Counting Sylow double cosets in the symmetric group

Paul Renteln

Department of Physics
California State University
San Bernardino, CA 92407
prenteln@csusb.edu

October 31, 2023; version of March 8, 2024

Abstract

An algorithm is developed for calculating the number of double cosets $P\backslash\mathfrak{S}_n/P$, where P is a Sylow-p-subgroup of the symmetric group $\mathfrak{S}_n$. Several examples of its use are given.

Keywords: Symmetric group, Sylow-p-subgroup, double cosets, cycle index, wreath product

1 Introduction

For the last several years, Persi Diaconis and his colleagues have studied random walks on the set of double cosets of a finite group (see [9] and references therein). One imediate question is, how many are there? When G is a symmetric group and H and K are parabolic subgroups, the double cosets $H\backslash G/K$ are in bijective correspondence with contingency tables, which play a central role in statistics, and which arise in many diverse areas of mathematics (see, *e.g.*, [7]). There are algorithms for computing the number of contingency tables with given fixed margins, but no closed formula, and it seems unlikely that such a formula exists. [1]

[1] For some recent work on parabolic double cosets in the symmetric group and other Coxeter groups, see [1, 2, 26].

In a recent paper [8], Diaconis *et. al.* consider instead the problem of enumerating the double cosets $P\backslash\mathfrak{S}_n/P$ of a Sylow-p-subgroup P of the symmetric group $\mathfrak{S}_n$. [2] Using sophisticated group theoretic methods including modular representation theory, they were able to obtain some very interesting results on the possible sizes of the Sylow double cosets. In the same paper they asked whether there exists a nice method of counting the number of such double cosets. We offer such a method here. Although the complexity of the algorithm increases rapidly with increasing n, it is possible to use our formula to evaluate the number of Sylow double cosets in some nontrivial cases.

To state the main result we need some notation. Every $\pi \in \mathfrak{S}_n$ can be written as a product of disjoint cycles. The *cycle type* of π (written in multiplicity notation) is $\nu = 1^{c_1(\pi)}2^{c_2(\pi)}\cdots n^{c_n(\pi)}$, where $c_i(\pi)$ is the number of cycles of π of length i. As $\sum_{i=1}^{n} ic_i(\pi) = n$, ν is a partition of n (written $\nu \vdash n$). Let s_i be indeterminates, and write $\boldsymbol{s}^{\mathbf{c}(\pi)}$ for the monomial $s_1^{c_1(\pi)}s_2^{c_2(\pi)}\cdots s_n^{c_n(\pi)}$ associated to the partition ν.

Theorem 1. *Let P be a Sylow-p-subgroup of $\mathfrak{S}_n$, and let*

$$\widetilde{Z}_P(x_1,\ldots,x_n) = \sum_{\pi\in P} \boldsymbol{s}^{\mathbf{c}(\pi)}$$

be the (augmented) cycle index *of P. Write a_ν for the coefficient of $\boldsymbol{s}^{\mathbf{c}(\pi)}$ in $\widetilde{Z}_P(s)$ associated to ν. Then the number of Sylow double cosets of $\mathfrak{S}_n$ is*

$$N_n := |P\backslash\mathfrak{S}_n/P| = \frac{1}{p^{2\,\mathrm{ord}_p(n!)}} \sum_{\nu\vdash n} a_\nu^2 z_\nu, \tag{1}$$

where z_ν is the order of the centralizer of a permutation having cycle type ν, and $\mathrm{ord}_p(n!)$ *is the highest power of p dividing $n!$.*

We prove Theorem 1 and provide some examples of its use in Section 3.

2 Preliminaries

In this section we collect some results that will be needed in the proof of Theorem 1.

[2] Recall that, if p is prime, a *p-group* is a group having order equal to the power of a prime. A *Sylow-p-subgroup* of G is a maximal p-subgroup of G. By the Sylow theorems, a Sylow-p-subgroup exists for every prime factor of the order of G.

2.1 Permutation Groups

First, we recall some well-known facts from the theory of permutation groups. [3] Let G be a group acting transitively on a set X. An *orbital* of G on X is a diagonal orbit of G on $X \times X$. That is, for $x, y \in X$,

$$\mathrm{orb}(x, y) = \{(gx, gy) : g \in G\}.$$

The number of orbitals is the *rank* of G, written $\mathrm{rk}\, G$.

Theorem 2. *Let $H = G_x$ be the stabilizer of the point $x \in X$. Then the rank of G equals the number of double cosets $H\backslash G/H$.*

Proof. See, *e.g.*, [13], 4.8, or [14], Prop. 1.6.2. □

Although the following proposition can be derived using character theory (see, *e.g.*, [14], Propositions 6.2.10 and 6.2.11) it is a simple matter to provide a direct proof. As the result in this form is difficult to find in the textbooks, we supply a proof here.

Theorem 3. *Let H be a subgroup of G, and let $\mathcal{C}$ denote the set of conjugacy classes of G. Then*

$$|H\backslash G/H| = \frac{|G|}{|H|^2} \sum_{C \in \mathcal{C}} \frac{|C \cap H|^2}{|C|}.$$

Proof. By the lemma that is not Burnside's [24], the number of orbitals of G on G/H is the average number of pairs (aH, bH) fixed by the diagonal action of G. Therefore, we may write

$$\mathrm{rk}\, G = \frac{1}{|G|} \sum_{g \in G} \mathrm{fix}(g)^2.$$

where

$$\mathrm{fix}(g) := |\{aH : gaH = aH\}| = |\{aH : a^{-1}ga \in H\}|.$$

As the condition $gaH = aH$ is manifestly independent of the coset representative a, so too is the condition $a^{-1}ga \in H$. Each coset has $|H|$ representatives, so we can write

$$\mathrm{fix}(g) = \frac{1}{|H|} |\{a \in G : a^{-1}ga \in H\}|.$$

[3] See, *e.g.*, [4], [28], [38].

