Symmetric functions, generalized blocks, and permutations with restricted cycle structure

Attila Maróti

November 2, 2005

Abstract

We present various techniques to count proportions of permutations with restricted cycle structure in finite permutation groups. For example, we show how a generalized block theory for symmetric groups, developed by Külshammer, Olsson, and Robinson, can be used for such calculations. The paper includes improvements of recurrence relations of Glasby, results on average numbers of fixed points in certain permutations, and a remark on a conjecture of Robinson related to the so-called $k(GV)$-problem of representation theory. We extend and give alternative proofs for previous results of Erdős, Turán; Glasby; Beals, Leedham-Green, Niemeyer, Praeger, Seress.

1 Introduction

Let $\ell \geq 2$ be an integer. An ℓ-regular element is a permutation of finite order where no cycle (in its disjoint cycle decomposition) has length divisible by ℓ. The notion of an ℓ-regular element appears naturally in combinatorics, computational group theory and in the representation theory of finite groups.

The starting point of this paper is an old result of Erdős and Turán [6] stating that the proportion of ℓ-regular elements $s_\ell(n)$ in the symmetric group S_n is $\prod_{i=1}^{[n/\ell]} \frac{\ell i-1}{\ell i}$ whenever ℓ is a power of a prime. Many mathematicians have noted that the Erdős-Turán argument, which uses power series, extends naturally for arbitrary integers $\ell \geq 2$. There are many different proofs for the formula $s_\ell(n)$. Bolker and Gleason [3] gave a bijective proof and indicated how an asymptotic formula for $s_\ell(n)$ can be obtained. Later, Bertram and Gordon [2] presented a somewhat simpler proof which had the consequence that if n is not divisible by ℓ, then the number of ℓ-regular permutations of S_n which take n to i is the same for all i with $1 \leq i \leq n$. The paper [4] of Bóna, McLennan, and White contains a short bijective argument. Two more proofs, one by Glasby [7] and one by Beals, Leedham-Green, Niemeyer, Praeger, and Seress [1] were motivated by questions in computational group theory. For another application of the formula for $s_\ell(n)$ see the paper [5] of Chernoff. In [7] Glasby established the estimate ${c_\ell}^{-1}(ew)^{-1/\ell} \leq s_\ell(n) \leq c_\ell w^{-1/\ell}$ where $w = [n/\ell]$ and $c_\ell = e^{\ell^{-2}\pi^2/6}$. This was improved by Beals, Leedham-Green, Niemeyer, Praeger, and Seress [1] to $s_\ell(n) = (1+o(1)) \cdot c_\ell \cdot n^{-1/\ell}$ for $n \geq \ell$ where $c_\ell = \ell^{1/\ell} \cdot \Gamma(1-1/\ell)^{-1}$ and where $\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt$ denotes the Gamma-function.

A formula for the proportion of ℓ-regular elements $a_\ell(n)$ in the alternating group A_n was obtained by Beals, Leedham-Green, Niemeyer, Praeger, and Seress [1]. Their formula involves an interesting function, $\delta_\ell(n)$ which is defined as follows. Write n in the form $n = \ell w + r$ where w, r are non-negative integers so that $0 \le r \le \ell - 1$. Let $\delta_\ell(n)$ be 0 if $2 \le r \le \ell - 1$, and $(-1)^{\ell w} \prod_{i=1}^{w}(1 - \frac{\ell-1}{\ell i})$ if $r = 0$ or $r = 1$. In [1] it was proved that $a_\ell(n) = s_\ell(n) + \delta_\ell(n)$, and that $a_\ell(n) = (1 + o(1))s_\ell(n)$ for $n \ge \ell$.

For permutation groups in general, the situation seems to be more complicated. An equivalent form of a deep and celebrated theorem of Isaacs, Kantor, and Spaltenstein [10] is the following. Let G be a permutation group of degree n, and let p be a prime dividing $|G|$. Then the proportion of p-regular elements in G is at most $(n-1)/n$ with equality only in the following cases: n is a power of p and G is sharply 2-transitive; or $n = p$ and G is the full symmetric group S_p.

In this paper we present a general formula for the proportion of ℓ-regular elements in an arbitrary finite permutation group. In Theorem 3.1 and in Corollary 3.1, we prove that if ℓ is an arbitrary integer, π is the set of prime divisors of ℓ, and G is a permutation group of degree n, then there exists an integer $\alpha_\ell(G)$ so that the proportion of ℓ-regular elements in G is equal to $\alpha_\ell(G)/d$ where $w = [n/\ell]$ and d is the greatest common divisor of $\ell^w (w!)_\pi$ and $|G|$.

In Section 4 we extend the Erdős-Turán argument to give an alternative proof for the Beals, Leedham-Green, Niemeyer, Praeger, Seress [1] result for the formula for $a_\ell(n)$. We use this result to answer a question of Robinson related to his conjecture which is in turn related to the recently solved $k(GV)$-problem of representation theory. Robinson's conjecture is an example where the proportion of p-regular elements (p prime) in a finite group is of fundamental importance.

In the next section we introduce generalized blocks for symmetric groups, a theory developed recently by Külshammer, Olsson, and Robinson [12]. We explain how their ideas could be used to calculate the proportions of ℓ-regular elements in permutation groups. As an example, we give yet another proof for a formula for $a_\ell(n)$.

In Section 6 we introduce symmetric functions to count proportions of other kinds of elements in the symmetric group. We do this, because we are searching for a possible generalization of the method of Külshammer, Olsson, Robinson described in Section 5. This section includes improvements of recursion formulas of Glasby [7], and yet other proofs for the formulas of $s_\ell(n)$ and $a_\ell(n)$.

We begin Section 7 by generalizing the notion of an ℓ-regular element. Let $\ell \ge 2$ be an arbitrary integer. Let H be a set of positive integers each of which is divisible by ℓ. A permutation (of finite order) is H-regular if no cycle has length equal to h for all $h \in H$. We then describe the results in [14]. We extend the generalized block theory for symmetric groups, and indicate how this extension could be used to count proportions of H-regular elements in a finite permutation group.

Section 8 uses Frobenius reciprocity to produce results on average numbers of fixed points of certain permutations in the symmetric group, S_n. For example, we prove that the average number of fixed points of ℓ-regular elements in S_n is 1 if $\ell \nmid n$ and is $n/(n-1)$ if $\ell | n$.

2 A lemma of Erdős and Turán

Let $p \geq 2$ be a prime dividing the order of a finite group G. A p-regular element in G is defined to be an element of order not divisible by p. Following [12] we generalize this concept for the case where p is not necessarily a prime and where G is a finite permutation group. Let $\ell \geq 2$ be an arbitrary integer. An ℓ-regular element is a permutation of finite order where no cycle (in the disjoint cycle decomposition) has length divisible by ℓ.

The starting point of this paper is an old result of Erdős and Turán [6] on the proportion $s_\ell(n)$ of ℓ-regular elements in the symmetric group S_n where ℓ is a prime power. Many mathematicians have noted that this result extends naturally for arbitrary integers $\ell \geq 2$. See also Theorem 6.1 of this paper. The idea of the proof of the following theorem goes back to Pólya.

Theorem 2.1 ([6]). *Let $\ell \geq 2$ be an integer. The proportion $s_\ell(n)$ of ℓ-regular elements in S_n is*

$$s_\ell(n) = \prod_{i=1}^{[n/\ell]} \frac{\ell i - 1}{\ell i}.$$

Proof. Notice that the number of permutations of the symmetric group S_n of cycle-shape $({n_1}^{m_1}, \ldots, {n_k}^{m_k})$ is

$$\frac{n!}{m_1! \ldots m_k! \cdot {n_1}^{m_1} \ldots {n_k}^{m_k}}.$$

This means that the proportion $s_\ell(n)$ is precisely the coefficient of z^n in the formal power series

$$\prod_{\substack{\nu=1 \\ \ell \nmid \nu}}^{\infty} \{1 + \frac{1}{1!}\frac{z^\nu}{\nu} + \frac{1}{2!}\Big(\frac{z^\nu}{\nu}\Big)^2 + \ldots\}.$$

For $|z| < 1$, this can be written in the form

$$\prod_{\substack{\nu=1 \\ \ell \nmid \nu}}^{\infty} \exp\Big(\frac{z^\nu}{\nu}\Big) = \exp\Big(\sum_{\nu=1}^{\infty} \frac{z^\nu}{\nu} - \sum_{\nu=1}^{\infty} \frac{z^{\nu\ell}}{\nu\ell}\Big) =$$

$$= \exp\Big(\sum_{\nu=1}^{\infty} \frac{z^\nu}{\nu}\Big) \cdot \Big(\exp\Big(\sum_{\nu=1}^{\infty} \frac{(z^\ell)^\nu}{\nu}\Big)\Big)^{-1/\ell}.$$

Since $\sum_{\nu=1}^{\infty} \frac{x^\nu}{\nu} = -\log(1-x)$ for $x = z$ and $x = z^\ell$, we can continue to write

$$\exp(-\log(1-z)) \cdot (\exp(-\log(1-z^\ell)))^{-1/\ell} = \frac{(1-z^\ell)^{1/\ell}}{1-z}.$$

Now the right-hand-side of the previous equation is equal to

$$\Big(\frac{1 + z + z^2 + \ldots + z^{\ell-1}}{(1-z)^{\ell-1}}\Big)^{1/\ell} = (1 + z + z^2 + \ldots + z^{\ell-1})(1-z^\ell)^{-\frac{\ell-1}{\ell}} =$$

$$= (1 + z + z^2 + \ldots + z^{\ell-1})\Big[1 + \sum_{m=1}^{\infty} \Big(1 - \frac{1}{\ell}\Big)\Big(1 - \frac{1}{2\ell}\Big) \ldots \Big(1 - \frac{1}{m\ell}\Big) \quad z^{m\ell}\Big],$$

which is exactly what we wanted.

□

Notice that for all non-negative integers $w \geq 0$, we have

$$s_\ell(\ell w) = s_\ell(\ell w + 1) = \ldots = s_\ell(\ell w + (\ell - 1)).$$

This observation will be used throughout the paper.

