = 0$, for if $n_4 = 1$ then by (6) exactly one of $n_1 + n_5 + n_9$ and $n_3 + n_7$ equals 2; by 5.6 one may take P_0 one of $[\hat{4}, \hat{1}^2]$, $[\hat{9}, \hat{4}, \hat{1}]$, $[\hat{9}^2, \hat{4}]$, $[\hat{5}^2, \hat{4}]$, $[\hat{4}, \hat{3}^2]$, $[\hat{7}^2, \hat{4}]$.

So far we see that $n_1 + n_5 + n_9 = n_3 + n_7 \leq 2$. Note that $n_1 + n_5 + n_9$, $n_3 + n_7$ are both even.

Suppose $n_1 + n_5 + n_9 = n_3 + n_7 = 2$. Then P is one of $[\hat{9}^2, \hat{7}^2]$, $[\hat{9}^2, \hat{3}^2]$, $[\hat{7}^2, \hat{5}^2]$, $[\hat{7}^2, \hat{1}^2]$, $[\hat{9}, \hat{7}^2, \hat{1}]$ (in $\mathcal{F}$ by 5.4), $[\hat{3}^2, \hat{1}^2]$, $[\hat{5}^2, \hat{3}^2]$ (5.10), or $[\hat{9}, \hat{3}^2, \hat{1}]$ (5.9). □

Proof of theorem 4.1, the $\mathcal{A} - \mathcal{E} \subseteq \mathcal{F}$ part. We may assume $P \neq [5, 1^m]$. If n_3 is odd and the condition 4.2(a) is satisfied, or n_3 is even, then by lemmas 4.2-4.4 P can be decomposed as a direct sum $P = P_0 \oplus P_1 \oplus P_2$ with $P_0, P_1, P_2 \in \mathcal{F}$, and we are done.

Now assume n_3 is odd and 4.2(b) holds. In any of the following cases we find $P_0 | P$ such that $P_0^{-1} P$ does not have this property, so we are again in the first case.

- $n_4 \geq 2$. Then take $P_0 = [\hat{5}, \hat{4}^2, \hat{3}]$ or $P_0 = [\hat{4}^2, \hat{3}, \hat{1}]$ (5.8).
- $n_4 = 1$, By (6) $n_1 + n_5 \equiv n_3 + 2 \pmod 4$. Recall that by assumption $n_3 = 1$ or $n_1 + n_5 = 1$.
  - $n_5 > 0$: take P_0 one of $[\hat{5}, \hat{4}, \hat{3}, \hat{1}^2]$,$[\hat{5}^2, \hat{4}, \hat{3}, \hat{1}]$, $[\hat{5}^3, \hat{4}, \hat{3}]$ or $[\hat{5}, \hat{4}, \hat{3}^3]$ (5.7).
  - $n_5 = 0$:
    - $n_3 = 1$ and $n_1 \equiv 3 \pmod 4$: If $n_2 \geq 1$ take $P_0 = [\hat{4}, \hat{3}, \hat{2}, \hat{1}^3]$ (by 5.7. the case $n_2 = 0$ is in $\mathcal{E}$).
    - $n_1 = 1$ and $n_3 \equiv 3 \pmod 4$: Take $P_0 = [\hat{4}, \hat{3}^3, \hat{1}]$ (5.7).
- $n_4 = 0$. By (6) $n_1 + n_5 \equiv n_3 \pmod 4$, and by assumption $n_3 = 1$ or $n_1 + n_5 = 1$.
  - $n_3 = 1$: The cases $n_1 + n_5 = 1$ are in $\mathcal{E}$, so assume $n_1 + n_5 \geq 5$.
    - $n_5 > 0$: Take P_0 one of $[\hat{5}^5, \hat{3}]$, $[\hat{5}^4, \hat{3}, \hat{1}]$, $[\hat{5}^3, \hat{3}, \hat{1}^2]$, $[\hat{5}^2, \hat{3}, \hat{1}^3]$, $[\hat{5}, \hat{3}, \hat{1}^4]$ (5.10).
    - $n_5 = 0$: necessarily $n_1 \geq 5$, so take $P_0 = [\hat{3}, \hat{2}^2, \hat{1}^5]$ (by 5.10), unless $n_2 = 0, 1$, cases which are in $\mathcal{E}$.

