ON THE NUMBER AND SIZES OF DOUBLE COSETS OF SYLOW SUBGROUPS OF THE SYMMETRIC GROUP

PERSI DIACONIS, EUGENIO GIANNELLI, ROBERT M. GURALNICK, STACEY LAW, GABRIEL NAVARRO, BENJAMIN SAMBALE, AND HUNTER SPINK

We dedicate this paper to the memory of Marty Isaacs, who helped it and us in many, many ways.

Abstract. Let P_n be a Sylow p-subgroup of the symmetric group S_n. We investigate the number and sizes of the $P_n \setminus S_n / P_n$ double cosets, showing that 'most' double cosets have maximal size when p is odd, or equivalently, that $P_n \cap P_n^x = 1$ for most $x \in S_n$ when n is large. We also find that all possible sizes of such double cosets occur, modulo a list of small exceptions.

1. Introduction

For n a natural number and p a prime, let P_n be a Sylow p-subgroup of the symmetric group S_n. This splits S_n into a disjoint union of P_n double cosets $P_n x P_n$ as x varies over S_n. We ask:

- How many double cosets are there?
- What are their typical sizes?

Motivation for these questions from probability, enumerative group theory and from modular representation theory are described in Section 1.1 below.

The double cosets have sizes varying between $|P_n|$ and $|P_n|^2$. In Corollary 2.8 below, we show that if $n \geq 9$ then S_n admits (P_n, P_n)-double cosets of all possible sizes. Moreover, our main result shows that, for $p > 2$ and n large, most double cosets are as large as possible. Equivalently, since $|P_n x P_n| = |P_n|^2/|P_n \cap P_n^x|$, we have that $P_n \cap P_n^x = 1$ for almost all x.

Theorem 1.1. *Let p be a prime. Let $f(n,p)$ be the probability that $|P_n \cap P_n^x| > 1$ where $x \in S_n$ is chosen uniformly at random.*

(a) For $p > 2$, $f(n,p) \to 0$ as $n \to \infty$, uniformly in $2 < p \leq n$.
(b) For $p = 2$, $\liminf_{n\to\infty} f(n,2) \geq 1 - e^{-1/2}$.

To familiarise the reader with the problem, in the following example we treat the smallest non-trivial case (i.e. we study in detail the case of S_p).

Example 1.2. Let us fix the rank n of our symmetric group to be equal to the prime number p. In this case, given $P_p \in \mathrm{Syl}_p(S_p)$ we have that P_p is isomorphic to C_p, the cyclic group of order p. Hence the double cosets have size p or p^2. Let n_i be the number of double cosets of size p^i, for each $i \in \{1, 2\}$. Then we have $p! = pn_1 + p^2 n_2$. If $|P_p w P_p| = |P_p|$, then $wP_p = P_p w$ so $w \in N_{S_p}(P_p)$. As explained in Section 2, we know that $N_{S_p}(C_p) = C_p \rtimes C_{p-1}$, so $n_1 = |N_{S_p}(C_p)/C_p| = p - 1$ and $n_2 = \frac{(p-1)! - (p-1)}{p}$. For instance, notice that if $p = 11$ then $n_1 = 10$ and $n_2 = 329890$. This illustrates our main results, that all possible double coset sizes appear, and most double coset sizes are as large as possible.

Theorem 1.1 shows that $p = 2$ is different; letting $P_n \in \mathrm{Syl}_2(S_n)$, Table 1 gives some data on the number of (P_n, P_n)-double cosets in S_n of size 2^{m+k}, $0 \leq k \leq m$, where $|P_n| =: 2^m$ (see (2.1)). Note that:

- The largest entry in each row almost always occurs in column 2^{2m-1} (although the 2^{2m-1} and 2^{2m} entries are roughly equal).
- The first column contains all 1s as P_n is self-normalising in S_n when $p = 2$ (see Lemma 2.2).
- The second column (number of double cosets of size 2^{m+1}) is explained in Section 5 below.
- Going from row $n = 2^k - 1$ to row $n = 2^k$, the entries decrease down each column. (Compare this with the structure of P_n; see Section 2.1.)