Thus, we must count the number of conjugates of g that lie in H. If C is the conjugacy class of g, this number is not simply $|C \cap H|$, because many different conjugates of g coincide. Indeed, the stabilizer of the conjugacy action of G on g is the centralizer $C_G(g)$ of g in G, so

$$|\{a \in G : a^{-1}ga \in H\}| = |C_G(g)||C \cap H| = \frac{|G||C \cap H|}{|C|}.$$

Hence

$$\operatorname{rk} G = \frac{|G|}{|H|^2} \sum_{g \in G} \left(\frac{|C \cap H|}{|C|} \right)^2 = \frac{|G|}{|H|^2} \sum_{C \in \mathcal{C}} \frac{|C \cap H|^2}{|C|}. \qquad \square$$

2.2 Wreath products

It is an old result of Kalužnin (see Section 2.5 below) that the Sylow-p-subgroups of the symmetric group are Cartesian products of wreath product groups. There are many different wreath products in the literature, so it is important to specify what type of wreath product we will be using here. [4] As wreath products are best understood in terms of trees, we spend a little more time than is strictly necessary for our ultimate aim discussing the relationship between trees and wreath products.

Let A be a permutation group acting on an n-set X, and let B be a permutation group acting on an m-set Y. From these data we construct a permutation group $A[B]$ on $X \times Y$, called the *wreath of A around B*, or the *wreath product $B \wr A$* of B with A. To every $a \in A$ and every function $\sigma : X \to B$ we associate a permutation $(a; \sigma)$ of $X \times Y$ by

$$(a; \sigma)(x, y) = (ax, \sigma(x)y). \tag{2}$$

At this point it is not even obvious that this defines a group. To see this, observe that, by (2),

$$(a; \sigma)(b; \tau)(x, y) = (a; \sigma)(bx, \tau(x)y) = (abx, \sigma_b(x)\tau(x)y).$$

[4] We will use the so-called *permutational* or *imprimitive* wreath product. See Rotman [33] pp. 172ff. See also Dixon and Mortimer ([11], Section 2.6). The permutational wreath product was used to great effect by Pólya [29] (although wreath products appeared earlier in the literature). Pólya referred to it as the *Kranz*. In Read's translation of Pólya's paper [30] it is called the *corona*. Huppert [17], Sec. 15) calls it the *Kranzprodukte*. One of the clearer expositions can be found in the work of de Bruijn [6]. Some other discussions of wreath products include ([14], Sec. 1.5), ([15], p. 164), [16], ([28], Sec. 2), and ([32], pp. 41ff).

where

$$\sigma_b(x) := \sigma(bx). \tag{3}$$

So, in order to construct a group out of the maps $(a;\sigma)$, we are led to define

$$(\sigma\tau)(x) := \sigma(x)\tau(x), \tag{4}$$

so that

$$(a;\sigma)(b;\tau) = (ab;\sigma_b\tau). \tag{5}$$

That is, we must first turn B^X (the set of all maps from X to B) itself into a group using componentwise multiplication. Effectively, we are defining B^X to be the Cartesian product of n copies of B. The group $A[B]$ has $|A||B|^n$ elements. [5]

To show that $A[B]$ is indeed a group, we need an identity element, inverse elements, and associativity for the product (5). The identity element is clearly $(1;1) := (1_A; 1_{B^X})$, where $1_{B^X}(x) = 1_B$. Also, if we define σ^{-1} by $\sigma^{-1}(x) := (\sigma(x))^{-1}$, then

$$(a;\sigma)^{-1} = (a^{-1};\sigma^{-1}_{a^{-1}}).$$

Lastly,

$$(a;\sigma)[(b;\tau)(c;\upsilon)] = (a;\sigma)(bc;\tau_c\upsilon) = (abc;\sigma_{bc}\tau_c\upsilon)$$

while

$$[(a;\sigma)(b;\tau)](c;\upsilon) = (ab;\sigma_b\tau)(c;\upsilon) = (abc;(\sigma_b\tau)_c\upsilon) = (abc;\sigma_{bc}\tau_c\upsilon),$$

so the product (5) is associative.

[5] In many sources the wreath product $B \wr A$ is defined as follows. Start with a group B and a subgroup $A \leq \mathfrak{S}_n$. Define an action of A on $B^n = B \times \cdots \times B$ (n times) by

$$\boldsymbol{b} := (b_1, \ldots, b_n) \mapsto \boldsymbol{b}^a := (b_{a^{-1}(1)}, \ldots, b_{a^{-1}(n)}) \qquad a \in A.$$

Then the *wreath product group* $B \wr A$ is the set $B^n \times A$ equipped with the binary operation

$$(\boldsymbol{b}_1; a_1)(\boldsymbol{b}_2; a_2) := (\boldsymbol{b}_1\boldsymbol{b}_2^{a_1}; a_1a_2).$$

where the product in the first entry is defined componentwise. This group is isomorphic to $A[B]$. In $B \wr A$ we identify $B^n \cong \{(\boldsymbol{b};1)\}$, and $A \cong \{(1;a)\}$. Then B^n is normal in $B \wr A$, which means we can think of $B \wr A$ as the semidirect product of B^n by A (with the above action). The order of the group is $|B|^n|A|$. The problem with this definition is that it is a bit too general for our purposes, as B need not be a permutation group.