    The cases $n_1 + n_5 = n_3 = 1$ are in $\mathcal{E}$, so we assume $n_3 \geq 5$.
  - $n_1 = 0, n_5 = 1$. Take $P_0 = [\hat{5}, \hat{3}^5]$ (5.10).
  - $n_1 = 1, n_5 = 0$.
    - $n_2 > 0$: Take $P_0 = [\hat{3}^5, \hat{2}, \hat{1}]$ (5.10).
    - $n_2 = 0$: If $n_3 \geq 9$ take $P_0 = [\hat{3}^9, \hat{1}]$ (by 5.10. $n_3 = 5$ is in $\mathcal{E}$).

□

5. Computations in $[2^{n/2}]^3$

In this section we provide the list of classes in $\mathcal{F}$ used in the proof of lemmas 4.2-4.4.

We deal with collections $P \in \hat{\mathcal{S}}$, where we should prove $P \subset \mathcal{F}$. Sometimes we prove more than that: let $\mathcal{F}_0$ be the union of all $[2^{n/2}] \cdot [(\frac{n}{2})^2]$. By 3.2, $\mathcal{F}_0 \subseteq \mathcal{F}$, and some of the claims in this section are of the form $P \subset \mathcal{F}_0$.

Permutations are multiplied from the left (like composition of functions).

If σ acts on a set containing a letter x, write $l_\sigma(x)$ for the length of the cycle in σ containing x.

Insertion lemma 5.1. *Let $\tau \in [2^{n/2}]$, $\sigma \in [(\frac{n}{2})^2]$, so that $\pi = \tau\cdot\sigma \in \mathcal{F}_0$ by definition.*

Let $[a_1, a_2, \dots, a_k]$ be the class containing π.

a. If the cycle of length a_1 is not contained in one cycle of σ, then for any m, $[a_1 + 4m, a_2, \dots, a_k] \subset \mathcal{F}_0$.

b. If the cycles of length a_1, a_2 are not contained both in the same cycle of σ, then for any m, $[a_1 + 2m, a_2 + 2m, a_3, \dots, a_k] \subset \mathcal{F}_0$.

Proof. Write $\sigma = (\dots AB \dots)(\dots CD \dots)$, so

$$\pi : A \mapsto \tau(B),\ C \mapsto \tau(D).$$

Let x, y, z, u be new four letters, and take

$$\tau' = \tau \cdot (xy)(zu),$$
$$\sigma' = (\dots AxzB \dots)(\dots CyuD\ \dots),$$
$$\pi' = \tau' \cdot \sigma'.$$

Then

$$\pi' : A \mapsto y \mapsto z \mapsto \tau(B),\ C \mapsto x \mapsto u \mapsto \tau(D),$$

so π' has the cycle structure of π except for the cycles containing A and B, each one of them now longer by 2 (4 if this is the same cycle).

These new cycles are again not contained in the same cycle of σ (*e.g.* y and z are in the same cycle of π' but not of σ), so the procedure can be carried out m times, as required. □

Using the insertion lemma we can expand any computation of the form $\tau \cdot \sigma = \pi$ to a claim of more general type.

Lemma 5.2. *If $n \equiv 2 \pmod 4$, then $[n] \in \mathcal{F}_0$.*

Proof. Start with $(12) \cdot Id = (12)$. Note that 1 and 2 belong to different cycles of the identity, so by the insertion lemma we get $[2 + 4m] \in \mathcal{F}_0$. □

This is equivalent to $[\hat{2}], [\hat{6}] \subset \mathcal{F}_0$.

Lemma 5.3. *If n, m are even, $n \equiv m \pmod 4$, then $[n, m] \in \mathcal{F}$.*

Proof. $(12)(34) \cdot (13)(24) = (14)(23)$. Insertion lemma on one cycle handles the case $n \equiv m \equiv 2 \pmod 4$, while one insertion on both cycles bring us to the $n \equiv m \equiv 0 \pmod 4$ case. □

This is equivalent to $[\hat{2}^2], [\hat{2}, \hat{6}], [\hat{6}^2], [\hat{4}^2] \subset \mathcal{F}$. The rest of the lemmas can be interpreted in this language as well.