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	$\sum$
1	1																			1
2	1																			1
3	1	1																		2
4	1	1																		2
5	1	1	1	1																4
6	1	2	2	2	1															8
7	1	3	7	13	11															35
8	1	1	2	4	3	3	2													16
9	1	1	2	5	6	10	15	11												51
10	1	1	3	8	13	22	32	43	22											145
11	1	2	4	14	39	97	218	395	342											1112
12	1	3	8	17	27	53	97	154	247	341	197									1145
13	1	3	9	23	53	150	399	965	2173	3818	3335									10929
14	1	4	15	50	135	341	826	1942	4399	8983	13737	10967								41400
15	1	5	22	89	328	1202	4268	13960	41210	104946	194791	181963								542785
16	1	1	2	6	15	24	55	100	209	407	955	1938	4755	8390	13783	9743				40384
17	1	1	2	6	16	29	77	189	537	1609	5223	15898	45965	113336	208574	191706				583169
18	1	1	2	7	21	51	158	442	1240	3555	10602	32233	95157	257733	589685	974086	816834			2781808
19	1	2	3	9	31	96	343	1281	4902	19274	77090	300762	1085019	3489029	9305449	17587577	16687838			48558706
20	1	2	4	15	50	136	366	995	2753	7755	22520	68507	218355	697784	2131976	5935593	13799562	23045073	19529900	65461347

TABLE 1. The number of (P_n, P_n)-double cosets in S_n according to their size, where P_n is a Sylow 2-subgroup of S_n. The leftmost column lists the values of n considered. The rightmost column lists, for each n, the total number of such double cosets for S_n. For each column in between, the column label i indicates the number of double cosets of size 2^{m+i}. Here, m is given by $|P_n| = 2^m$; see (2.1) for explicit formulas for the value of m. Note that the size of any such double coset must be a power of 2 between 2^m and 2^{2m}; see (2.6).

1.1. **Motivation.** Our route to studying these problems comes from 'Pólya theory' – enumeration under symmetry. Let $\mathcal{X}$ be a finite set and G a finite group acting on $\mathcal{X}$. This splits $\mathcal{X}$ into disjoint orbits

$$\mathcal{X} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_k.$$

Natural questions are:

- How many orbits are there?
- What are the typical sizes?
- Do the orbits have 'nice names'?
- How can one 'pick a random orbit'?

Of course, in this generality, this is a hopelessly out of focus question; there are too many groups acting on too many sets. Nonetheless, there are many important special cases. See [Kel03] for a review when $\mathcal{X}$ is a group.

Computer scientists Jerrum and Goldberg [J93, GJ02] introduced a general algorithm for random generation which allows the first two problems to be studied – the Burnside process. Their interest was computational complexity and they highlight special examples where the questions are #P-complete.

In contrast, [BD24, DHow25, DZ23, DZ25] show that there are many examples where enumeration is feasible (and interesting):

- Suppose $\mathcal{X} = G$ and G acts on itself by conjugation ($x^g = g^{-1}xg$). Then the orbits are conjugacy classes and the questions become: how many classes? What are their typical sizes?

  When $G = S_n$, the conjugacy classes are indexed by partitions and the Burnside process gives a useful algorithm for generating a random partition of n. Work in [DHow25] shows this is effective for n up to 10^9, for instance.
- Let H and K be subgroups of a finite group G. Then $H \times K$ acts on G via $(h, k) \cdot g = hgk^{-1}$, with orbits the double cosets $H \setminus G/K$.

  When $G = S_n$ and $H = S_\lambda$, $K = S_\mu$ for two partitions λ and μ of n (i.e H and K are parabolic subgroups), the double cosets are indexed by contingency tables: arrays of non-negative integers with row sums λ and column sums μ [JK81, Theorem 1.3.10]. For references, enumerative theory and statistical applications, see [DHow25, DSi22].

  If $G = \mathrm{GL}_n(\mathbb{F}_q)$ and $H = K = B$, the Borel subgroup of invertible upper triangular matrices, then we have the Bruhat decomposition $\mathrm{GL}_n(\mathbb{F}_q) = \bigcup_{w \in S_n} BwB$; see [DRS23] for probabilistic applications.

Michael Geline asked about $P_n \setminus S_n/P_n$. This connects to modular representation theory by the following route. Consider a finite group G with a split BN-pair B, N, U in characteristic p (see [Car72] or [Car85] for definitions and references). Let k be an algebraically closed field of characteristic p. The irreducible representations of G over k can be studied via the approach of [Saw77, Cur70, Ric69, Gre78] and [T80] (this last reference is a well written account with full references). A central piece of the story is the Hecke algebra

$$E = L_k(U \setminus G/U) = \mathrm{End}_G((\mathbb{1}_U)^G).$$

They show:

- E is a Frobenius algebra.
- Every simple right E–module is 1-dimensional, given by a multiplicative character $\psi : E \to k$.
- Each such ψ is determined by a vector of parameters $(\chi, u_1, u_2, \ldots, u_m)$ with χ a linear character of the Borel subgroup B and $u_i \in k$.
- There is a bijective correspondence between the set of irreducible kG–modules and the set of such characters ψ.