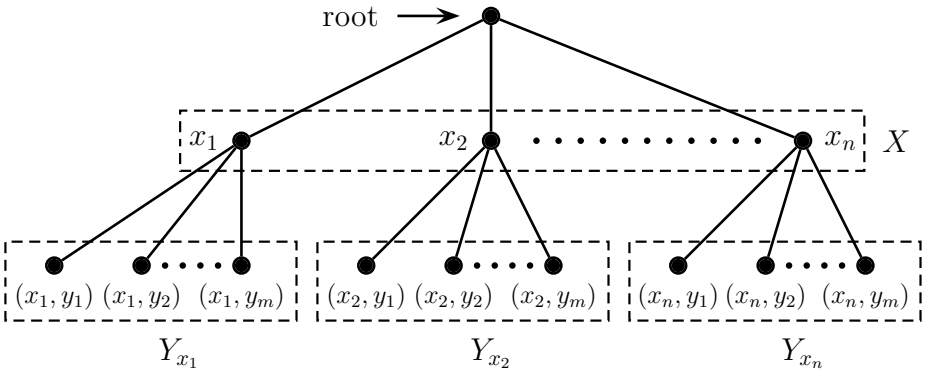

Figure 1: A rooted tree

2.3 Wreath products as automorphism groups of trees

Although the definition of the wreath product given above is clean, it is not very intuitive. The best way to understand the wreath product is as a set of automorphisms of a certain kind of tree. [6] Consider the rooted tree T illustrated in Figure 1. The root has n children, which we identify with the elements of an n-set X. Each node $x \in X$ has m children, labeled Y_x, where each Y_x is a copy of an m-set Y. In particular, the leaves of the tree can be labeled by the pairs (x, y), where $x \in X$ and $y \in Y$, and so identified with the Cartesian product $X \times Y$. Let A be a permutation group acting on X, and let B be a permutation group acting on Y.

Theorem 4. *(See, e.g., [33], pp. 174-175) Let G be the subgroup of the automorphism group of T that fixes the root, permutes the vertices of X according to an element $a \in A$, and sends the vertices of Y_x to the vertices of Y_{ax} according to some element of B. Then, viewed as a permutation group on the leaves of T, G is precisely the wreath product $A[B]$.*

Proof. For every $g \in G$ and $(x, y) \in X \times Y$ we have

$$g(x, y) = (ax, \sigma(x)y).$$

This is precisely the action of the wreath product $A[B]$ on $X \times Y$. □

[6] See, *e.g.*, [25] or ([33], pp. 174-175). For undefined graph theoretic nomenclature, see [15].

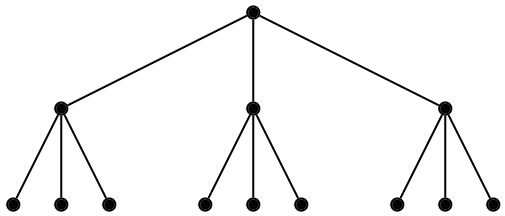

Figure 2: A simple rooted tree.

For instance, the wreath product $G := \mathbb{Z}_3 \wr \mathbb{Z}_3$ may be viewed as a subgroup of the automorphism group of the tree in Figure 2. The group G cyclically permutes the nodes at depth 1 and, independently, cyclically permutes the nodes at depth 2. If we were to label the leaves by the integers 1 to 9 in order, then the group $\mathbb{Z}_3 \wr \mathbb{Z}_3$ would be generated by the permutations

$$(123), (456), (789), (147)(258)(369).$$

In this way, $\mathbb{Z}_3 \wr \mathbb{Z}_3$ is naturally a subgroup of $\mathfrak{S}_9$.

Next we show that the wreath product is associative. [7]

Theorem 5. *Let A, B, and C be permutation groups acting on sets X, Y, and Z, respectively. Let $S := X \times Y \times Z$. Then $A[B[C]] \cong (A[B])[C]$ (equivalently, $(C \wr B) \wr A \cong C \wr (B \wr A))$) as permutation groups of S. That is, the wreath product is associative.*

Proof. It is easiest to see this by examining the rooted tree T, shown schematically in Figure 3. Using the construction of Theorem 4, one simply observes that the automorphism subgroups $A[B[C]]$ and $(A[B])[C]$ act in precisely the same way on the leaves of T. (One imagines constructing T in two ways: first, by forming the tree associated to $X \times Y$, then attaching copies of the Z's, and second, by forming the tree with X, then attaching copies of the $Y \times Z$ tree.) More explicitly, we first identify triples of $X \times Y \times Z$:

$$(x, (y, z)) \leftrightarrow (x, y, z) \leftrightarrow ((x, y), z). \tag{6}$$

[7] As previously mentioned, there are different, inequivalent, notions of a 'wreath product' in the literature. For example, in addition to the permutational wreath product that we have defined here, Rotman ([33], pp. 172ff) also defines the so-called *regular wreath product*. The regular wreath product is not associative.