Lemma 5.4. *If n, m are odd, $n \not\equiv m \pmod 4$, and $\{n, m\} \neq \{1, 3\}, \{3, 5\}$, then $[n, m] \in \mathcal{F}$.*

Proof. Assume $n \equiv 1 \pmod 4$, $m \equiv 3 \pmod 4$. If $n \geq 9$, use the insertion lemma with

$$(18)(23)(4A)(59)(6B)(7C) \cdot (13579B)(2468AC) = (1A6)(25B834C97).$$

If $n \leq 5$ then $m \geq 7$ by assumption, so use insertion on

$$(15)(28)(34)(67) \cdot (1357)(2468) = (1784536)(2)$$

or

$$(1C)(29)(37)(45)(6A)(8B) \cdot (13579B)(2468AC) = (12BA8)(394756C).$$

□

Lemma 5.5. *If n_1, n_2, n_3, n_4 are odd, $n_i \equiv n_j \bmod 4$, and $\{n_1, \ldots, n_4\} \neq \{1, 1, 1, 5\}$, then $[n_1, n_2, n_3, n_4] \in \mathcal{F}$.*

Proof. If $n_1, \ldots, n_4 \equiv 3 \pmod 4$, use insertion on cycles of

$$(1A)(28)(3C)(47)(5B)(69) \cdot (13579B)(2468AC) = (1C5)(2A3)(498)(6B7).$$

Assume $n_1, \ldots, n_4 \equiv 1 \pmod 4$, and $n_1 \leq n_2 \leq n_3 \leq n_4$.

- $n_1 = n_2 = n_3 = 1$. By assumption $n_4 \geq 9$, so use

$$(18)(2C)(3B)(46)(5A)(79) \cdot (13579B)(2468AC) = (1A7B5C483)(2)(6)(9).$$

- $1 = n_1 = n_2 < n_3 \leq n_4$. Use insertion on

$$(13)(2C)(45)(67)(89)(AB) \cdot (13579B)(2468AC) = (1569A)(2)(3)(478BC).$$

- $1 = n_1 < n_2 \leq n_3 \leq n_4$. Use insertion on

$$(17)(23)(48)(AC)(5E)(Ba)(9D)(6F) \cdot (13579BDF)(2468ACEa) =$$
$$= (128C5)(3EB9a)(4F7D6)(A).$$

- $5 \leq n_1 \leq n_2 \leq n_3 \leq n_4$. Use insertion twice on the cycles $(2)(3)$ of the case $1 = n_1 = n_2 < n_3 \leq n_4$, and continue from that point.

□

Lemma 5.6. *If n, m are odd, $n \equiv m \pmod 4$, and $k \equiv 0 \pmod 4$, then $[k, n, m] \in \mathcal{F}$.*

Proof. Consider

$$(13)(25)(46) \cdot (152)(364) = (1234)(5)(6).$$

Using insertion on the cycles $(5)(6)$, we get a member of $[4, 3^2]$, on which insertion can be applied again. Now use insertion on one cycle to finish all cases with $n, m > 1$.

For the case $m = 1, n \geq 5$ use insertion on

$$(15)(29)(36)(48)(7A) \cdot (19745)(26A38) = (1234)(5)(6789A).$$

□

Lemma 5.7. *Suppose n_1, n_2, n_3, n_4 are odd, $n_1 + \cdots + n_4 \equiv 2 \pmod 4$, and $k \equiv 0 \pmod 4$. If $\{n_1, \ldots, n_4\} \neq \{3, 1, 1, 1\}$ then $[k, n_1, n_2, n_3, n_4] \in \mathcal{F}$.*

Also $[k, 3, 2, 1, 1, 1] \in \mathcal{F}$.

Proof. By assumption, 3 of the n_i are equivalent to 1 mod 4 and one to 3 mod 4, or *vice versa*.

Successive insertions in

$$(1A)(2E)(36)(48)(5B)(7D)(9C) \cdot (1AD26E9)(38C74B5) =$$
$$= (1)(23456)(789A)(B)(CDE)$$

and the equality

$$(19)(27)(3D)(48)(5B)(6A)(CE) \cdot (17BEC38)(2D5A496) =$$
$$= (1234)(567)(89A)(BCD)(E)$$

prove all cases with $n_i \leq 5$. The other cases may be seen by more insertions, or by direct sum of 5.4 and 5.6.