One hope for studying the difficult problem of understanding representations of S_n over k [Kle05] is to study the Hecke algebra $\mathcal{H}_n(k) := L_k(P_n \setminus S_n/P_n)$. Understanding the number of double cosets (i.e. the k-dimension of $\mathcal{H}_n(k)$) and their sizes seems like a natural first step. It is worth mentioning that the representation theory of the algebra $\mathcal{H}_n(k)$ is closely related to the decomposition of the permutation character $(\mathbb{1}_{P_n})^{S_n}$ into irreducible constituents. (We refer the reader to [CR81, Chapter 11D] for the complete definition and properties of this correspondence.) Exploiting this connection, the exact number of irreducible representations of $\mathcal{H}_n(k)$ has been computed in [GL18, Corollary B] for any field k of odd characteristic.

Alas, our main results show that most double cosets have the same size, so that 'size' does not usefully distinguish them. Still, it does give a good hold on dimension.

1.2. **Outline.** Section 2 gives background on P_n and double coset enumeration. Furthermore, we prove that all possible sizes occur for $n \geq 9$. Section 3 studies a special case when $n = kp$ and $1 \leq k \leq p-1$. Then, sharp formulas and asymptotics are available. It may be read now for further motivation. Section 4 deduces Theorem 1.1. Our proof uses a result on random generation of A_n due to Eberhard–Garzoni [EG21, EG22]. Section 5 develops a complete understanding of double cosets of size $p|P_n|$ for all p. It also contains useful facts for size $p^k|P_n|$ for general k. The final section contains remarks and open problems.

Acknowledgements. We thank Michael Geline, Michael Howes, Marty Isaacs, Markus Linckelmann, Radha Kessar, John Murray and Richard Stanley for many interesting comments and helpful discussions. We also thank Gereon Koßmann for computational support. P.D. acknowledges support from NSF grant 1954042. E.G. acknowledges support from the European Union - Next Generation EU, M4C1, CUP B53D23009410006, PRIN 2022.

2. Background

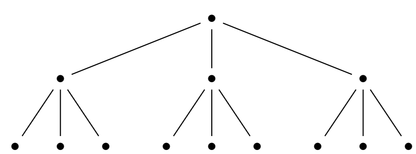
2.1. **Sylow subgroups of S_n.** The Sylow p-subgroups of S_n were first determined in [Kal48]. This is also sometimes attributed to Cauchy, see [M04]. The facts below are standard, see [O94] or [JK81]; see also [W16] for an alternative description.

The largest power of p dividing $n!$ is p^m where m is given as follows:

$$m = \sum_{a=1}^{\infty} \left\lfloor \frac{n}{p^a} \right\rfloor = \frac{n - D_p(n)}{p-1}. \tag{2.1}$$

Here, if $n = \sum_{i=0}^{\infty} a_i p^i$ is the p-adic expansion of n, i.e. $a_i \in \{0, 1, \ldots, p-1\}$ for all i, then $D_p(n) = \sum_{i=0}^{\infty} a_i$ is the sum of the digits (this was known to Legendre; see [L00], whose first edition was published in 1798).

For example, if $n = p^2$ then $m = \frac{p^2-1}{p-1} = p+1$, so $|P_n| = p^{p+1}$. For this case, P_n may be pictured as $C_p^p \rtimes C_p \cong C_p \wr C_p$. When $p = 3$, we have the following diagram:



Here, each of the p copies of C_p in the base group acts cyclically on each set of leaves, and the wreathing C_p permutes the p branches from the root cyclically. Iterating this construction, for $n = p^k$ we have that

$$P_n = \underbrace{C_p \wr C_p \wr \cdots \wr C_p}_{k \text{ times}}, \qquad |P_n| = p^{1+p+\cdots+p^{k-1}}. \tag{2.2}$$

For general n, write $n = \sum_{j=0}^{\infty} a_j p^j$ where $0 \leq a_j \leq p-1$ for each j. Then P_n is isomorphic to the direct product of a_j copies of the Sylow p-subgroup of S_{p^j} taken over all $j \geq 0$. A useful fact, needed below, is

$$N_{S_n}(P_n) \cong \prod_j N_{S_{p^j}}(P_{p^j}) \wr S_{a_j} \tag{2.3}$$

where the direct product is taken over all those j such that $a_j \neq 0$ and where $N_{S_{p^j}}(P_{p^j}) = P_{p^j} \rtimes (C_{p-1})^j$. A careful version of the isomorphism and further details can be found in [Gia21, Section 2B] where it is applied to give explicit McKay bijections for S_n and A_n.