To illustrate the importance of Theorem 2.1 (in the special case when ℓ is a prime) we quote Glasby from Page 501 of [7]. "Suppose we are given a 'black box' group G which is known to be isomorphic to S_n for some n. How do we find n? The relative frequency of finding an element of G of odd order should be close to the probability $s_2(k)$ for precisely two values of k, say m and $m+1$. If p is the smallest prime divisor of m or $m+1$, then by determining the relative frequency of elements of G of order co-prime to p, one can determine, with quantifiable probability, whether n equals m or $m+1$."

3 Permutation groups and characters

Let us take a closer look at the formula of Theorem 2.1. How can we simplify the fraction? Let $\ell \geq 2$ be an arbitrary integer. If we put $w = [n/\ell]$, then Theorem 2.1 gives $s_\ell(n) = (\prod_{i=1}^{w}(\ell i - 1))(\ell^w w!)$. Now let π be a set of primes. If m is an arbitrary positive integer, then m_π denotes the π-part of m. If $\pi = \{p\}$ where p is a prime, then we write m_p instead of $m_{\{p\}}$. Put $m_{\pi'} = m/m_\pi$. We will need the following observation.

Lemma 3.1. *Let $\ell \geq 2$ be an integer. If π is the set of all primes dividing ℓ, then we have*

$$(w!)_{\pi'} \mid \prod_{i=1}^{w}(\ell i - 1).$$

Proof. It is sufficient to see that if p is an arbitrary prime not dividing ℓ, then

$$(w!)_p \leq (\prod_{i=1}^{w}(\ell i - 1))_p. \tag{1}$$

Let p be such a prime. We may suppose that $p \leq w$ for otherwise there is nothing to show. Let j, t be arbitrary positive integers so that $j \cdot p^t \leq w$. Since $p \nmid \ell$, the set $\{((j-1)p^t+1)\ell-1, \ldots, jp^t\ell-1\}$ is a complete set of representatives of the congruence classes of p^t. From this observation it is possible to deduce (1).

□

From Theorem 2.1, the above remark, and by Lemma 3.1, we see that

$$s_\ell(n) = \frac{\alpha_\ell(S_n)}{\ell^w \cdot (w!)_\pi} \tag{2}$$

where $\alpha_\ell(S_n)$ is a positive integer co-prime to $\ell^w \cdot (w!)_\pi$.

Using character theory of symmetric groups we will extend formula (2) for arbitrary finite permutation groups.

Theorem 3.1. *Let $\ell \geq 2$ be an integer, and let G be a permutation group of degree n. Put $w = [n/\ell]$, and let π be the set of primes dividing ℓ. Then the proportion of ℓ-regular elements in G is*

$$\frac{\alpha_\ell(G)}{\ell^w \cdot (w!)_\pi}$$

for some integer $\alpha_\ell(G)$.

The case of the symmetric group $G = S_n$ (see also formula (2)) shows that the denominator of the fraction $\alpha_\ell(G)/\ell^w (w!)_\pi$ in Theorem 3.1 is best possible in the sense that $\ell^w (w!)_\pi$ cannot be replaced by a smaller integer.

Before we begin the proof of Theorem 3.1, let us review a couple of basic facts about characters of finite groups.

Let G be a finite group. A class function of G is a complex-valued function on G which is constant on the conjugacy classes of G. If H is a subgroup of G and α is a class function of G, then the restriction $Res_H^G(\alpha)$ of α from G to H is also a class function. Furthermore, if α is a class function of the subgroup H of G, then the induced class function

$$Ind_H^G(\alpha)(g) = \frac{1}{|H|} \sum_{x \in G} \alpha^0(xgx^{-1})$$

is a class function of G where $\alpha^0(h) = \alpha(h)$ if $h \in H$ and $\alpha^0(y) = 0$ if $y \notin H$. If α, β are two class functions of a finite group G, then we define their inner product by

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}.$$

So if 1_G is the class function which is defined by $\alpha(g) = 1$ if g is an ℓ-regular element and $\alpha(g) = 0$ otherwise, then $\langle 1_G, 1_G \rangle$ is precisely the proportion of ℓ-regular elements in the permutation group G.

If $\mathcal{C}$ is a union of a set of conjugacy classes of G, then we write $\langle \alpha, \beta \rangle_{\mathcal{C}}$ for

$$\frac{1}{|G|} \sum_{g \in \mathcal{C}} \alpha(g)\overline{\beta(g)}$$

and call it the truncated inner product of α and β across $\mathcal{C}$. We will only need this general setup in later parts of the paper. At the moment we are only interested in the situation where $\mathcal{C}$ is the set of ℓ-regular elements in a finite permutation group. In this case we write $\langle \alpha, \beta \rangle_{\ell-reg}$ instead of $\langle \alpha, \beta \rangle_{\mathcal{C}}$.

There are simple identities, which we will use throughout the paper. Let H be a subgroup of G, let α be a class function of H, and β be a class function of G. Then

$$\langle Ind_H^G(\alpha), \beta \rangle = \langle \alpha, Res_H^G(\beta) \rangle. \tag{3}$$

Furthermore, if G is a permutation group and H is a subgroup in G, then we have the identity

$$\langle Ind_H^G(\alpha), \beta \rangle_{\ell-reg} = \langle \alpha, Res_H^G(\beta) \rangle_{\ell-reg}. \tag{4}$$

We will refer to both (3) and (4) as Frobenius reciprocity. We note that the formula (4) will still hold true if we replace ℓ-reg with some other 'nice' union of conjugacy classes $\mathcal{C}$. At this point the reader could read Section 8 to see (in a certain sense) a more general form of Frobenius reciprocity together with an application.

The trace function of a complex (irreducible) representation of a finite group G is called a(n) (irreducible) character of G. Since a character is constant on conjugacy classes, we see that it is a class function. A character χ is irreducible if and only if $\langle \chi, \chi \rangle = 1$. The set of all irreducible characters of G is denoted by $Irr(G)$. The constant 1 class function 1_G of G is an irreducible character called the trivial character of G. If χ, $\psi \in Irr(G)$ are different irreducible characters, then $\langle \chi, \psi \rangle = 0$. The set $Irr(G)$ is a basis for the complex vector space of all class functions of G, so $|Irr(G)|$ is equal to the number of conjugacy classes of G. Each character is a non-negative integer combination of irreducible characters, and a class function which is an integer combination of irreducible characters is called a generalized character. Restrictions and induced class functions of characters are characters.

Since we will be working with permutation groups soon, we need some basic facts about the character theory of the symmetric group, S_n.

Let n be a positive integer. A partition λ of n is an ordered k-tuple $(\lambda_1, \ldots, \lambda_k)$ for some positive integer k where $\lambda_1 \geq \ldots \geq \lambda_k$ are positive integers with $\sum_{i=1}^{k} \lambda_i = n$. If λ is a partition of n, then we write $\lambda \vdash n$. For each partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n, we define S_λ to be a subgroup of S_n isomorphic to $S_{\lambda_1} \times \ldots \times S_{\lambda_k}$ with orbits of sizes $\lambda_1, \ldots, \lambda_k$. Such groups are called Young subgroups. For each partition λ, the Young subgroups, S_λ form a single conjugacy class of subgroups in S_n. Let λ be a partition of n. The character $Ind_{S_\lambda}^{S_n}(1_{S_\lambda})$ is called the Young character of S_n associated to the conjugacy class of Young subgroups, S_λ. The irreducible characters (and the conjugacy classes) of S_n are labelled canonically by partitions of n. Denote the irreducible character of S_n labelled by the partition λ by χ_λ. Since the χ_λ's are irreducible, each Young character is a non-negative integer combination of $Irr(S_n)$. However, surprisingly, the converse is also true: each irreducible character is an integer combination of Young characters. (See Theorem 2.2.10 of [11].) This means that each character of S_n is an integer combination of Young characters.

We are now in the position to prove Theorem 3.1. Fix an arbitrary integer $\ell \geq 2$. Let G be a permutation group of degree n. Put $n = \ell w + r$ where w and r are integers with $0 \leq r \leq \ell - 1$. Let $\alpha_\ell(G)$ be the real number so that the probability that an element of G is ℓ-regular is equal to

$$\frac{\alpha_\ell(G)}{\ell^w w!_\pi},$$

where m_π denotes the π-part of the integer m with π the set of primes dividing ℓ.

We need to show that $\alpha_\ell(G)$ is an integer.

By the remark after the proof of Lemma 3.1, we know that $\alpha_\ell(S_n)$ is an integer. More generally, if G is a Young subgroup S_λ where $\lambda = (\lambda_1, \ldots, \lambda_k)$, then

$$\frac{\alpha_\ell(G)}{\ell^w w!_\pi} = \prod_{i=1}^{k} \frac{\alpha_\ell(S_{\lambda_i})}{\ell^{[\lambda_i/\ell]}([\lambda_i/\ell])!_\pi} = \frac{m(\lambda, \ell) \cdot \prod_{i=1}^{k} \alpha_\ell(S_{\lambda_i})}{\ell^w \cdot w!_\pi}$$

for some integers $m(\lambda, \ell)$, $\alpha_\ell(S_{\lambda_1}), \ldots, \alpha_\ell(S_{\lambda_k})$. Finally, let G be an arbitrary permutation group of degree n. Then the character $Ind_G^{S_n}(1_G)$ is an integer combination

$$Ind_G^{S_n}(1_G) = \sum_{\lambda \vdash n} a_\lambda \cdot Ind_{S_\lambda}^{S_n}(1_{S_\lambda}) \tag{5}$$

of Young characters, $Ind_{S_\lambda}^{S_n}(1_{S_\lambda})$. From (5) we have

$$\langle Ind_G^{S_n}(1_G), 1_{S_n}\rangle_{\ell-reg} = \sum_{\lambda \vdash n} a_\lambda \cdot \langle Ind_{S_\lambda}^{S_n}(1_{S_\lambda}), 1_{S_n}\rangle_{\ell-reg}$$

which, by Frobenius reciprocity, translates to

$$\langle 1_G, 1_G\rangle_{\ell-reg} = \sum_{\lambda \vdash n} a_\lambda \cdot \langle 1_{S_\lambda}, 1_{S_\lambda}\rangle_{\ell-reg}.$$

We conclude that $\alpha_\ell(G)$ is an integer combination of the $\alpha_\ell(S_\lambda)$'s, so it is itself an integer.