For $[k, 3, 2, 1, 1, 1] \in \mathcal{F}$ use

$$(1A)(2B)(36)(47)(58)(9C) \cdot (1B264A)(378C95) =$$
$$= (1234)(567)(89)(A)(B)(C).$$

□

Lemma 5.8. *Suppose n, m are odd, $n \not\equiv m \pmod 4$, and $k_1, k_2 \equiv 0 \pmod 4$. Then $[k_1, k_2, n, m] \in \mathcal{F}$.*

Proof. Insert in

$$(1A)(27)(35)(4C)(6B)(89) \cdot (17983C)(25B4A6) =$$
$$= (1234)(5678)(9)(ABC).$$

□

Lemma 5.9. *a. Let $k \in \hat{6}$. Then $[k,5,3],[k,3,1],[k,5,1^3] \in \mathcal{F}$.*
b. Let $k \in \hat{7}$. Then $[k,5^2,3],[k,5,3,1],[k,3,1^2] \in \mathcal{F}$.
c. Let $k \in \hat{9}$. Then $[k,3^2,1],[k,5,3^2],[k,5,3,1^3] \in \mathcal{F}$.

Proof. a. Insertion in

$$(15)(2A)(36)(48)(7E)(9C)(BD)\cdot(1ADBE74)(26538C9) =$$
$$= (123456)(789AB)(C)(D)(E)$$

and in

$$(17)(26)(3A)(48)(59)\cdot(16749)(2A385) = (123456)(789)(A).$$

b. Insertion in

$$(15)(26)(3C)(48)(79)(AB)\cdot(169BA4)(2C3875) =$$
$$= (1234567)(89A)(B)(C).$$

c. Insertion in

$$(1c)(2e)(3a)(4B)(5F)(6D)(7A)(8C)(9E)(bd)\cdot$$
$$\cdot(1e2adb5D9c)(3B8E7C6A4F) =$$
$$= (123456789)(ABCDE)(Fab)(c)(d)(e)$$

and insertion in

$$(1D)(2B)(3F)(4a)(58)(6E)(7A)(9C)\cdot(1B9D6A2F)(3a48C75E) =$$
$$= (123456789)(ABC)(DEF)(a).$$

□

The last lemma collects some special cases left untreated.

Lemma 5.10. *The following classes are all in $\mathcal{F}_0$:*
a. $[3^2,1^2]$, $[5,3^2,1]$, $[5^2,3^2]$.
b. $[5,2,1^3]$.
c. $[5^i,3^3,1^{3-i}]$ *($0 \le i \le 3$),* $[5^i,3,1^{5-i}]$ *($1 \le i \le 5$),* $[5,3^5]$.
d. $[3^5,2,1]$.
e. $[3,2^2,1^5]$.
f. $[3^9,1]$.

Proof. a. Insert once and twice in

$$(18)(24)(35)(67)\cdot(1438)(2576) = (123)(456)(7)(8).$$

b. Insert in $(19)(24)(36)(58)(7A)\cdot(14859)(26A73) = (12345)(67)(8)(9)(A)$.
c. Several insertions in

$$(14)(25)(36)(7A)(8B)(9C)\cdot(152634)(7B9A8C) =$$
$$= (123)(4)(5)(6)(789)(ABC)$$

and in

$$(18)(2B)(36)(4A)(59)(7C)\cdot(1B26C7)(3A4958)=$$
$$(12345)(678)(9)(A)(B)(C).$$

d. Insert in

$$(1D)(2A)(38)(4a)(5E)(69)(7B)(CF)(bc)\cdot$$
$$\cdot(1A73D59BF)(286acb4EC)$$
$$=(123)(456)(789)(ABC)(DEF)(ab)(c).$$

e. Insert in

$$(1B)(29)(3C)(46)(5A)(78)\cdot(192C3B)(4A5687)=$$
$$=(123)(45)(67)(8)(9)(A)(B)(C).$$

f. Insert in

$$(1m)(2b)(3B)(4j)(57)(6i)(8D)(9C)(Ad)(Ek)(Fl)(ah)(ce)(fg)\cdot$$
$$\cdot(1bega2B95ifA3m)(47DkF8Cdch6jEl)=$$
$$=(123)(456)(789)(ABC)(DEF)(abc)(def)(ghi)(jkl)(m).$$

□

6. Classes outside $[2^{n/2}]^3$

In this section we finish the proof of theorem 4.1, by showing that none of the classes in $\mathcal{E}$ (as defined in section 4) is contained in $[2^{n/2}]^3$.