2.2. **Double cosets for $H \times K$ acting on G.** Let G be a finite group and H and K be subgroups of G. The set of orbits of $H \times K$ acting on G by $(h,k)\cdot g = hgk^{-1}$ is denoted $H \backslash G/K$, the set of (H,K)-double cosets of G. For a textbook treatment, see [Suz82, p.23]. The Orbit–Stabiliser theorem implies

$$|HxK| = \frac{|H||K|}{|H \cap xKx^{-1}|} \tag{2.4}$$

for $x \in G$. Here are three formulas for the number of double cosets: the first is an easy application of Orbit–Stabiliser; see for example [Sta99, Ex. 7.77] and [Cur99, p.44] for the latter two.

$$|H \backslash G/K| = \frac{1}{|H||K|} \sum_{h\in H, k\in K} |G_{hk}|, \quad \text{where } G_{hk} = \{g \mid hgk^{-1} = g\}, \tag{2.5a}$$

$$|H \backslash G/K| = \sum_{\chi\in \mathrm{Irr}(G)} a(\chi)b(\chi) = \langle (\mathbb{1}_H)^G, (\mathbb{1}_K)^G\rangle$$

$$\text{where } (\mathbb{1}_H)^G = \sum_{\chi\in \mathrm{Irr}(G)} a(\chi)\chi,\ (\mathbb{1}_K)^G = \sum_{\chi\in \mathrm{Irr}(G)} b(\chi), \tag{2.5b}$$

$$|H \backslash G/K| = \frac{|G|}{|H||K|} \sum_{\mathcal{C}} \frac{|\mathcal{C}\cap H||\mathcal{C}\cap K|}{|\mathcal{C}|} \tag{2.5c}$$

where $\mathcal{C}$ runs over the conjugacy classes of G. See [Ren24] for applications of (2.5c) to $|P_n \backslash S_n/P_n|$: this paper contains a useful review for Sylow p-subgroups of S_n with full proofs.

Remark 2.1. In the case of $p = 2$, the sequence of numbers $|P_n \backslash S_n/P_n|$ is recorded on the Online Encyclopedia of Integer Sequences as A360808 [OEIS23], and the formula given there follows from (2.5b).

To see this: $|P_n \backslash S_n/P_n|$ is calculated as $\langle U_n, U_n\rangle$ where Stanley defines the symmetric functions U_n and T_k as follows. Set $U_n = T_{a_0}T_{a_1}...T_{a_s}$, where T_k is recursively defined by $T_0 = p_1$ (power sum) and $T_k = h_2[T_{k-1}]$ (plethysm) for $k > 0$. Under the Frobenius characteristic isomorphism, U_n corresponds to the symmetric group character $(\mathbb{1}_{P_n})^{S_n}$, since T_k corresponds to $(\mathbb{1}_{S_2 \wr S_2 \wr \cdots \wr S_2})^{S_{2^k}}$. In this latter expression the trivial character is induced from a k-fold wreath product of cyclic groups of order 2, and such a group is exactly a Sylow 2-subgroup of S_{2^k}.

All of these formulas were useful in our preliminary work, collecting examples. We have not seen how to use any of them to derive results for general n.

Despite these nice formulas, it is worth remembering that there are many examples where computing $|HxK|$ or $|H \backslash G/K|$ exactly is #P-complete. See [DSi22] or [DMal21] for references and examples.

2.3. **Smallest and largest sizes.** Let G be a finite group and $x \in G$. Take $H = K \le G$ in this section. From (2.4) we immediately observe that

$$|H| \le |HxH| \le |H|^2. \tag{2.6}$$

Clearly the lower bound is attained at $x = 1$. More generally, we observe that $|HxH| = |H|$ if and only if $xH = Hx$, that is, if and only if $x \in N_G(H)$.