This proves Theorem 3.1.

Note that we have the trivial lower bound $\alpha_\ell(G) \geq 1$. This is attained by infinitely many groups, while a sharp upper bound for $\alpha_\ell(G)$ (not supposing it is an integer) in the special case when ℓ is a prime such that ℓ divides $|G|$, is a celebrated theorem of Isaacs, Kantor, and Spaltenstein [10]. To be precise, let us state this very deep and interesting result. Let G be a permutation group of degree n, and let p be a prime divisor of $|G|$. Then the number of elements of order divisible by p (i.e. the p-singular elements) is at least $|G|/n$ with equality only in the following cases: n is a power of p and G is sharply 2-transitive; or $n = p$ and G is the full symmetric group S_p.

G. R. Robinson [17] kindly pointed out that Theorem 3.1 can be improved.

Corollary 3.1. *Let $\ell \geq 2$ be an integer, and let G be a permutation group of degree n. Put $w = [n/\ell]$, and let π be the set of primes dividing ℓ. Then there exists an integer $\beta_\ell(G)$ so that the proportion of ℓ-regular elements in G is*

$$\frac{\beta_\ell(G)}{d}$$

where d denotes the greatest common divisor of the integers $\ell^w (w!)_\pi$ and $|G|_\pi$.

Proof. Let $\ell \geq 2$ be an integer, and let G be a permutation group of degree n. Put $w = [n/\ell]$, and let π be the set of primes dividing ℓ. Let m denote the proportion of ℓ-regular elements in G. By Theorem 3.1, the rational number $m \cdot \ell^w (w!)_\pi$ is an integer. Also, $m \cdot |G|$ is an integer. If we denote the greatest common divisor of $\ell^w (w!)_\pi$ and $|G|_\pi$ by d, then there are integers a and b so that

$$d = a \cdot |G| + b \cdot \ell^w (w!)_\pi.$$

From this we see that md is an integer.

□

4 The alternating group and a conjecture of Robinson

Sometimes even the precise formula for the proportion of ℓ-regular elements in a permutation group can be given. Below we will use the idea of the proof of Theorem 2.1 and Frobenius reciprocity to determine the proportion $a_\ell(n)$ of ℓ-regular elements in the alternating group, A_n. The formula for $a_\ell(n)$ is due to Beals, Leedham-Green, Niemeyer, Praeger, Seress [1], and it involves an interesting function, $\delta_\ell(n)$. Put $n = \ell w + r$ for integers w and $0 \le r \le \ell - 1$. Then we define $\delta_\ell(n)$ to be 0 if $2 \le r \le \ell - 1$, and $(-1)^{\ell w} \prod_{i=1}^{w}(1 - \frac{\ell-1}{\ell i})$ if $r = 0$ or $r = 1$.

Theorem 4.1 (Beals, Leedham-Green, Niemeyer, Praeger, Seress, [1])**.** *Let $\ell \ge 2$ be an integer, and let $\delta_\ell(n)$ be as above. Then the proportion $a_\ell(n)$ of ℓ-regular elements in A_n is*

$$a_\ell(n) = s_\ell(n) + \delta_\ell(n),$$

where $s_\ell(n)$ is the proportion of ℓ-regular elements in S_n.

Proof. Let ϵ_{S_n} be the class function of S_n which is 1 on even permutations and -1 on odd permutations. This class functions is actually a character, called the sign character of S_n. Using Frobenius reciprocity (see identity (4)), we find that

$$a_\ell(n) = \langle 1_{A_n}, 1_{A_n} \rangle_{\ell-reg} = \langle Ind_{A_n}^{S_n}(1_{A_n}), 1_{S_n} \rangle_{\ell-reg} = \langle 1_{S_n} + \epsilon_{S_n}, 1_{S_n} \rangle_{\ell-reg} =$$

$$= \langle 1_{S_n}, 1_{S_n} \rangle_{\ell-reg} + \langle \epsilon_{S_n}, 1_{S_n} \rangle_{\ell-reg} = s_\ell(n) + \langle \epsilon_{S_n}, 1_{S_n} \rangle_{\ell-reg}.$$

Hence it is sufficient to see that $\langle \epsilon_{S_n}, 1_{S_n} \rangle_{\ell-reg} = \delta_\ell(n)$ is the coefficient of z^n in

$$\prod_{\substack{\nu=1 \\ \ell \nmid \nu}}^{\infty} \{1 + \frac{1}{1!}\frac{(-z)^\nu}{(-\nu)} + \frac{1}{2!}\Big(\frac{(-z)^\nu}{(-\nu)}\Big)^2 + \ldots\}.$$

This can be written for $|z| < 1$ as

$$\Big(\prod_{\substack{\nu=1 \\ \ell \nmid \nu}}^{\infty} exp\Big(\frac{(-z)^\nu}{\nu}\Big)\Big)^{-1} =$$

$$= \Big(\frac{(-z)^\ell - 1}{(-z) - 1} \cdot (1 - (-z)^\ell)^{-\frac{\ell-1}{\ell}}\Big)^{-1} = (z+1)(1 - z^\ell)^{-\frac{1}{\ell}} =$$

$$= (z+1)\Big(1 + \sum_{m=1}^{\infty} (-1)^{m\ell} \cdot \frac{1}{\ell} \cdot \frac{\ell+1}{2\ell} \cdot \ldots \cdot \frac{(m-1)\ell + 1}{m\ell} \quad z^{m\ell}\Big).$$

This proves the theorem.

□

We note here that Beals, Leedham-Green, Niemeyer, Praeger, and Seress [1] also proved the estimate $a_\ell(n) = (1 + o(1))s_\ell(n)$ for $n \ge \ell$.

Later we will give (essentially) two more proofs for Theorem 4.1. We will mainly be interested in the function $\delta_\ell(n)$.

Theorem 4.1 is useful in answering a question of Robinson.

We recall a recent conjecture of Robinson [16] which is related to the famous $k(GV)$-problem of representation theory.

Let p be a prime number. Let G be a finite group with a non-trivial Abelian normal p-subgroup V such that $C_G(V)$ is a p-group. Let S be a Sylow p-subgroup of G, and set $P = S/V$. For each $v \in C_V(S)$, set $H(v) = C_G(v)/V$ and let $H(v)_{p'}$ denote the set of p-regular elements of $H(v)$. Put $H(1) := H$.

Let $k_d(G)$ be the number of irreducible characters, χ of G which satisfy $p^d\chi(1)_p = |G|_p$.

The conjecture is the following.

Conjecture 4.1 (Robinson, [16]). *Under the hypotheses above, we have*

$$\sum_{d=0}^{\infty} \frac{k_d(G)}{p^{2d}} \leq max\{\frac{|H(v)_{p'}|}{|V||H(v)|} : v \in C_V(S)\}.$$

A special case of this is proved in [16]. See also [8]. In [16] it is noted that if we additionally assume that G/V has a normal p-complement, then the conjectured bound translates to

$$\sum_{\mu \in Irr(G)} \mu(1)_p^2 \leq |G|_p$$

which is stronger than the recently solved $k(GV)$-conjecture stating only that $|Irr(G)| \leq |G|_p$ (when G/V is a p'-group). The implication above follows from the fact that in this special case we have

$$max\{\frac{|H(v)_{p'}|}{|H(v)|} : v \in C_V(S)\} = \frac{|H_{p'}|}{|H|}. \tag{6}$$

Does (6) hold in general? The answer is no.

Let $p > 2$ be a prime, and let $n = pw + 2$ for some even integer w. Let V be the natural n-dimensional permutation A_n-module over $GF(p)$ with basis $\{e_1, \ldots e_n\}$. Put H to be A_n and G to be the semidirect product VA_n. Let $v = e_1$. Now $H(v) = A_{n-1}$, so $H(v)$ contains a Sylow p-subgroup of H. By Theorem 4.1 we see that the proportion of p-regular elements in $H(v)$ is greater than the proportion of p-regular elements in H, since

$$a_\ell(n) = s_\ell(n) < s_\ell(n) + (-1)^{\ell w} \prod_{i=1}^{w} (1 - \frac{\ell - 1}{\ell i}) =$$

$$= s_\ell(n-1) + \delta_\ell(n-1) = a_\ell(n-1).$$

For $p = 2$ the previous argument does not work. In this case, take V to be the natural 23-dimensional permutation M_{23}-module over $GF(2)$ with basis $\{e_1, \ldots e_{23}\}$. So H is M_{23} and G is the semidirect product VM_{23}. Put $v = e_1$ as before. Now $H(v) = M_{22}$, so it contains the Sylow 2-subgroup of M_{23}. Finally, it is checked that the proportion of 2-regular elements in M_{23} is 79/128, while the proportion of 2-regular elements in M_{22} is greater, it is 89/128.

5 Generalized blocks for symmetric groups

The reason why we could determine $a_\ell(n)$ was that we knew the character $Ind_{A_n}^{S_n}(1_{A_n})$. Next we will show a method to calculate the proportion of ℓ-regular elements in a given permutation group G in case we are able to decompose the character $Ind_G^{S_n}(1_G)$ of S_n into its irreducible constituents. The theory we need was developed by Külshammer, Olsson, Robinson in [12] where they generalized the notion of a p-block (where p is prime) of the symmetric group.

Let us remind the reader what a p-block is. Let G be a finite group, let p be a prime, and let F be an algebraically closed field of characteristic p. The group algebra FG may be written as the direct sum of minimal two-sided ideals called p-blocks. Each complex irreducible character χ of G is associated with a unique p-block B. We say that χ is in the p-block B.

In the special case of the symmetric group, there is a combinatorial description for the distribution of complex irreducible characters to p-blocks. This is called the Nakayama conjecture (which is already a theorem).