We first state that $[3^5,1]\not\subseteq[2^8]^3$. This can be checked by using Burnside's formula (2) to compute the coefficient of $\widehat{[3^5,1]}$ in $\widehat{[2^8]}^3$, which turns out to be zero.

Another way is to fix a representative $\pi\in[3^5,1]$, count through all the $|[2^8]|=2027025$ members $\tau\in[2^8]$, and use 3.2 to check whether $\tau\cdot\pi\in[2^8]^2$ (no, it is not).

We will now show that classes with many fixed points in $\mathcal{E}$ are not contained in $[2^{n/2}]^3$.

The key is the following cute fact.

Lemma 6.1. *Let $\pi=\sigma_1\sigma_2\sigma_3$, $\sigma_i\in[2^{n/2}]$.*

If, for some point x, $\forall i:\pi(\sigma_i(x))=\sigma_i(x)$, then $\pi(x)=x$.

More generally, if any 3 of the points $\{x,\sigma_1(x),\sigma_2(x),\sigma_3(x)\}$ are fixed under π, then so is the forth.

Proof. Construct a 3-regular graph, as in the proof of theorem 3.3: a point y is connected to $\sigma_i(y)$ in color $\#i$.

From $\pi(\sigma_3(x)) = \sigma_3(x)$ we see that $\sigma_2(x)$ and $\sigma_3(x)$ are connected with color #1. From $\pi(\sigma_1(x)) = \sigma_1(x)$ we see that $\sigma_1(x)$ and $\sigma_2(x)$ are connected with color #3.

From $\pi(\sigma_2(x)) = \sigma_2(x)$ we now see that $\sigma_1(x)$ and $\sigma_3(x)$ are connected with color #2. By traveling on the resulting graph, we see that $\pi = \sigma_1\sigma_2\sigma_3$ takes x to itself.

The other cases are proved by similar arguments. □

Theorem 6.2. *Let $C = C_0 \oplus [1^k] \subseteq [2^{n/2}]^3$, where C_0 is fixed-point free on m points, $m \leq k$.*

Then $C_0 \oplus [1^m] \subseteq [2^{n/2}]^3$.

Proof. Let $\pi \in C \subseteq [2^{n/2}]^3$. Construct the 3-regular graph as above. Let A be the support of π (so $|A| = m$), and $A \cup B$ the connected component containing A, $A \cap B = \phi$.

We count connections from A to B. First, any point in A must have at least one connection to another point in A (otherwise it would be a fixed point by 6.1). Again by 6.1, a point in B cannot have exactly one connection to A, so any point in B must have at least two connections to A.

The points in A have $3|A|$ connections all together, so

$$3|A| \geq |A| + 2|B|,$$

and thus $|B| \leq |A| = m$.

Write $\pi = \sigma_1\sigma_2\sigma_3$, $\sigma_i \in [2^{n/2}]$. The claim is proved by observing that all permutations can be restricted to $A \cup B$. □

Corollary 6.3. $[31^{1+4k}], [4,3,1^{3+4k}], [5,1^{3+4k}], [3,2,1^{1+4k}]$ *are not in* $[2^{n/2}]^3$ *for any* n.

Proof. By 6.2 we need only check the following claims: $[3,1] \not\subseteq [2^2]^3$, $[4,3,1^3] \not\subseteq [2^5]^3$, $[4,3,1^7] \not\subseteq [2^7]^3$, $[5,1^3] \not\subseteq [2^4]^3$, $[3,2,1] \not\subseteq [2^3]^2$, $[3,2,1^5] \not\subseteq [2^5]^2$.

This may be done directly. □

It remains to show that $[3,2^m,1], [5,3,2^m] \not\subseteq [2^{n/2}]^3$.