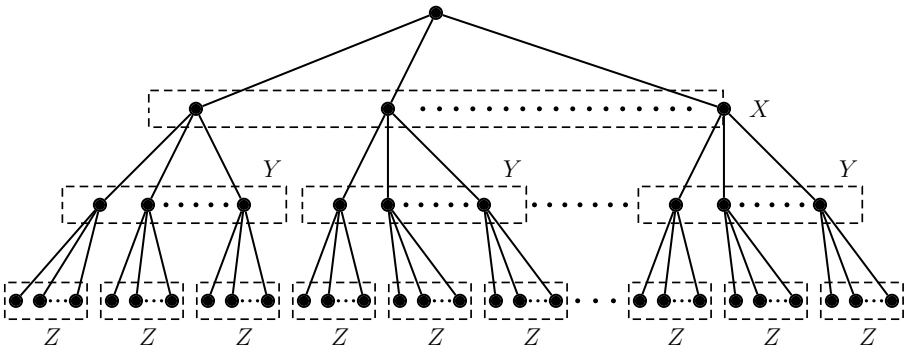

Figure 3: Schematic of the rooted tree illustrating Theorem 5.

Elements of $A[B[C]]$ are of the form $(a;\tau)$, where $a \in A$, and $\tau \in B[C]^X$. Their action on points of S is given by

$$\begin{aligned}(a;\tau)(x,y,z) &= (a;\tau)(x,(y,z)) \\ &= (ax,\tau(x)(y,z)) \\ &= (ax,(\beta(x)y,\gamma(x,y)z)) \\ &= (ax,\beta(x)y,\gamma(x,y)z),\end{aligned}$$

where $\beta(x) \in B^X$ and $\gamma(x,y) \in C^{X\times Y}$. Elements of $(A[B])[C]$ are of the form $((a;\beta);\gamma)$, where $a \in A$, $\beta \in B^X$, and $\gamma \in C^{X\times Y}$. Their action on points of S is given by

$$\begin{aligned}((a;\beta);\gamma)(x,y,z) &= ((a;\beta);\gamma)((x,y),z) \\ &= ((a;\beta)(x,y),\gamma(x,y)z) \\ &= ((ax,\beta(x)y),\gamma(x,y)z) \\ &= (ax,\beta(x)y,\gamma(x,y)z).\end{aligned}$$

□

Remark. Modulo the identification (6), the two groups $(C \wr B) \wr A$ and $C \wr (B \wr A)$ are not merely isomorphic, but are essentially the same permutation group acting on $X \times Y \times Z$.

2.4 The cycle index

In his monumental paper on the enumeration of various chemical compounds, Pólya [29] (see also [30]) introduced and employed the notion of the *cycle index* of a permutation

group. It has become an essential tool for the enumeration of combinatorial objects with symmetries, and it has been generalized in many directions. [8] We recall a few facts here.

Let G be a permutation group acting on a set X with $|X| = n$. We may view G as a subgroup of $\mathfrak{S}_n$, so that every element of G has a cycle decomposition. Let $c_i(g)$ be the number of cycles of length i of g, and let s_i be indeterminates. Write $\boldsymbol{s}^{\boldsymbol{c}(g)}$ for the monomial $s_1^{c_1(g)} s_2^{c_2(g)} \cdots s_n^{c_n(g)}$. Then the *cycle index* of G is

$$Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} \boldsymbol{s}^{\boldsymbol{c}(g)}.$$

It is important to note that the cycle index depends on the specific representation of G as a permutation group, as isomorphic groups can give rise to different cycle indices. [9]

Pólya showed that one can obtain the cycle index of various composite groups from the cycle indices of their constituents. Suppose that A and B be permutation groups on disjoint sets X and Y, respectively.

Theorem 6. *(Pólya [29]) The cycle index of the Cartesian product $A \times B$ acting as a permutation group of $X \times Y$ is given by*

$$Z_{A \times B}(s) = Z_A(s) Z_B(s).$$

Proof. Every $g \in A \times B$ is of the form (a, b) for $a \in A$ and $b \in B$. The group elements a and b act independently on their respective sets, so $\boldsymbol{s}^{c((a,b))} = \boldsymbol{s}^{c(a)} \boldsymbol{s}^{c(b)}$. As $|A \times B| = |A||B|$, the result follows. □

Theorem 7. *(Pólya [29]) The cycle index of the wreath product $A[B]$ acting as a permutation group of $X \times Y$ is given by*

$$Z_{A[B]}(s_1, s_2, s_3, \ldots) = Z_A(t_1, t_2, t_3, \ldots), \quad \textit{where} \quad t_k := Z_B(s_k, s_{2k}, s_{3k}, \ldots).$$

Proof. The proof requires a careful consideration of the cycle structure of the permutations $(a; \sigma)$. For the details, see *e.g.*, ([3], Prop. 15.5.2) or ([6], Theorem 5.5). □

[8] The cycle index and its uses were anticipated by Redfield [31], so the associated theory is often called *Pólya-Redfield theory*. It is discussed in most combinatorics and many group theory texts. See, *e.g.*, Cameron [3], de Bruijn [6], Grove [14], Harary [15], Harary and Palmer [16], Merris [22], Palmer and Robinson [27], Stanley [35, 36], and van Lint and Wilson [37].

[9] The standard example is $H_1 := \{1, (12), (34), (12)(34)\}$, with cycle index $Z_1 = (1/4!)(s_1^4 + 2s_1^2 s_2 + s_2^2)$ and $H_2 := \{1, (12)(34), (13)(24), (14)(23)\}$, with cycle index $Z_2 = (1/4!)(s_1^4 + 3s_2^2)$. The groups are isomorphic, but the cycle indices are different.

This theorem was used by Pólya to enumerate various chemical compounds, and was used by Harary, Palmer, Robinson and others to enumerate different classes of graphs. It is related to the concept of plethysm in symmetric function theory (*e.g.,* [35]). We will use it to obtain the cycle indices of iterated wreath products.