Lemma 2.2. *For finite groups $H \le G$, the number of double cosets HxH of size $|H|$ is $|N_G(H) : H|$ and such double cosets are naturally labelled by $N_G(H)/H$.*

Remark 2.3. Lemma 2.2 shows that the set $N_G(H)/H$ naturally labels those double cosets in $H \backslash G/H$ of minimal size. Despite this, it seems to be extremely difficult to find a labelling for all double cosets. For instance, even for $P_p \le S_p$, we do not have a natural labelling of those double cosets of size p^2. When $p = 2$, (2.3) shows that $|N_{S_n}(P_n) : P_n| = 1$, explaining the column of Table 1 labelled by 0 (i.e. that which describes the number of double cosets of size 2^{m+0}).

On the other end of the spectrum, double cosets of maximal size need not always exist in general. For instance, if $H \trianglelefteq G$ then all double cosets are simply one-sided cosets, of minimal size $|H|$. Nevertheless, the following result by Zenkov and Mazurov in [ZM96] settles the case for $P_n \backslash S_n/P_n$.

Theorem 2.4. [ZM96, Theorem 1] *For p a prime and n a natural number, the symmetric group S_n contains at least two Sylow p-subgroups with trivial intersection if and only if*

$$(p, n) \notin \{(3, 3), (2, 2), (2, 4), (2, 8)\}.$$

Remark 2.5. Another way to see this when $p \notin \{2,3\}$ is to use a theorem of Granville–Ono [GO96], which asserts that for $p \notin \{2,3\}$ and all n, S_n admits p-blocks with trivial defect group. This implies the existence of $P \in \mathrm{Syl}_p(S_n)$ and $x \in S_n$ such that $P \cap P^x = 1$, using a theorem of Green [N98, Corollary 4.21].

Indeed, following a suggestion of Radha Kessar, by considering p-defect zero characters we can also obtain a first bound on the number of Sylow-p double cosets of S_n of maximal size. Let X denote the set of irreducible characters of S_n of p-defect 0 (under the natural bijection between $\mathrm{Irr}(S_n)$ and the set $\mathcal{P}(n)$ of partitions of n, such characters are labelled by p-core partitions). Then the number of (P_n, P_n)-double cosets of S_n of size $|P_n|^2$ is at least $\sum_{\chi\in X}(\chi(1)_{p'})^2$, where if $m \in \mathbb{N}$ then $m_{p'}$ denotes its p'-part. This follows from the fact that a defect zero block is projective as a kP_n-kP_n-bimodule.

The next section treats double cosets of intermediate sizes. As mentioned in the introduction, our first main result (Theorem 2.7) extends Theorem 2.4 by showing that $P_n \setminus S_n / P_n$ admits double cosets of any possible size (modulo a few exceptions when $n < 9$).

2.4. **Intermediate sizes.** Let n be a natural number and p a prime. Let P denote a Sylow p-subgroup of S_n and $x \in S_n$. Since $|PxP| = |P|/|P : P \cap xPx^{-1}|$ from (2.4), it is easy to see that $|PxP|$ must be a p-power between $|P|$ and $|P|^2$. Moreover, it turns out that all possible sizes can occur for such Sylow-p double cosets. In order to prove this statement, we first need the following technical lemma.

Lemma 2.6. *Let $k \in \mathbb{N}$ with $k \geq 2$ and $n = 2^k+1$. Then there exist $P, Q \in \mathrm{Syl}_2(S_n)$ such that $|P\cap Q| = 2$ and P and Q have no common fixed point.*

Proof. The case $k \leq 4$ can be checked using [GAP]. Now assume $k \geq 5$. Let $n_1 = 2^{k-1}$, $Y_1 = \mathrm{Sym}(\{1,\ldots,n_1\})$ and $n_2 = 2^{k-1}+1$, $Y_2 = \mathrm{Sym}(\{n_1+1,\ldots,n\}) \cong S_{n_2}$. By Theorem 2.4, there exist $P_1, Q_1 \in \mathrm{Syl}_2(Y_1)$ such that $P_1 \cap Q_1 = 1$. By induction there exist $P_2, Q_2 \in \mathrm{Syl}_2(Y_2)$ such that $|P_2\cap Q_2| = 2$ and P_2 and Q_2 have no common fixed point. Observe that $P_i \cong Q_i$. Take involutions $x, y \in S_n$ such that $P_2 = P_1^x$ and $Q_2 = Q_1^y$. The claim holds for $P = P_1P_2\langle x\rangle$ and $Q = Q_1Q_2\langle y\rangle$. ☐