Let $\pi = \sigma_1\sigma_2\sigma_3$, $\sigma_i \in [2^{n/2}]$. By 3.2, the cycles of $\sigma_2\sigma_3$ come in pairs, where the cycles of a pair have the same length.

We refer to the length of the cycle of a point x in π as the *order of* x.

Note that if $\{x_1, x_2, \ldots, x_m\}$ are order-2 points on the same cycle of $\sigma_2\sigma_3$, with $\sigma_2\sigma_3(x_i) = x_{i+1}$ $(1 \leq i < m)$, then $\sigma_2\sigma_3(\sigma_1(x_{i+1})) =$

$\sigma_1^2\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3(x_i) = \sigma_1\pi^2(x_i) = \sigma_1(x_i)$, so $\{\sigma_1(x_m), \dots, \sigma_1(x_2), \sigma_1(x_1)\}$ are on a cycle of $\sigma_2\sigma_3$.

This simple observation has quite important consequences. First of all, if all points on a cycle of $\sigma_2\sigma_3$ have order 2, then the σ_1-image of this cycle is also a full cycle, and this pair of cycles may be omitted from expressions like $\pi = \sigma_1\sigma_2\sigma_3$ (as in 6.2).

Other corollaries are the following:

(a) If, on a cycle of $\sigma_2\sigma_3$, there is one point of order $d > 2$ and all the rest are of order 2, then the image of the cycle is part of a *larger* cycle. On this larger cycle there are at least two different points of order d.

(b) If x is a point of order 2 and $x, \pi(x)$ belong to the same $\sigma_2\sigma_3$-cycle, then on the section $x \to \pi(x)$ of the cycle there is an order-1 point, or at least two points of order $d > 2$. Note that this argument can be applied to $\pi(x)$ as well.

We can now prove

Theorem 6.4. $[3, 2^{n/2-2}, 1] \not\subseteq [2^{n/2}]^3$.

Proof. Assume, on the contrary, that $\pi = \sigma_1\sigma_2\sigma_3$ for $\sigma_1 \in [2^{n/2}]$, $\sigma_2\sigma_3 \in [2\lambda]$, while $\pi \in [3, 2^{n/2-2}, 1]$.

By the above remarks, we may assume that on each cycle of $\sigma_2\sigma_3$ there is some point of order $\neq 2$. Let x be the point with $\pi(x) = x$. If $(\sigma_2\sigma_3)^{-1}(x)$ has order 3, then so is $\sigma_1(x) = \pi(\sigma_2\sigma_3)^{-1}(x)$, and these two points are on the same cycle as x. Otherwise $(\sigma_2\sigma_3)^{-1}(x)$ has order 2, so the assumptions of (b) above are satisfied, and again there are (at least) two points of order 3 on this cycle.

In any case there is only one non-order-2 point left, so we may assume that $\sigma_2\sigma_3$ has only two cycles. By (a) they cannot have the same length, which contradicts theorem 3.2. □

By similar arguments (much more elaborated, though), we could prove $[5, 3, 2^{n/2-4}] \not\subseteq [2^{n/2}]^3$. With this theorem 4.1 is proved.

7. Graph-theoretic applications

In this section, the connection between graphs and powers of $[2^{n/2}]$ is used to motivate a classification of regular colorable graphs.

If g is a graph, we denote by g_V the set of vertices, and by g_E the set of edges ($g_E \subseteq g_V \times g_V$).

An *edge* m-coloring of g is a function $\alpha : g_E \to \{1, \cdots, m\}$, such that edges $e, f \in g_E$ with common vertex satisfy $\alpha(e) \neq \alpha(f)$. $\alpha(e)$ is the **color** of e.

Let $\mathcal{G}_m$ be the collection of m-regular loopless graphs.

If $g \in \mathcal{G}_m$ is a graph and α is an m-coloring of g, then σ_i ($i = 1, \cdots, m$) is defined by transferring vertex x to its neighbor along an edge with color i. Note that not all m-regular graphs are m-colorable.

For 3-regular graphs, we define the following invariant.