2.5 Sylow-p-subgroups of the symmetric group

Let p be a prime. The Sylow-p-subgroups of the symmetric groups $\mathfrak{S}_p$ are all isomorphic to $\mathbb{Z}_p$, for the only power of p dividing $p!$ is p itself, and the only groups of prime order are the cyclic ones. Clearly, these are simply the subgroups generated by a p-cycle. But already the Sylow-p-subgroups of $\mathfrak{S}_{p^2}$ are a little tricky, and those of $\mathfrak{S}_n$ more so. The general answer was supplied by Kalužnin [19]. [10]

Let $\mathbb{Z}_p$ be the cyclic subgroup of order p. Define the *iterated wreath product* [11]

$$W_{m,p} := \underbrace{\mathbb{Z}_p \wr \mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p}_{m \text{ times}},$$

where $W_{m+1,p} := W_{m,p} \wr \mathbb{Z}_p$ and $W_{0,p} := 1$. We understand this to be the permutational wreath product defined in Section 2.2, so by Theorem 5, we can drop any parentheses. If $X = \{1, 2, \ldots, p\}$ then $W_{m,p}$ acts on X^m, so it may be viewed as a subgroup of $\mathfrak{S}_{p^m}$. By a simple inductive argument, we see that $W_{m,p}$ has order $p^{\mu(m)}$, where

$$\mu(m) = p^{m-1} + p^{m-2} + \cdots + 1 = \frac{p^m - 1}{p - 1}.$$

As with general wreath products, the iterated wreath product $W_{m,p}$ is best understood as the group of automorphisms of a rooted tree. An *r-tree* is just a tree consisting of one root with r children. The *complete r-ary tree of depth m* is the rooted tree constructed inductively by attaching r-trees to the leaves of the complete r-ary tree of depth $m-1$, where the complete r-ary tree of depth zero is just a single node. For instance, the tree

[10] Kalužnin is also transliterated as Kaluzhnin and Kaloujnine. Actually, the existence of the Sylow subgroups of the symmetric group (that is, subgroups having the requisite order) was observed about a century earlier by Cauchy [5] (who obviously did not call them Sylow subgroups). See also Miller [23] and Findlay [12]. Modern treatments can be found in Grove ([14], Section 2.3), Kalužnin *et. al.* [20], Robinson ([32], Theorem 1.6.19), or Rotman ([33], pp. 176-177). For some recent work on Sylow subgroups of the symmetric group, see Im and Oğuz [18] and references therein.

[11] For more about iterated wreath products of cyclic groups, see Orellana *et. al.* [25].

in Figure 2 is a complete 3-ary tree of depth 2. The iterated wreath product $W_{m,p}$ can therefore be viewed as the subgroup of a complete p-ary tree of depth m generated by cyclic permutations of the nodes of the subtrees at each level. Because the nodes are only allowed to be permuted cyclically, a better structure to represent $W_{m,p}$ might be something more akin to a mobile, in which one hangs p-gons from each node. In any case, with the scene now set, we can state Kalužnin's theorem.

Theorem 8. *(Kalužnin, [19]) Let p be a prime.*

- *A Sylow-p-subgroup of $\mathfrak{S}_{p^m}$ is isomorphic to an iterated wreath product $W_{m,p}$.*
- *Let*

$$n = a_0 + a_1 p + \cdots + a_r p^r$$

be the p-adic expansion of n. Then a Sylow-p-subgroup of $\mathfrak{S}_n$ is isomorphic to the direct product

$$P := W_{0,p}^{a_0} \times W_{1,p}^{a_1} \times W_{2,p}^{a_2} \times \cdots \times W_{r,p}^{a_r}. \tag{7}$$

Proof. By the Sylow theorems, it suffices to show that P is a subgroup of $\mathfrak{S}_n$ having the correct order. Recall that the p-adic valuation $\mathrm{ord}_p(n!)$ is the highest power of p dividing $n!$. By an old result of Legendre [21],

$$\mathrm{ord}_p(n!) = \sum_k \left\lfloor \frac{n}{p^k} \right\rfloor.$$

where $\lfloor x \rfloor$ is the least integer greater than or equal to x. Note that

$$\left\lfloor \frac{n}{p^k} \right\rfloor = a_k + a_{k+1} p + \cdots + a_r p^{r-k},$$

because $1 \leq a_i < p$ for all i. Hence,

$$\begin{aligned} \mathrm{ord}_p(n!) &= a_1 + a_2(1+p) + a_3(1+p+p^2) + \cdots + a_r(1+p+\cdots+p^{r-1}) \\ &= \sum_{k=1}^{r} a_k \left(\frac{p^k - 1}{p-1} \right) = \sum_{k=1}^{r} a_k \mu(k). \end{aligned}$$

By (7), P has order $p^{\sum_{k=1}^r a_k \mu(k)} = p^{\mathrm{ord}_p(n!)}$, which is the correct order for a Sylow-p-subgroup of $\mathfrak{S}_n$. Moreover, as previously noted, $W_{m,p}$ may be viewed as a subgroup of $\mathfrak{S}_{p^m}$, so P is naturally a subgroup of $\mathfrak{S}_n$. □

3 Enumerating Sylow double cosets

With these preliminaries out of the way, the proof of Theorem 1 is now straightforward.