To state the Nakayama conjecture, we need some basic notions and results about partitions. Let $\ell \geq 2$ be an arbitrary integer. To each partition λ we associate its ℓ-core and its ℓ-quotient denoted by γ_λ and β_λ, respectively. (See [11] and Example 1.8 of [13] for details.) The ℓ-core is obtained from λ by removing all ℓ-hooks from λ. The number of ℓ-hooks to be removed from λ to go to the core is called the ℓ-weight of λ and is denoted by w_λ. The quotient β_λ is an ℓ-tuple of partitions whose cardinalities add up to w_λ. It is known that γ_λ and β_λ determine λ uniquely.

For example, if $\lambda = (n)$, then the arithmetic construction of the ℓ-core and the ℓ-quotient is an analogue of the division algorithm for integers. Indeed, if we write $n = \ell w + r$ where w and $0 \leq r \leq \ell - 1$ are integers, then $\gamma_{(n)} = (r)$ (for a suitably chosen integer $m \geq n$ in Example 1.8 of [13]) and $\beta_{(n)}$ is the ℓ-tuple of partitions where the 0-th entry is (w) and all other entries are the empty partitions. For another example, let $\lambda = (1^n)$ and put $n = \ell w + r$ as above. Then the ℓ-core is $\gamma_{(1^n)} = (1^w)$, and the ℓ-quotient, $\beta_{(1^n)}$ is the ℓ-tuple of partitions where the i-th entry is (1^w) where $i \equiv 1 - 2r \pmod{\ell}$ and all other entries are the empty partitions (when taking the same integer $m \geq n$ as above). See part (d) of Example 1.8 of [13] for details.

To clarify these concepts, we give other examples. However, the reader may skip this part, and continue with the Nakayama conjecture.

Let $n = 19$, $\ell = 3$, and $\lambda = (6, 5, 5, 1, 1, 1)$. Then the ℓ-core of λ is $\gamma_\lambda = (3, 1)$. The diagram below displays λ and γ_λ. The 3-core γ_λ is obtained from λ by removing five 3-hooks in the order defined by the letters a, b, c, d, and e. Hence the 3-weight of λ is 5.

			d	c	c
	e	d	d	c	
e	e	b	b	b	
a					
a					
a					

Note that it is possible to get the 3-core of λ by removing the 3-hooks in a different order. See the diagram below.

			c	c	c
	e	b	b	a	
e	e	b	a	a	
d					
d					
d					

To obtain the 3-quotient of λ, we must first fix an integer m that is at least the number of parts of λ. If we start with another integer m', then the construction given in [11] and in Example 1.8 of [13] will yield a new sequence where the components are cyclically permuted. If we fix $m = 19$, then the 3-quotient of λ is $\beta_\lambda = (\emptyset, (1,1), (2,1))$. Notice that $0+1+1+2+1$ is exactly the 3-weight of λ. This indicates that the 3-quotient records the 3-hook removals from λ.

Next we give a different partition μ of 19 having the same 3-core.

			d	c	c	c
	e	d	d			
e	e	a	a			
b	b	a				
b						

The 3-weight of μ is also 5. Only the 3-quotients, β_λ and β_μ distinguish between the partitions, λ and μ. We should choose m to be 19 again. Then the method given in [11] and in Example 1.8 of [13] gives $\beta_\mu = ((2), \emptyset, (3))$.

Now we state the Nakayama conjecture. Recall that the complex irreducible characters of S_n are labelled canonically by partitions of n.

Theorem 5.1 (Nakayama conjecture)**.** *Let $\ell \geq 2$ be a prime, and let λ and μ be partitions of n. Then the irreducible characters χ_λ and χ_μ lie in the same ℓ-block of S_n, if and only if, λ and μ have the same ℓ-core.*

The Külshammer, Olsson, Robinson [12] result is essentially a generalization of the Nakayama conjecture for arbitrary integers $\ell \geq 2$.

We use the truncated inner product across ℓ-regular elements to define a graph on $Irr(S_n)$. We join the distinct vertices χ_λ and χ_μ by an undirected edge, if and only if, $\langle \chi_\lambda, \chi_\mu \rangle_{\ell-reg} \neq 0$. The (sets of vertices of the) connected components of this graph are called the ℓ-linked blocks of S_n. A combinatorial ℓ-block of S_n is a subset of $Irr(S_n)$ consisting of all characters labelled by partitions with a fixed ℓ-core. So the Nakayama conjecture says that the ℓ-linked blocks and the combinatorial ℓ-blocks coincide for S_n in case ℓ is a prime. This was generalized in [12].

Theorem 5.2 (Külshammer, Olsson, Robinson, [12])**.** *Let $\ell \geq 2$ be an arbitrary integer. Then ℓ-linked blocks and combinatorial ℓ-blocks are the same for S_n.*

From now on, we will call an ℓ-linked block or a combinatorial ℓ-block simply an ℓ-block. The ℓ-block containing the trivial character of S_n is called the principal ℓ-block.

So suppose we have a permutation group G of degree n, and we want to know the proportion of ℓ-regular elements in G. By Frobenius reciprocity, we wish to calculate $\langle 1_G, 1_G \rangle_{\ell-reg} = \langle Ind_G^{S_n}(1_G), 1_{S_n} \rangle_{\ell-reg}$. For this, by Theorem 5.2, we only need to know the multiplicities of just those irreducible constituents of $Ind_G^{S_n}(1_G)$ which lie in the principal ℓ-block of S_n. This explains why $\delta_\ell(n)$ was 0 in case $r \neq 0$ and $r \neq 1$. (The partitions (n) and (1^n) have different ℓ-cores if $r \neq 0$ and $r \neq 1$.)

If we know the multiplicities of all those irreducible constituents of $Ind_G^{S_n}(1_G)$ which do lie in the principal ℓ-block of S_n, then our problem reduces to calculating $\langle \chi_\lambda, 1_{S_n} \rangle_{\ell-reg}$ for all partitions λ of n with ℓ-cores equal to $\gamma_{(n)}$. This was also done by Külshammer, Olsson, and Robinson [12] in their proof of Theorem 5.2.

Let us explain their ideas.

In [12] it was found that it is easier to work in a smaller generalized symmetric group than in the symmetric group itself. Let λ, μ be partitions of n with the same ℓ-core. We want to calculate $\langle \chi_\lambda, \chi_\mu \rangle_{\ell-reg}$ where $\gamma_\lambda = \gamma_\mu$. We may suppose that $n \geq \ell$. Put $n = \ell w + r$ for non-negative integers $w \geq 1$ and $0 \leq r \leq \ell - 1$ as before, and consider the generalized symmetric group $Z_\ell \wr S_w$.

The group $Z_\ell \wr S_w$ is a semidirect product of the base group Z_ℓ^w with S_w, so its elements are of the form $(a_1, \ldots, a_w)\sigma$ where the a_i's are elements of Z_ℓ and $\sigma \in S_w$. We think of Z_ℓ as the multiplicative group of the set of complex ℓ-th roots of unity.

Let reg be the set of all elements $(a_1, \ldots, a_w)\sigma$ of $Z_\ell \wr S_w$ where the product of the a_i's corresponding to each cycle of σ is different from 1. The set reg is a union of conjugacy classes of $Z_\ell \wr S_w$. An element in reg is called a regular element.

Regular elements of $Z_\ell \wr S_w$ have an alternative description which was communicated to the author by G. R. Robinson. The group S_w can be represented as a group of w-by-w permutation matrices. Similarly, $Z_\ell \wr S_w$ can also be represented as a group of w-by-w matrices where each element $(a_1, \ldots, a_w)\sigma \in Z_\ell \wr S_w$ corresponds to a matrix $M_{(a_1,\ldots,a_w)\sigma}$ where the $(i, \sigma(i))$-entry is the complex ℓ-th root of unity a_i for all $1 \leq i \leq w$ and where all other entries are 0's. An alternative description [17] of regular elements is

Proposition 5.1. *An element $(a_1, \ldots, a_w)\sigma \in Z_\ell \wr S_w$ is regular if and only if $M_{(a_1,\ldots,a_w)\sigma}$ has no eigenvalue equal to* 1.

Proof. Let $(a_1, \ldots, a_w)\sigma$ be an arbitrary element of $Z_\ell \wr S_w$ where the a_i's are complex ℓ-th roots of unity and $\sigma \in S_w$. Let $M_{(a_1,\ldots,a_w)\sigma}$ be the corresponding w-by-w matrix as defined above.

First suppose that σ is a single cycle of length w. Without loss of generality, we may assume that $\sigma = (1, \ldots, n)$. Then the matrix $M_{(a_1,\ldots,a_w)\sigma}$ has the form

$$\begin{pmatrix} 0 & a_1 & 0 & \ldots & 0 \\ 0 & 0 & a_2 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & a_{n-1} \\ a_n & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

This matrix has characteristic polynomial $(-1)^n(\lambda^n - a_1 \dots a_n)$. This means that $M_{(a_1,\dots,a_w)\sigma}$ has an eigenvalue equal to 1 if and only if $a_1 \dots a_n = 1$, that is, if and only if $(a_1, \dots, a_w)\sigma$ is not regular.

Now suppose that σ is a product of $t \geq 2$ disjoint cycles. Then the rows and columns of $M_{(a_1,\dots,a_w)\sigma}$ can be permuted in such a way, so that we get a block diagonal matrix $M'_{(a_1,\dots,a_w)\sigma}$ with exactly t blocks each of the above form. It is clear that the set of eigenvalues of $M_{(a_1,\dots,a_w)\sigma}$ is the same as that of $M'_{(a_1,\dots,a_w)\sigma}$. Furthermore, the set of eigenvalues of $M'_{(a_1,\dots,a_w)\sigma}$ is equal to the union of the sets of eigenvalues of the t block diagonal matrices of $M'_{(a_1,\dots,a_w)\sigma}$. By the first part of the proof, we see that the matrix $M'_{(a_1,\dots,a_w)\sigma}$ has no eigenvalue equal to 1 if and only if $(a_1, \dots, a_w)\sigma$ is not regular. This finishes the proof of the proposition.