Definition 7.1. *Let $g \in \mathcal{G}_3$ be a graph on n vertices, α a 3-coloring of g. Then $\psi(g, \alpha)$ is the conjugacy class of S_n defined by*

$$\psi(g, \alpha) = [\sigma_1 \sigma_2 \sigma_3].$$

We require $\psi(g, \alpha)$ to be independent of the order of colors. Indeed,

$$\sigma_1 \sigma_2 \sigma_3 = \sigma_1 (\sigma_2 \sigma_3 \sigma_1) \sigma_1^{-1}$$

and

$$\sigma_1 \sigma_2 \sigma_3 = (\sigma_3 \sigma_2 \sigma_1)^{-1}.$$

Since (123) and (13) generate S_3, we see that $\psi(g)$ is indeed invariant under reordering the colors.

Example 7.2. *Let G be a group generated by three elements a, b, c of order 2. Then the Cayley graph of G is 3-regular with natural 3-coloring, and $\psi(G) = [r^{|G|/r}]$ where r is the order of abc.*

ψ may be used, for example, to prove that two given graphs are non-isomorphic. More details can be obtained from considering various colorings of the same graph.

Theorem 4.1 can be formulated in the following way:

Theorem 7.3. *There exist (g, α) on n vertices with $\psi(g, \alpha) = C$ iff $C \subseteq A_n^*$ and $C \notin \mathcal{E}_n$.*

Let (g, α) be a 3-colored 3-regular graph.

Let R be an equivalence relation on g_V such that $x \equiv y$ implies $\sigma_i(x) \equiv \sigma_i(y)$. The **quotient graph** $(g/R, \alpha)$ is defined as the graph on g_V/R with the induces coloring.

If g, g' are disjoint colored graphs, then $\psi(g \cup g')$ is the direct sum $\psi(g) \oplus \psi(g')$. Another property is that $\psi(g/R)$ is obtained from ψ by raising some of the cycles in $\psi(g)$ to certain powers.

Consider the infinite 3-regular tree. Every 3-colored 3-regular finite graph is a quotient graph is this tree, so theorem 7.3 is a claim about the quotients of the regular graph.

Likewise, we can interpret the Cayley graph situation in the light of 7.3. Let Γ be the Cayley graph of $< a, b, c | a^2 = b^2 = c^2 = 1, (abc)^3 = 1 >$ - this is the generic situation of $\psi(g, \alpha)$ of exponent 3. We may use 7.3 to describe the finite quotient graphs of Γ: they might have

$\psi(g)$ any class of exponent 3, except $[3, 1^m]$. This may be rephrased as condition on the number of triangles in the quotient graph.

Similar results can be obtained for the other families in $\mathcal{E}$.

References

[1] Z.Arad, M.Herzog and J.Stavi, *Powers and Products of Conjugacy Classes in Groups*, *in*, Products of Conjugacy Classes in Groups, eds. Z.Arad and M.Herzog, LNM **1112**, 1985.

[2] J.L.Brenner and J.Riddell, *Covering Theorems for Finite Nonablian Simple Groups VII, Asymptotics in the Alternating Groups*, Ars. Combinatoria, Vol. **1**, (1976), 77-108.

[3] 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.

[4] P.Diaconis, "Group Representations in Probability and Statistics", Lecture Notes - Monograph Series, Vol. 11.

[5] P. Diaconis and M. Shahshahani, *Generating a Random Permutation with Random Transpositions*, Z.Wahrscheinlichkeitstheorie Verw. Gebiete **57**, (1981), 159-179.

[6] Y. Dvir, *Covering Properties of Permutation Groups*, *in*, Products of Conjugacy Classes in Groups, eds. Z.Arad and M.Herzog, LNM **1112**, 1985.

[7] S. Fomin and N. Lulov, *On the number of rim hook tableaux*, Zapiski Nauch. Sem. POMI, **223**, (1995), 219-226.

[8] N.Lulov, *Random Walks on the Symmetric Groups*, Ph.D. Thesis, Harvard University, 1996.

[9] J.Riordan, "An Introduction to Combinatorial Analysis", John Wiley & Sons Inc., 1958.

[10] Y.Roichman, *Cayley Graphs of the Symmetric Groups*, Ph.D. Thesis, Jerusalem University, 1994.

Department of Mathematics, Bar-Ilan University, Ramat-Gan 52900, ISRAEL

E-mail address: vishne@macs.biu.ac.il