Proof of Theorem 1. Let P be a Sylow-p-subgroup of $\mathfrak{S}_n$. By Theorem 3,

$$|P\backslash\mathfrak{S}_n/P| = \frac{n!}{p^{2\,\mathrm{ord}_p(n!)}} \sum_{\nu\vdash n} \frac{|C_\nu \cap P|^2}{|C_\nu|},$$

where C_ν is the conjugacy class of $\mathfrak{S}_n$ containing all permutations of cycle type ν. Let z_ν be the order of the centralizer of any permutation having cycle type ν. Then $|C_\nu| = n!/z_\nu$, and so

$$|P\backslash\mathfrak{S}_n/P| = \frac{1}{p^{2\,\mathrm{ord}_p(n!)}} \sum_{\nu\vdash n} z_\nu |C_\nu \cap P|^2.$$

But $|C_\nu \cap P|$ just counts the number of elements of P having cycle type ν in $\mathfrak{S}_n$, so from the definition of the augmented cycle index,

$$a_\nu := |C_\nu \cap P| = [s_1^{i_1} s_2^{i_2} \cdots s_n^{i_n}] \widetilde{Z}_P(s). \tag{8}$$

Theorem 1 now follows. □

We next turn to some examples to illustrate Theorem 1. The idea is to use Theorem 7 and Kalužnin's Theorem 8 to evaluate the cycle index of P, then substitute into (1) using the well-known result (*e.g.*, [34], Prop. 1.3.2) that, for any partition $\nu = 1^{i_1} 2^{i_2} \cdots n^{i_n}$ of n,

$$z_\nu := 1^{i_1} i_1! 2^{i_2} i_2! \cdots n^{i_n} i_n!. \tag{9}$$

3.1 $\mathfrak{S}_p$

The Sylow-p-subgroups of $\mathfrak{S}_p$ are all isomorphic to $\mathbb{Z}_p$. These are just the groups generated by a p-cycle. Thus, the cycle index of $\mathbb{Z}_p$ is

$$Z_{\mathbb{Z}_p}(s) = \frac{1}{p}(s_1^p + (p-1)s_p), \tag{10}$$

corresponding to the identity permutation with p cycles of length 1 and $p-1$ cycles of length p. By (8),

$$a_{1^p} = 1 \quad \text{and} \quad a_p = p - 1.$$

Equation (1) yields

$$N_p = |P\backslash\mathfrak{S}_p/P| = \frac{1}{p^2}(a_{1^p}^2 p! + a_p^2 p) = \frac{1}{p^2}(p! + p(p-1)^2) = \frac{1}{p}((p-1)! + (p-1)^2). \quad (11)$$

It is not immediately obvious that the right hand side of (11) is integral, but of course it must be. And, indeed, integrality follows from Wilson's theorem ($(p-1)! = -1 \bmod p$). (As pointed out by Diaconis *et. al.* [8], this provides a somewhat convoluted proof of Wilson's theorem.) We could now use (11) to calculate the number of double cosets of a given size in $\mathfrak{S}_p$, as in [8], but we do not do so here.

3.2 $\mathfrak{S}_{p^2}$

Let $P := \mathbb{Z}_p \wr \mathbb{Z}_p$ be a Sylow-p-subgroup of $\mathfrak{S}_{p^2}$. According to Theorem 7,

$$\begin{aligned} Z_P &= \frac{1}{p}((Z_{\mathbb{Z}_p}(s_1, s_2, \dots)^p + (p-1)Z_{\mathbb{Z}_p}(s_p, s_{2p}, \dots)) \\ &= \frac{1}{p}\left(\left(\frac{1}{p}(s_1^p + (p-1)s_p)\right)^p + (p-1)\left(\frac{1}{p}(s_p^p + (p-1)s_{p^2}\right)\right) \\ &= \frac{1}{p^{p+1}}\left(\sum_{k=0}^{p}\binom{p}{k}s_1^{pk}((p-1)s_p)^{p-k}\right) + \frac{(p-1)}{p^2}(s_p^p + (p-1)s_{p^2}). \end{aligned}$$

As $|P| = p^{p+1}$ we may read off the coefficients of $\widetilde{Z}_P = p^{p+1}Z_P$:

$$\begin{aligned} a_{1^{pk}p^{p-k}} &= \binom{p}{k}(p-1)^{p-k} \quad (1 \le k \le p) \\ a_{p^p} &= (p-1)^p + p^{p-1}(p-1) \\ a_{p^2} &= p^{p-1}(p-1)^2. \end{aligned}$$

Therefore, by (9) and (1),

$$\begin{aligned} N_{p^2} = |P\backslash\mathfrak{S}_{p^2}/P| = \frac{1}{p^{2p+2}}\Bigg(&\sum_{k=1}^{p}\binom{p}{k}^2(p-1)^{2p-2k}(pk)!p^{p-k}(p-k)! \\ &+ ((p-1)^p + p^{p-1}(p-1))^2 p^p p! + p^{2p}(p-1)^4\Bigg). \end{aligned} \quad (12)$$

The value of N_{p^2} grows extremely rapidly with p. For instance, for $p = 2, 3, 5, 7, 11$ we get 2, 88, 6.4×10^{16}, 1.8×10^{49}, and 8.2×10^{175}, respectively. With additional work one could derive an asymptotic expression for N_{p^2}. As a quick check that these orders are

reasonable, observe that the number of (ordinary) cosets of P in $\mathfrak{S}_{p^2}$ is $(p^2)!/p^{p+1}$. For $p = 2, 3, 5, 7, 11$ this gives 3, 4480, 9.9×10^{20}, 1.1×10^{56}, and 2.6×10^{188}, respectively.

Remark. The parenthetical expression on the right hand side of (12) must be divisible by p^{2p+2}, but this is certainly not obvious.