□

The irreducible characters (and conjugacy classes) of $Z_\ell \wr S_w$ are canonically labelled by ℓ-quotients of partitions of n of ℓ-weight w. For a reference, see the book [11]. Let the irreducible characters of $Z_\ell \wr S_w$ associated with the ℓ-quotients, β_λ and β_μ be ψ_{β_λ} and ψ_{β_μ}, respectively. Now Theorem 5.9 of [12] states that $\langle \chi_\lambda, \chi_\mu \rangle_{\ell-reg}$ is a particular sign times

$$\langle \psi_{\beta_\lambda}, \psi_{\beta_\mu} \rangle_{reg} := \frac{1}{\ell^w w!} \sum \psi_{\beta_\lambda}(g) \psi_{\beta_\mu}(g^{-1}),$$

where the sum is over reg, the set of regular elements g of $Z_\ell \wr S_w$.

The 'particular sign' we mentioned before is the ℓ-sign of λ multiplied by the ℓ-sign of μ. For every partition λ of n, the ℓ-sign of λ, σ_λ, is $(-1)^t$ where t is the sum of the leg lengths of all ℓ-hooks removed from λ when going to γ_λ. (The leg length of an ℓ-hook is the number of boxes in the longest column of the ℓ-hook minus 1.) For example, $\sigma_{(n)} = 1$ and $\sigma_{(1^n)} = (-1)^{w(\ell-1)}$.

We are now in the position to state Theorem 5.9 of [12].

Theorem 5.3 (Külshammer, Olsson, Robinson, [12])**.** *Let $\ell \geq 2$ and $n \geq \ell$ be arbitrary integers. Let λ and μ be partitions of n with the same ℓ-core, and let β_λ and β_μ be the ℓ-quotients of λ and μ, respectively. Then, with the notations above, we have*

$$\langle \chi_\lambda, \chi_\mu \rangle_{\ell-reg} = \langle \sigma_\lambda \psi_{\beta_\lambda}, \sigma_\mu \psi_{\beta_\mu} \rangle_{reg},$$

where σ_λ and σ_μ are the ℓ-signs of λ and μ, respectively.

This theorem provides the link between S_n and $Z_\ell \wr S_w$ that we need. On Page 543 of [12] it is proved that if χ is an irreducible character of $H = Z_\ell \wr S_w$ that lies over an S_w-stable linear character $\alpha \otimes \dots \otimes \alpha$ of the base group Z_ℓ^w, then

$$\langle \chi, 1_H \rangle_{reg} = \frac{1}{\ell^w w!} \sum_{\sigma \in S_w} \chi(\sigma)(\delta_{\alpha,1}\ell - 1)^{c(\sigma)} \ell^{w-c(\sigma)}, \tag{7}$$

where $c(\sigma)$ denotes the number of cycles of σ and where $\delta_{\alpha,1} = 1$ if $\alpha = 1_H$ and $\delta_{\alpha,1} = 0$ otherwise. Using Frobenius reciprocity, one can also write up a similar (but more complicated) formula for $\langle \chi, 1_H \rangle_{reg}$ in the case where χ does not lie over an S_w-stable linear character.

Let us try to use this theory to deduce the formula for $a_\ell(n)$. Fix arbitrary integers $\ell \geq 2$ and $n = \ell w + r$, where w and r are non-negative integers with $0 \leq r \leq \ell - 1$. First of all, notice that if $\lambda = (n)$, then β_λ may be chosen so that $1_{S_n} = \chi_{(n)} = \psi_{\beta_\lambda} = 1_H$ where $H = Z_\ell \wr S_w$. This means that we have

$$s_\ell(n) = \langle 1_{S_n}, 1_{S_n} \rangle_{\ell-reg} = \langle \chi_{(n)}, \chi_{(n)} \rangle_{\ell-reg} = \langle 1_H, 1_H \rangle_{reg} = p_\ell(w),$$

where $p_\ell(w)$ denotes the proportion of regular elements in $H = Z_\ell \wr S_w$. Also, by Frobenius reciprocity, we have

$$a_\ell(n) = \langle Ind_{A_n}^{S_n}(1_{A_n}), 1_{S_n} \rangle_{\ell-reg} = \langle \chi_{(n)} + \chi_{(1^n)}, \chi_{(n)} \rangle_{\ell-reg} =$$

$$= \langle \chi_{(n)}, \chi_{(n)} \rangle_{\ell-reg} + \langle \chi_{(1^n)}, \chi_{(n)} \rangle_{\ell-reg} = s_\ell(n) + \langle \chi_{(1^n)}, \chi_{(n)} \rangle_{\ell-reg}.$$

If r is different from 0 and 1, then $\langle \chi_{(1^n)}, \chi_{(n)} \rangle_{\ell-reg} = 0$, since the partitions (1^n) and (n) then have different ℓ-cores, so they are in different ℓ-blocks. Hence we may suppose that $r = 0$ or 1. In this case, by Theorem 4.1, we would need to show that

$$\delta_\ell(n) = \langle \sigma_{(1^n)} \psi_{\beta_{(1^n)}}, \sigma_{(n)} \psi_{\beta_{(n)}} \rangle_{reg}.$$

As noted before, we may put $\psi_{\beta_{(n)}} = 1_H$. Also, notice that $\sigma_{(n)} = 1$, $\sigma_{(1^n)} = (-1)^{w(\ell-1)}$, and that $\psi_{\beta_{(1^n)}}$ is an S_w-stable irreducible character, so formula (7) gives us

$$\langle \sigma_{(1^n)} \psi_{\beta_{(1^n)}}, \sigma_{(n)} \psi_{\beta_{(n)}} \rangle_{reg} = (-1)^{w(\ell-1)} \cdot \frac{1}{w!} \sum_{\sigma \in S_w} (-1)^w \ell^{-c(\sigma)}.$$

At this moment we are unable to show the identity

$$\delta_\ell(n) = (-1)^{w\ell} \cdot \frac{1}{w!} \sum_{\sigma \in S_w} \ell^{-c(\sigma)} \tag{8}$$

for $r \geq 2$. We will prove (8) only after Theorem 6.2 by use of symmetric functions. But before we introduce symmetric functions, let us summarize our results

Theorem 5.4. *Let $\ell \geq 2$ and $n \geq \ell$ be arbitrary integers. Let $s_\ell(n)$ and $a_\ell(n)$ be as before. Write $n = \ell w + r$ where $w \geq 1$ and $0 \leq r \leq \ell - 1$. Let $p_\ell(w)$ be the proportion of regular elements in $Z_\ell \wr S_w$. Then we have $s_\ell(n) = p_\ell(w)$; $a_\ell(n) = s_\ell(n)$ if $2 \leq r \leq \ell - 1$; and*

$$a_\ell(n) = s_\ell(n) + (-1)^{w\ell} \cdot \frac{1}{w!} \sum_{\sigma \in S_w} \ell^{-c(\sigma)}$$

if $r = 0$ or $r = 1$ where $c(\sigma)$ denotes the number of cycles in the permutation σ.

6 Symmetric functions

So far we used characters of finite groups and the theory of generalized blocks for symmetric groups to count ℓ-regular elements in permutation groups. Can we extend our methods to count other kinds of elements? To what extent do the above methods generalize?

Again, let our starting point be Theorem 2.1. The argument in the proof of Theorem 2.1 can be used to calculate proportions of various other types of elements in S_n. The only problem is that most of these proportions seem to have no closed, explicit, or 'nice' form, like that of the proportion of ℓ-regular elements. The proportion of fixed-point-free elements, or more generally, the proportion of elements with no cycle of length equal to a given integer ℓ is an exception. This proportion is $\sum_{i=1}^{[n/\ell]} (-1)^i \frac{1}{\ell^i \cdot i!}$.

The proof of Theorem 2.1 used only one variable, z. What if we increase the number of variables and use symmetric functions?

Let us introduce some basic notions and results on symmetric functions from Chapter 7 of [18] and Chapter 1 of [13].

Let $x = (x_1, x_2, \ldots)$ be a set of indeterminates. For a non-negative integer n, a homogeneous symmetric function of degree n over the ring of rationals $\mathbb{Q}$ is a formal power series

$$f(x) = \sum_{\alpha} c_\alpha x^\alpha,$$

where the sum is over all weak compositions $\alpha = (\alpha_1, \alpha_2, \ldots)$ of n, $c_\alpha \in \mathbb{Q}$, x^α stands for the monomial ${x_1}^{\alpha_1} {x_2}^{\alpha_2} \ldots$, and $f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots) = f(x_1, x_2, \ldots)$ holds for every permutation σ of the set of positive integers.

The set of all homogeneous symmetric functions of degree n over $\mathbb{Q}$ is denoted by $\Lambda_{\mathbb{Q}}^n$. The set $\Lambda_{\mathbb{Q}}^n$ is not just a $\mathbb{Q}$-vector space but it has the structure of a $\mathbb{Q}$-module. Now define $\Lambda_{\mathbb{Q}}$ to be the vector space direct sum $\Lambda_{\mathbb{Q}}^0 \oplus \Lambda_{\mathbb{Q}}^1 \oplus \ldots$. This has the structure of a $\mathbb{Q}$-algebra. The $\mathbb{Q}$-algebra $\Lambda_{\mathbb{Q}}$ is called the algebra of symmetric functions.

Let us give some examples of symmetric functions. Let $n > 0$ be a positive integer. Then the formal power series $h_0 = e_0 = p_0 = 1$, $h_n = \sum_{i_1 \leq \ldots \leq i_n} x_{i_1} \ldots x_{i_n}$, $e_n = \sum_{i_1 < \ldots < i_n} x_{i_1} \ldots x_{i_n}$, and $p_n = \sum_i {x_i}^n$ are symmetric functions. Furthermore, if $\lambda = (\lambda_1, \lambda_2, \ldots)$ is a partition of a non-negative integer, then the formal power series $h_\lambda = h_{\lambda_1} h_{\lambda_2} \ldots$; $e_\lambda = e_{\lambda_1} e_{\lambda_2} \ldots$; $p_\lambda = p_{\lambda_1} p_{\lambda_2} \ldots$ are also symmetric functions. For $r \geq 0$, h_r is called the r-th complete symmetric function, e_r is the r-th elementary symmetric function, and p_r is the r-th power sum. All three sequences of symmetric functions $h_1, h_2, \ldots$; $e_1, e_2, \ldots$; $p_1, p_2, \ldots$ are algebraically independent and generate Λ as a $\mathbb{Q}$-algebra. See these facts for example in Corollary 7.6.2, Theorem 7.4.4, and Corollary 7.7.2 of [18].