3.3 $\mathfrak{S}_{p^m}$

The enumeration of Sylow double cosets of $\mathfrak{S}_{p^m}$ follows along the same lines as above, but the computations rapidly become involved. Define, recursively,

$$A^{(r)}(p^k) := \frac{1}{p}([A^{(r-1)}(p^k)]^p + (p-1)A^{(r-1)}(p^{k+1})) \quad \text{with} \quad A^{(0)}(k) := s_k. \tag{13}$$

Then, following the procedure above, we have

$$Z_{W_{r,p}} = A^{(r)}(1) \qquad (r \geq 1). \tag{14}$$

This yields, for instance,

$$\begin{aligned}
Z_{W_{1,p}} = A^{(1)}(1) &= \frac{1}{p}\left([A^{(0)}(1)]^p + (p-1)A^{(0)}(p)\right) \\
&= \frac{1}{p}\left(s_1^p + (p-1)s_p\right) \\
Z_{W_{2,p}} = A^{(2)}(1) &= \frac{1}{p}\left([A^{(1)}(1)]^p + (p-1)A^{(1)}(p)\right) \\
&= \frac{1}{p}\left(\left[\frac{1}{p}(s_1^p + (p-1)s_p)\right]^p + (p-1)\left(\frac{1}{p}[s_p^p + (p-1)s_{p^2}]\right)\right) \\
&= \frac{1}{p^{p+1}}(s_1^p + (p-1)s_p)^p + \frac{p-1}{p^2}(s_p^p + (p-1)s_{p^2}) \\
Z_{W_{3,p}} = A^{(3)}(1) &= \frac{1}{p}\left([A^{(2)}(1)]^p + (p-1)A^{(2)}(p)\right) \\
&= \frac{1}{p}\left(\left[\frac{1}{p^{p+1}}(s_1^p + (p-1)s_p)^p + \frac{p-1}{p^2}(s_p^p + (p-1)s_{p^2})\right]^p \right. \\
&\qquad \left. + \frac{p-1}{p^{p+1}}(s_p^p + (p-1)s_{p^2})^p + \frac{p-1}{p^2}(s_{p^2}^p + (p-1)s_{p^3})\right).
\end{aligned}$$

3.4 $\mathfrak{S}_n$

We now turn to the general case. By Theorem 8, a Sylow-p-subgroup $P \leq \mathfrak{S}_n$ is a direct product of copies of iterated wreath products. Suppose

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

is the p-adic expansion of n. Then by Theorems 6 and 8, the cycle index of $W_{n,p}$ is given by

$$Z_P = Z_{W_{0,p}}^{a_0} Z_{W_{1,p}}^{a_1} \cdots Z_{W_{r,p}}^{a_r} = [A^{(0)}(1)]^{a_0} [A^{(1)}(1)]^{a_1} [A^{(2)}(1)]^{a_2} \cdots [A^{(r)}(1)]^{a_r}. \tag{15}$$

From this, we may compute N_n in the manner above. Clearly, this procedure becomes prohibitively complex as n increases. But, using the results above, we can compute N_n in some simple cases.

For instance, let $p = 5$, and suppose that $n = 38$. As $38 = 3 + 2 \cdot 5 + 5^2$, we have

$$P = W_{0,5}^3 \times W_{1,5}^2 \times W_{2,5},$$

so

$$\begin{aligned}
Z_P &= [A^{(0)}(1)]^3 [A^{(1)}(1)]^2 [A^{(2)}(1)] \\
&= s_1^3 \left[\frac{1}{5} \left(s_1^5 + 4 s_5 \right) \right]^2 \left[\frac{1}{5^6} (s_1^5 + 4 s_5)^5 + \frac{4}{5^2} (s_5^5 + 4 s_{25}) \right] \\
&= \frac{1}{5^8} \left(\sum_{k=0}^{7} \binom{7}{k} s_1^{5k+3} (4 s_5)^{7-k} \right) \\
&\qquad + \frac{4}{5^4} s_1^3 (s_1^{10} s_5^5 + 8 s_1^5 s_5^6 + 16 s_5^7 + 4 s_1^{10} s_{25} + 32 s_1^5 s_5 s_{25} + 64 s_5^2 s_{25}).
\end{aligned}$$

As $|P| = p^{a_1 + a_2(1+p)} = 5^8$ we have

$$\begin{aligned}
\widetilde{Z}_P = {s_1}^{38} &+ 28\, {s_1}^{33} s_5 + 336\, {s_1}^{28} {s_5}^2 + 2240\, {s_1}^{23} {s_5}^3 + 8960\, {s_1}^{18} {s_5}^4 \\
&+ 24004\, {s_1}^{13} {s_5}^5 + 10000\, {s_1}^{13} s_{25} + 48672\, {s_1}^8 {s_5}^6 + 80000\, {s_1}^8 s_5 s_{25} \\
&+ 56384\, {s_1}^3 {s_5}^7 + 160000\, {s_1}^3 {s_5}^2 s_{25}.
\end{aligned}$$

Reading off the coefficients a_ν and plugging into (1) and computing yields

$$N_{38} = 342790411251088016041510491311308 8.$$

4 Questions

Evidently, calculating the exact number of Sylow-p-subgroups starting from (1) is essentially impossible for very large n. Hence, a natural question is whether (1) can be used to calculate an asymptotic formula of some kind. Diaconis *et. al.* [8] have demonstrated that 'most' double cosets of Sylow-p-subgroups of $\mathfrak{S}_n$ have the maximum size possible. So another natural question is whether these double cosets can be enumerated by a simple formula, perhaps using some of the results above.