Since the power sums generate Λ as a $\mathbb{Q}$-algebra, we may express h_n and e_n ($n > 0$) as a $\mathbb{Q}$-linear combination of the p_λ's. It is possible to show that these expressions are

$$h_n = \sum_{\lambda \vdash n} {z_\lambda}^{-1} p_\lambda$$

and

$$e_n = \sum_{\lambda \vdash n} \epsilon_\lambda {z_\lambda}^{-1} p_\lambda$$

where z_λ is the order of the centralizer of an element of cycle-shape λ in the symmetric group S_n and ϵ_λ is $(-1)^{n-\ell(\lambda)}$ where $\ell(\lambda)$ denotes the number of parts of the partition λ.

Let us give another example of a symmetric function. Let G be any subgroup of S_n. The cycle indicator of G is the symmetric function

$$c(G) = \frac{1}{|G|} \sum_{\lambda \vdash n} n_G(\lambda) p_\lambda$$

where $n_G(\lambda)$ is the number of elements in G of cycle-shape λ. In the special cases of the symmetric and the alternating groups, it is possible to prove that

$$c(S_n) = \sum_{\lambda \vdash n} {z_\lambda}^{-1} p_\lambda = h_n \tag{9}$$

and

$$c(A_n) = h_n + e_n. \tag{10}$$

Let the generating function of the complete symmetric functions, the elementary symmetric functions, and the power sums be $H(t)$, $E(t)$, and $P(t)$, respectively. On Page 23 of [13] two recursion formulas are deduced from the identities $P(t) = H'(t)/H(t)$ and $P(-t) = E'(t)/E(t)$. These are

$$h_n = \frac{1}{n} \sum_{r=1}^{n} p_r h_{n-r} \tag{11}$$

and

$$e_n = \frac{1}{n} \sum_{r=1}^{n} (-1)^{r-1} p_r e_{n-r}. \tag{12}$$

Formulas (9), (10) together with (11), (12) are very useful in calculating proportions of elements of restricted cycle structure in S_n and in A_n. The key idea in these calculations is that since the power sums $p_1, p_2, \dots$ are algebraically independent over $\mathbb{Q}$, we can assign values to them (specialize them) in any way we like. Such a specialization will give us a homomorphism from the ring of symmetric functions Λ to $\mathbb{Q}$. (See Section 7.8 of [18] for more information.)

To show the power of these elementary ideas, we deduce simpler recurrence relations than those given by Glasby in [7].

Let ℓ be an arbitrary positive integer. Denote the probabilities that an element of S_n has a cycle (in its disjoint cycle decomposition) of length a multiple of ℓ, dividing ℓ, and equal to ℓ, by $h_n(\mathcal{CM}_\ell)$, $h_n(\mathcal{CD}_\ell)$, and $h_n(\mathcal{CE}_\ell)$, respectively. Similarly, let $h_n(\mathcal{OM}_\ell)$, $h_n(\mathcal{OD}_\ell)$, and $h_n(\mathcal{OE}_\ell)$ be the probabilities that an element of S_n has order a multiple of ℓ, order dividing ℓ, and order equal to ℓ, respectively. For convenience, for all $h_n(M)$ above, define $h_n(\overline{M})$ to be $1 - h_n(M)$.

We also need a technical definition. Let ℓ and r be both positive integers. Define $d(\ell, r)$ to be the product of all those prime power divisors of ℓ of highest possible exponent which do not divide r. (So for example, $d(2^2 3^2, 2^2 3) = 3^2$.)

Proposition 6.1. *Let ℓ be an arbitrary positive integer. With the notations above, we have*

$$h_n(\overline{\mathcal{CM}_\ell}) = \frac{1}{n} \sum_{\substack{r=1 \\ \ell \nmid r}}^{n} h_{n-r}(\overline{\mathcal{CM}_\ell}); \tag{13}$$

$$h_n(\overline{\mathcal{CD}_\ell}) = \frac{1}{n} \sum_{\substack{r=1 \\ r \nmid \ell}}^{n} h_{n-r}(\overline{\mathcal{CD}_\ell}); \tag{14}$$

$$h_n(\overline{\mathcal{CE}_\ell}) = \frac{1}{n}\sum_{\substack{r=1\\ r\neq\ell}}^{n} h_{n-r}(\overline{\mathcal{CE}_\ell}); \tag{15}$$

$$h_n(\mathcal{OM}_\ell) = \frac{1}{n}\sum_{r=1}^{n} h_{n-r}(\mathcal{OM}_{d(\ell,r)}); \tag{16}$$

$$h_n(\mathcal{OD}_\ell) = \frac{1}{n}\sum_{\substack{r=1\\ r|\ell}}^{n} h_{n-r}(\mathcal{OD}_\ell); \tag{17}$$

and

$$h_n(\mathcal{OE}_\ell) = \frac{1}{n}\sum_{\substack{r=1\\ r|\ell}}^{n} \sum_{d(\ell,r)|i|\ell} h_{n-r}(\mathcal{OE}_i) \tag{18}$$

with the initial condition that $h_0(M) = h_0(\overline{M}) = 1$ *for all* M.

Note that the sum is 0 if there is nothing to sum over.

Proof. Fix an arbitrary positive integer ℓ. If we put $p_r = 1$ if $\ell \nmid r$ and $p_r = 0$ otherwise, then (9) becomes an expression for $h_n(\overline{\mathcal{CM}_\ell})$, and (11) gives (13). If we put $p_r = 1$ if $r \nmid \ell$ and $p_r = 0$ otherwise, then (9) is an expression for $h_n(\overline{\mathcal{CD}_\ell})$, and (11) gives (14). If we put $p_r = 1$ if $r \neq \ell$ and $p_r = 0$ otherwise, then (9) is an expression for $h_n(\overline{\mathcal{CE}_\ell})$, and (11) gives (15). Finally, if we specialize $p_r = 1$ in case $r|\ell$ and put $p_r = 0$ otherwise, then (9) is an expression for $h_n(\mathcal{OD}_\ell)$, and (11) gives (17).

The proofs of equations (16) and (18) do not involve symmetric functions. (Though (interestingly) they are of similar form.) Count the number of elements of the given subset of S_n with respect to the length r of the cycle containing a fixed letter, and use induction.

□

Using the additional identities (10) and (12), similar recurrence relations may be given for alternating groups too, but we will not state those.

It can be very difficult to solve recurrence relations such as (13)-(18) for symmetric (and alternating) groups. One problem is that an explicit and 'nice' solution may not even exist. This is not the case for the recurrence relations (13) and (15).

It is difficult to derive the solution to (15). However, by the inclusion-exclusion principle, one can see that the solution is $\sum_{i=1}^{[n/\ell]} (-1)^i \frac{1}{\ell^i \cdot i!}$. The solution to (13) is $s_\ell(n)$ which we know well. To demonstrate the power of symmetric functions, let us give yet another proof for this explicit formula.

Theorem 6.1. *Let* $\ell \geq 2$ *be an integer. Then for all integers* $n \geq 0$ *we have*

$$s_\ell(n) = \prod_{i=1}^{[n/\ell]} \frac{\ell i - 1}{\ell i}.$$

Proof. Let us prove the theorem by induction on n. The claim is obviously true for $0 \leq n \leq \ell-1$. So suppose that $n = \ell w + r$ where $0 \leq r \leq \ell - 1$ and $w \geq 1$, and assume that the claim is true for all integers less than n. Consider the identity (9). For all $r \geq 1$, we put $p_r = 1$ if $\ell \nmid r$ and $p_r = 0$ if $\ell \mid r$. Then we get $h_m = s_\ell(m)$ for all integers m. By (11) and the induction hypothesis, we are now able to calculate the rational number h_n. In the following calculation we will repeatedly use the observation that if n_1, n_2 are integers less than n and $[n_1/\ell] = [n_2/\ell]$, then $h_{n_1} = h_{n_2}$.

$$s_\ell(n) = h_n = \frac{1}{n}\sum_{j=1}^{n} p_j h_{n-j} = \frac{1}{n}\big(\sum_{j=1}^{\ell} p_j h_{n-j} + \sum_{j=\ell+1}^{n} p_j h_{n-j}\big) =$$

$$= \frac{1}{n}\big(\ell - 1 - r + r\frac{\ell w - 1}{\ell w} + n - \ell\big)h_{n-\ell} = \frac{1}{n}\big(n - 1 - \frac{r}{\ell w}\big)h_{n-\ell} =$$

$$= \frac{\ell w - 1}{\ell w} h_{n-\ell} = \prod_{i=1}^{[n/\ell]} \frac{\ell i - 1}{\ell i}.$$

□

The same idea may be extended to the case of alternating groups.

Theorem 6.2. *Let $\ell \geq 2$ be an integer. Let $a_\ell(n)$, $s_\ell(n)$, $\delta_\ell(n)$ be as in Section 2. Then for all integers $n \geq 2$, we have*

$$a_\ell(n) = s_\ell(n) + \delta_\ell(n).$$

Proof. Let us specialize the power sums as before. For all $r \geq 1$, put $p_r = 1$ if $\ell \nmid r$ and $p_r = 0$ if $\ell \mid r$. By (10), we only need to show that $e_n = \delta_\ell(n)$ for $n \geq 2$. (Note that $e_0 = e_1 = 1$.)