5 Declarations

5.1 Funding and/or Conflicts of interests/Competing interests

The author declares that no funding was received during the preparation of this manuscript.

5.2 Data

Data sharing is not applicable to this article.

References

[1] S.C. Billey, M. Konvalinka, T.K. Petersen, W. Slofstra, and B.E. Tenner, "Parabolic double cosets in Coxeter groups", *Electron. J. Combin.* **25 (1)** (2018) P1.23.

[2] T. Browning, "Counting parabolic double cosets in symmetric groups", *Electron. J. Combin.* **28 (3)** (2021) P3.40.

[3] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms* (Cambridge University Press, Cambridge, 1994).

[4] P.J. Cameron, *Permutation Groups* (Cambridge University Press, Cambridge, 1999).

[5] A. Cauchy, "Mémoires sur diverses propriétés remarquables des substitutions régulières ou irrégulières, et des systèmes des substitutions conjuguées", *Compte Rendu des Séances de L'Académie des Sciences* **21 (13)** (1845) 835-852.

[6] N.G. de Bruijn, "Pólya's theory of counting", in *Applied Combinatorial Mathematics*, edited by E.F. Beckenbach (Wiley, New York, 1964), pp. 144-184.

[7] P. Diaconis and A. Gangolli, "Rectangular arrays with fixed margins", in *Discrete Probability and Algorithms*, D. Aldous, P. Diaconis, J. Spencer, J.M. Steele (eds.) (Springer, New York, 1995), pp. 15-41.

[8] P. Diaconis, E. Giannelli, R. Guralnick, S. Law, G. Navarro, and H. Spink, "p-Sylow double cosets for the symmetric group", unpublished manuscript (2023).

[9] P. Diaconis, A. Ram and M. Simper, "Double coset Markov chains", *Forum of Mathematics Sigma* **11 (E2)** (2023) 1-45.

[10] P. Diaconis and M. Simper, "Statistical enumeration of groups by double cosets", *J. Algebra* **607** (2022) 214-246.

[11] J.D. Dixon and B. Mortimer, *Permutation Groups* (Springer, New York, 1996).

[12] W. Findlay, "The Sylow subgroups of the symmetric group", *Trans. Amer. Math. Soc.* **5** (1904) 263-278.

[13] D. Goldschmidt, *Group Characters, Symmetric Functions, and the Hecke Algebra* (American Mathematical Society, Providence, 1993).

[14] L.C. Grove, *Groups and Characters* (Wiley, New York, 1997).

[15] F. Harary, *Graph Theory* (Addison-Wesley, Reading, MA, 1969).

[16] F. Harary and E.M. Palmer, *Graphical Enumeration* (Academic Press, New York, 1973).

[17] B. Huppert, *Endliche Gruppen I* (Springer, Berlin, 1967).

[18] M.S. Im and C.O. Oğuz, "Natural transformations between induction and restriction on itterated wreath product of symmetric group of order 2", *Mathematics* **10** (2022) 3761. https://doi.org/10.3390/math10203761

[19] L. Kaloujnine, "La stucture des p-groupes de Sylow des groupes symétriques finis", *Annales scientifiques de l'É.N.S., 3e série* **65** (1948) 239-276.

[20] L.A. Kaluzhnin, P.M. Beletskiĭ, and V.Z. Feĭnberg, *Kranzprodukte* (Teubner, Leipzig, 1987).

[21] A.M. Legendre, *Théorie des Nombres* (Firmin Didot Freères, Paris, 1830).

[22] R. Merris, *Combinatorics* 2nd ed. (Wiley, New York, 2003).

[23] G.A. Miller, "On the transitive substitution groups whose order is a power of a prime number", *Amer. J. Math.* **23 (2)** (1901) 173-178.

[24] P.M. Neumann, "A lemma that is not Burnside's", *The Mathematical Scientist* **4 (2)** (1979) 133-141.

[25] R. Orellana, M. Orrison, and D. Rockmore, "Rooted trees and iterated wreath products of cyclic groups", *Adv. Appl. Math.* **33** (2004) 531-547.

[26] J.E. Paguyo, "Fixed points, descents, and inversions in parabolic double cosets of the symmetric group", arXiv:2112.07728v2 (April 2023).

[27] E.M. Palmer and R.W. Robinson, "Enumeration under two representations of the wreath product", *Acta Mathematica* **131** (1973) 123-143.

[28] D.S. Passman, *Permutation Groups* (Dover, Mineola, NY, 2012).

[29] G. Pólya, "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und chemische Verbindungen", *Acta Mathematica* **68** (1937) 145-254.

[30] G. Pólya and R.C. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds* (Springer, New York, 1987).

[31] J.H. Redfield, "The theory of group reduced distributions", *Amer. J. Math.* **49** (1927) 433-455.

[32] D.J.S. Robinson, *A Course in the Theory of Groups*, 2nd ed. (Springer, New York, 1996).

[33] J.J. Rotman, *An Introduction to the Theory of Finite Groups*, 4th ed. (Springer, New York, 1995).

[34] R.P. Stanley, *Enumerative Combinatorics* Vol. 1, 2nd ed. (Cambridge, Cambridge University Press, 2011).

[35] R.P. Stanley, *Enumerative Combinatorics* Vol. 2 (Cambridge, Cambridge University Press, 1999).

[36] R.P. Stanley, *Algebraic Combinatorics*, 2nd ed. (Springer, New York, 2018).

[37] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, 2nd ed. (Cambridge University Press, Cambridge, 2001).

[38] H. Wielandt, *Finite Permutation Groups* (Academic Press, New York, 1964).