Let us prove this latter identity by induction on n. By (12), one readily sees that this is indeed true for $2 \leq n \leq \ell - 1$. Suppose that $n = \ell w + r$ where $0 \leq r \leq \ell - 1$ and $w \geq 1$, and assume that $e_n = \delta_\ell(n)$ is true for all integers less than n. (Note that this r is different from the r in the previous paragraph.) Applying (12) again, we have

$$e_n = \frac{1}{n} \cdot \big(\sum_{j=1}^{\ell} (-1)^{j-1} p_j e_{n-j} + \sum_{j=\ell+1}^{n} (-1)^{j-1} p_j e_{n-j}\big). \tag{19}$$

If $r = 0$, then by (19) and by the induction hypothesis, we have

$$e_n = \frac{1}{n} \cdot (-1)^{\ell} \cdot \big(e_{n-\ell+1} + (n-\ell)e_{n-\ell}\big) = \frac{1}{n} \cdot (-1)^{\ell} \cdot (n - \ell + 1)e_{n-\ell} =$$

$$= (-1)^{\ell w} \cdot \frac{\ell(w-1)+1}{\ell w} \cdot \prod_{i=1}^{w-1} \frac{(\ell(i-1)+1}{\ell i} = \delta_\ell(n).$$

If $r = 1$, then by (19) and the induction hypothesis we see that

$$e_n = \frac{1}{n} \cdot \big(e_{n-1} + (-1)^{\ell}(n-\ell)e_{n-\ell}\big).$$

From this we get

$$e_n = \frac{(-1)^{\ell}(n-\ell)}{n-1} \cdot (-1)^{\ell(w-1)} \cdot \prod_{i=1}^{w-1} \frac{\ell(i-1)+1}{\ell i} = \delta_\ell(n).$$

Finally, if $2 \leq r \leq \ell - 1$, then by (19) again, we see that

$$e_n = \frac{1}{n} \cdot \left(0 + (-1)^{\ell} \cdot (n-\ell) e_{n-\ell}\right) = 0.$$

□

We have a debt: to show the identity (8) for $r \geq 2$. Notice that by (9), the absolute value of the right-hand-side of (8) is $c(S_n) = h_n$ after specializing the power sums $p_t = 1/\ell$ for all $t > 0$. Hence (11) specializes to $h_w = \frac{1}{w\ell} \sum_{t=1}^{w} h_{w-t}$ for all $w > 0$ where $h_0 = 1$ as usual. Finally, easy induction shows that $h_w = (-1)^{w\ell} \delta_\ell(n)$.

7 Further extensions

Since the proportion of fixed-point-free elements and the proportion of ℓ-regular elements have a 'nice' form, we proceed to introduce the following definitions.

Let $\ell \geq 2$ be an integer, and let H be a set of positive integers divisible by ℓ. A permutation (of finite order) is H-regular if no cycle (in its disjoint cycle decomposition) has length equal to h for all $h \in H$. For example, if H is the set of all positive integers divisible by ℓ, then a permutation is H-regular if and only if it is ℓ-regular.

As before, write $n \geq \ell$ in the form $n = \ell w + r$ for some integers $w \geq 1$ and $0 \leq r \leq \ell - 1$. Now consider the generalized symmetric group, $Z_\ell \wr S_w$. Let $H(\ell)$ be the set $\{h/\ell : h \in H\}$. We say that an element $(a_1, \ldots, a_w)\sigma$ of $Z_\ell \wr S_w$ is $H(\ell)$-regular if for all $h \in H(\ell)$, the product of the a_i's corresponding to each cycle of σ of length h is different from 1. Recall that the irreducible characters of $Z_\ell \wr S_w$ are naturally labelled by ℓ-quotients. For irreducible characters ψ_{β_λ}, ψ_{β_μ} of $Z_\ell \wr S_w$, define $\langle \psi_{\beta_\lambda}, \psi_{\beta_\mu} \rangle_{H(\ell)}$ to be

$$\frac{1}{\ell^w w!} \sum \psi_{\beta_\lambda}(g) \cdot \psi_{\beta_\mu}(g^{-1})$$

where the sum is over $H(\ell)$-regular elements g of $Z_\ell \wr S_w$.

It is easy to see that Frobenius reciprocity holds even in this more general situation. (See formulas (3), (4), and Proposition 8.1.) If $\mathcal{C}$ denotes the set of all H-regular elements in S_n and $K \leq G \leq S_n$ are permutation groups of degree n, then we have

$$\langle Ind_K^G(\alpha), \beta \rangle_{\mathcal{C} \cap K} = \langle \alpha, Res_K^G(\beta) \rangle_{\mathcal{C}}$$

for arbitrary class functions α of K and β of G. For simplicity, we will write $\langle \alpha, \beta \rangle_H$ instead of $\langle \alpha, \beta \rangle_{\mathcal{C}}$ for arbitrary class functions α, β of a given group. By induction on $|H|$, the inclusion-exclusion principle and the Murnaghan-Nakayama rule, it is also possible to show that if λ and μ are partitions of n with different ℓ-cores, then $\langle \chi_\lambda, \chi_\mu \rangle_H = 0$. (See [14] for details.) This implies the following. Let $s_H(n)$ and $a_H(n)$ be the proportions of H-regular elements in

S_n and A_n, respectively. Let $n = \ell w + r$ be as above. By Frobenius reciprocity (see Proposition 8.1), we see that

$$a_H(n) = \langle 1_{A_n}, 1_{A_n}\rangle_H = \langle Ind_{A_n}^{S_n}(1_{A_n}), 1_{S_n}\rangle_H =$$

$$\langle \chi_{(n)} + \chi_{(1^n)}, \chi_{(n)}\rangle_H = s_H(n) + \langle \chi_{(1^n)}, \chi_{(n)}\rangle_H.$$

Define $\delta_{H,\ell}(n)$ to be $\langle \chi_{(1^n)}, \chi_{(n)}\rangle_H$. If $r \geq 2$, then $\delta_{H,\ell}(n) = 0$, since then the partitions (n) and (1^n) have different ℓ-cores.

From the above observations, the following theorem is not very surprising. Let $p_{H(\ell)}(w)$ be the proportion of $H(\ell)$-regular elements in $Z_\ell \wr S_w$.

Theorem 7.1. *With the notations above, there exists a function $\delta_{H,\ell}(n)$ such that*

$$a_H(n) = p_{H(\ell)}(w) + \delta_{H,\ell}(n) = s_H(n) + \delta_{H,\ell}(n)$$

with $\delta_{H,\ell}(n) = 0$ whenever $r \geq 2$.

Notice that the theorem also states that

$$s_H(\ell w) = s_H(\ell w + 1) = \ldots = s_H(\ell w + \ell - 1)$$

for all $w \geq 0$. This may be shown by induction on $|H|$ and by the inclusion-exclusion principle as in [14]. The existence and the property of the function $\delta_{H,\ell}(n)$ follow from the remark made before the statement of the theorem. Hence to verify Theorem 7.1, we only need to show the following. (For an alternative proof using characters, see [14].)

Lemma 7.1. *For all integers $w > 0$, we have $s_H(w\ell) = p_{H(\ell)}(w)$.*

Proof. For convenience, put $h_{w\ell} := s_H(w\ell)$ and $h^*_w := p_{H(\ell)}(w)$ for all $w > 0$. Also, for each non-negative integer j, put $h_{j\ell} = h_{j\ell+1} = \ldots = h_{j\ell+\ell-1}$. Furthermore, define h_0 and h^*_0 to be 1.

Put $K = Z_\ell \wr S_w$. Notice that 1_K is an S_w-stable character in K. Similarly, as in formula (7) (see also Page 543 of [12]), we see that

$$h^*_w = p_{H(\ell)}(w) = \langle 1_K, 1_K\rangle_{H(\ell)} = \frac{1}{w!}\sum_{\sigma\in S_w}((\ell-1)/\ell)^{v(\sigma)},$$

where $v(\sigma)$ is the number of cycles of σ of lengths belonging to H. This gives the recurrence relation

$$h^*_w = \frac{1}{w\ell}\cdot\Big(\sum_{\substack{i=1\\ i\notin H(\ell)}}^{w} \ell\cdot h^*_{w-i} + \sum_{\substack{i=1\\ i\in H(\ell)}}^{w} (\ell-1)\cdot h^*_{w-i}\Big). \tag{20}$$

Let us prove $h^*_w = h_{w\ell}$ by induction on w. By inspection, this is true for $w = 0$ and also for $w = 1$. Suppose that $h_{j\ell} = h^*_j$ holds for all non-negative integers $j < w$. By (20) and by the induction hypothesis, we see that

$$h^*_w = \frac{1}{w\ell}\cdot\Big(\sum_{i=1}^{w\ell} h_{w\ell-i} - \sum_{\substack{i=1\\ i\in H}}^{w\ell} h_{w\ell-i}\Big) = \frac{1}{w\ell}\cdot\sum_{\substack{i=1\\ i\notin H}}^{w\ell} h_{n-i} = h_{w\ell},$$

which is exactly what we wanted.

∎

The proof of Theorem 7.1 is complete.

These results give us hope to generalize the theory of generalized blocks for symmetric groups. Let H be a set of positive integers. Let the greatest common divisor of all elements in H be $\ell \geq 2$. We use the truncated inner product across H-regular elements to define a graph on $Irr(S_n)$. We join the distinct vertices χ_λ and χ_μ by an undirected edge, if and only if, $\langle \chi_\lambda, \chi_\mu \rangle_H \neq 0$. The (sets of vertices of the) connected components of this graph are called the H-linked blocks of S_n. Notice that if H is the set of all positive integers divisible by ℓ, then H-linked blocks are the same as ℓ-linked blocks. In [14] the following was proved.

Theorem 7.2 ([14])**.** *Let $\ell \geq 2$ be an arbitrary integer. Let H be a set of positive integers so that the greatest common divisor of all elements in H is ℓ. Then H-linked blocks and combinatorial ℓ-blocks are the same for S_n.*

If H is the set of all multiples of ℓ, then Theorem 7.2 reduces to Theorem 5.2. Furthermore, if we additionally assume that ℓ is a prime, then we obtain the Nakayama conjecture.

An analogue of Theorem 5.3 is also true.

Theorem 7.3 ([14])**.** *Let us use the notations of Theorem 5.3. If H is an arbitrary set of positive integers divisible by $\ell \geq 2$, then*

$$\langle \chi_\lambda, \chi_\mu \rangle_H = \langle \sigma_\lambda \psi_{\beta_\lambda}, \sigma_\mu \psi_{\beta_\mu} \rangle_{H(\ell)}$$

where the latter truncated inner product is across $H(\ell)$-regular elements of $Z_\ell \wr S_w$.

We note that the proof of this theorem is shorter and more elementary than the proof of Theorem 5.3. Finally, Theorem 5.12 of [12], which was used in this paper to perform calculations in the generalized symmetric group (see formula (7)), can also be extended to the case of $H(\ell)$-regular elements. (See Theorem 5.2 of [14].)

8 On average numbers of fixed points

Let Ω be the set of all positive integers. Let S_Ω be the group of all permutations of Ω. For each integer $n > 0$, let S_n be the finite permutation group on the set $\{1, \dots n\}$ (fixing all other integers). Let $\mathcal{C}$ be a subset of S_Ω such that for all $n > 0$ the set $\mathcal{C} \cap S_n$ is a union of certain conjugacy classes of S_n. (The sets involved in (13)-(18) may be thought of such sets, $\mathcal{C}$.)

Proposition 8.1 (Frobenius reciprocity)**.** *Let α be a class function of the symmetric group S_n, and let β be a class function of S_{n-1}. With the notations of Section 3 we have*

$$\langle \alpha, Ind_{S_{n-1}}^{S_n}(\beta) \rangle_{\mathcal{C} \cap S_n} = \langle Res_{S_{n-1}}^{S_n}(\alpha), \beta \rangle_{\mathcal{C} \cap S_{n-1}}.$$

For a proof, one can modify the argument of the proof of the usual Frobenius reciprocity found on Pages 62-63 of [9].

Let $\mathcal{C}$ be as above. By following the notation of Section 6, for each integer $n > 0$, define $h_n(\mathcal{C})$ to be $|\mathcal{C} \cap S_n|/n!$. A direct consequence of Proposition 8.1 is the following.

Proposition 8.2. *The the average number of fixed points on the set* $\{1,\ldots,n\}$ *of elements of* $\mathcal{C}\cap S_n$ *is* $h_{n-1}(\mathcal{C})/h_n(\mathcal{C})$.

Proof. By Frobenius reciprocity (Proposition 8.1), the average number of fixed points on the set $\{1,\ldots,n\}$ of elements of $M\cap S_n$ is

$$(h_n(M))^{-1}\langle 1_{S_n}, Ind_{S_{n-1}}^{S_n}(1_{S_{n-1}})\rangle_{M\cap S_n} =$$
$$= (h_n(M))^{-1}\langle 1_{S_{n-1}}, 1_{S_{n-1}}\rangle_{M\cap S_{n-1}} = h_{n-1}(M)/h_n(M).$$

□

Let $\ell\geq 2$ be an arbitrary integer, and let H be a set of positive integers divisible by ℓ. From now on, let $\mathcal{C}$ denote any of the following subsets of S_Ω: the set of ℓ-regular elements, the set of H-regular elements (see the previous section for the definition), the set of ℓ-th powers of elements, the set of elements with orders dividing ℓ, or the set of elements with orders equal to ℓ.

The main result of this section is the following.

Theorem 8.1. *(1) The average number of fixed points of ℓ-regular elements of S_n is 1 if $\ell\nmid n$ and is $n/(n-1)$ if $\ell|n$.*

(2) The average number of fixed points of ℓ-th powers of elements of S_n tends to 1 as n tends to infinity.

(3) The average number of fixed points of elements with orders dividing ℓ is asymptotically equal to $n^{1/\ell}$ as n tends to infinity.

(4) The average number of fixed points of elements with orders equal to ℓ is asymptotically equal to $n^{1/\ell}$ as n tends to infinity.

Theorem 2.1 and Proposition 8.2 yields (1) of Theorem 8.1.

If $\mathcal{C}$ is the set of ℓ-th powers of elements of S_Ω, then by a result of [15], we have $|\mathcal{C}\cap S_n|\sim An!n^{(\phi(\ell)/\ell)-1}$ as n tends to infinity, where A is some constant and ϕ is Euler's function. This observation together with Proposition 8.2 yields (2) of Theorem 8.1.

Let $\mathcal{C}_\ell$ be the set of all permutations of S_Ω with orders dividing ℓ. By a result of [19] we have the following.

$$h_n(\mathcal{C}_\ell)\sim\frac{\tau^n}{\sqrt{2\pi\ell n}}\quad \exp(\sum_{d|\ell}\frac{1}{d\tau^d}),$$

where

$$\tau=\tau(\ell,n)=n^{-1/\ell}\Big(1+\frac{1}{\ell n}\sum_{\substack{d|\ell\\ d<\ell}}n^{d/m}+\epsilon(\ell,n)\Big),$$

and $\epsilon(\ell,n)=(2\ell^2n)^{-1}$ if ℓ is even and $\epsilon(\ell,n)=0$ if ℓ is odd. From this, we may deduce that $h_{n-1}(M_\ell)/h_n(M_\ell)$ is asymptotically equal to

$$o(1)\frac{\tau(\ell,n-1)^{n-1}}{\tau(\ell,n)^n}\exp\Big(\sum_{d|\ell}\frac{1}{d(\tau(\ell,n-1))^d}-\frac{1}{d(\tau(\ell,n))^d}\Big)\quad\sim$$

$$\sim \quad o(1)(en)^{1/\ell} \exp\Big(\sum_{d|\ell} \frac{1}{d(\tau(\ell,n-1))^d} - \frac{1}{d(\tau(\ell,n))^d}\Big) \quad \sim$$

$$\sim \quad o(1)(en)^{1/\ell} \exp(-1/\ell) = o(1) \cdot n^{1/\ell}$$

not depending on whether ℓ is even or odd. This gives (3) of Theorem 8.1.

Now let $\mathcal{C'}_\ell$ be the set of all permutations of S_Ω with orders equal to ℓ. To show (4) of Theorem 8.1, it is sufficient to see that

$$h_{n-1}(\mathcal{C'}_\ell)/h_n(\mathcal{C'}_\ell) \sim h_{n-1}(\mathcal{C}_\ell)/h_n(\mathcal{C}_\ell). \tag{21}$$

Let $\ell = {p_1}^{k_1} \dots {p_t}^{k_t}$ where the p_i's are distinct prime powers and the k_i's are positive. Let $\mathcal{S} = \{p_1, \dots, p_t\}$. For any subset A of $\mathcal{S}$, define $\Pi(A)$ to be ℓ divided by the product of all primes in A. Put $\Pi(\emptyset) = \ell$. Little inspection yields

$$h_n(\mathcal{C'}_\ell) = \sum_{A \subseteq \mathcal{S}} (-1)^{|A|} h_n(\mathcal{C}_{\Pi(A)}). \tag{22}$$

By Proposition 8.2 and by part (3) of Theorem 8.1, it follows that the right-hand-side of (22) is asymptotically equal to $o(1)h_n(\mathcal{C}_\ell)$ as n tends to infinity.

Hence (21) readily follows.

Acknowledgements

The author thanks G. R. Robinson for conversations on this topic, and is grateful to L. Pyber and E. Bertram for drawing his attention to the papers [1] and [5] respectively. The research was mainly supported by the School of Mathematics and Statistics of the University of Birmingham, U.K., by NSF Grant DMS 0140578, and by OTKA T049841.

References

[1] Beals, R.; Leedham-Green, C. R.; Niemeyer, A. C.; Praeger, C. E.; Seress, Á. Permutations with restricted cycle structure and an algorithmic application. *Combin. Probab. Comput.* **11** (2002), no. 5, 447–464.

[2] Bertram, E. A.; Gordon, B. Counting special permutations. *European J. Combin.* **10** (1989), no. 3, 221–226.

[3] Bolker, E. D.; Gleason, A. M. Counting permutations. *J. Combin. Theory Ser. A* **29** (1980), no. 2, 236–242.

[4] Bóna, M.; McLennan, A.; White, D. Permutations with roots. *Random Structures Algorithms* **17** (2000), no. 2, 157–167.

[5] Chernoff, W. W. Permutations with p^l-th roots. 13th British Combinatorial Conference (Guildford, 1991). *Discrete Math.* **125** (1994), no. 1-3, 123–127.

[6] Erdős, P.; Turán, P. On some problems of a statistical group-theory. II. *Acta math. Acad. Sci. Hungar.* **18** 1967, 151–163.

[7] Glasby, S. P. Using recurrence relations to count certain elements in symmetric groups. *European J. Combin.* **22** (2001), no. 4, 497–501.

[8] Guralnick, R. M.; Tiep, P. H. The non-coprime $k(GV)$ problem, to appear in *J. Algebra*.

[9] Isaacs, I. M. Character theory of finite groups. Dover Publications, Inc., New York, 1994.

[10] Isaacs, I. M.; Kantor, W. M.; Spaltenstein, N. On the probability that a group element is p-singular. *J. Algebra* **176** (1995), no. 1, 139–181.

[11] James G., Kerber A. The representation theory of the symmetric group, Addison-Wesley 1981.

[12] Külshammer, B.; Olsson, J. B.; Robinson, G. R. Generalized blocks for symmetric groups. *Invent. math.* **151** (2003), 513-552.

[13] Macdonald, I. G. Symmetric functions and Hall polynomials. *Oxford University Press* Second edition. (1995).

[14] Maróti, A. A proof for a generalized Nakayama conjecture, submitted.

[15] Mineev, M. P; Pavlov, A. I. The number of permutations of a special form. (Russian) *Mat. Sb. (N.S.)* **99 (141)** (1976), no. 3, 468–476, 480.

[16] Robinson, G. R. Bounding numbers and heights of characters in p-constrained groups. Proceedings of the Conference "Finite Groups 2003", Gainesville, March 2003, de Gruyter (2004).

[17] Robinson, G. R. Personal communication.

[18] Stanley, R. P. Enumerative combinatorics. Vol. 2. Cambridge Studies in Advanced Mathematics, **62**. *Cambridge University Press*, Cambridge, 1999.

[19] Wilf, H. S. The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n. *Bull. Amer. Math. Soc. (N.S.)* **15** (1986), no. 2, 228–232.

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-1113, U.S.A.

E-mail address: maroti@math.usc.edu