Theorem 2.7. *Let $n \in \mathbb{N}$ and p be a prime. Let p^m be the p-part of $n!$. Then for every $k \in \{0, 1, \ldots, m\}$ there exist $P, Q \in \mathrm{Syl}_p(S_n)$ such that $|P \cap Q| = p^k$, if and only if*

$$(n, p, k) \notin \{(2, 2, 0), (4, 2, 0), (4, 2, 1), (8, 2, 0), (3, 3, 0), (6, 3, 1)\}.$$

Proof. The case $n \leq 10$ can be checked with [GAP]. Now assume $n \geq 11$. The case $k = 0$ follows from Theorem 2.4. For $k = m$ we can choose $P = Q$. Thus, let $1 \leq k < m$ and $P \in \mathrm{Syl}_p(S_n)$. We argue by induction on n.

Case 1: Let us first assume that $n = p^\ell$ is a prime power.
Let $m(\ell) \in \mathbb{N}$ be such that $|P| = p^{m(\ell)}$. The description of the algebraic structure of the Sylow p-subgroups of symmetric groups implies that $m(\ell) = p \cdot m(\ell-1) + 1$, for any $\ell \geq 2$. Since $0 < k < m(\ell)$, we have $\ell \geq 2$. We partition $\{1, \ldots, n\} = N_1 \cup \ldots \cup N_p$ where $N_i := \{n(i-1)/p + 1, \ldots, ni/p\}$ for $i = 1, \ldots, p$. Let $Y_i := \mathrm{Sym}(N_i)$ and $P_i \in \mathrm{Syl}_p(Y_i)$ for each i. Let $x \in S_n$ be an element of order p which permutes the P_i cyclically, e.g. $P_{i+1} = P_i^x$ for $i = 1, \ldots, p-1$. Then $P := P_1 \ldots P_p\langle x\rangle \cong P_1 \wr C_p$ is a Sylow p-subgroup of S_n. Suppose first that $n \neq 16$. Since $n \geq 11$ and $k < m(\ell) - 1 = p \cdot m(\ell-1)$ we can choose inductively $Q_i \in \mathrm{Syl}_p(Y_i)$ such that

$$|(P_1 \cap Q_1) \times \ldots \times (P_p \cap Q_p)| = p^k \text{ and such that } |P_1 \cap Q_1| \neq |P_2 \cap Q_2|.$$

Let $Q \in \mathrm{Syl}_p(S_n)$ be such that $Q_1 \times\cdots\times Q_p \leq Q$. For any $y \in P\cap Q$ we have that $\langle y\rangle$ acts on $\{P_1, \ldots, P_p\}$ and on $\{Q_1, \ldots, Q_p\}$. Since $\{N_1, \ldots, N_p\}$ is a system of imprimitivity for both P and Q we have that $P_i^y = P_j$ if and only if $Q_i^y = Q_j$. It follows that $\langle y\rangle$ acts on the set $\Omega := \{P_1 \cap Q_1, P_2 \cap Q_2, \ldots, P_p \cap Q_p\}$. Since $|P_1 \cap Q_1| \neq |P_2 \cap Q_2|$ the action is not transitive. We deduce that $\langle y\rangle$ acts trivially on Ω and hence that $P_i^y = P_i$ and $Q_i^y = Q_i$. This shows that $y \in Y_1 \times \cdots \times Y_p$ and therefore that $P \cap Q = (P_1 \cap Q_1) \times \ldots \times (P_p \cap Q_p)$. We conclude that $|P \cap Q| = p^k$, as desired.

Next suppose $k = m(\ell) - 1$. Here we choose a different partition $\{1, \ldots, n\} = N_1 \cup \ldots \cup N_{n/p}$ where $N_i := \{(i-1)p + 1, \ldots, ip\}$ for $i = 1, \ldots, n/p$. Let $Y_i = \mathrm{Sym}(N_i) \cong S_p$ and $P_i \in \mathrm{Syl}_p(Y_i)$. We let $B := P_1 \times P_2 \times \cdots \times P_{n/p}$ and $S \cong S_{n/p}$ be a fixed subgroup of $N_{S_n}(B)$ permuting the sets $N_1, \ldots, N_{n/p}$. Since $11 \leq n \neq 16$, using the inductive hypothesis we can find $T_1, T_2 \in \mathrm{Syl}_p(S)$ such that $|T_1 : T_1\cap T_2| = p$. Now let $P = B \rtimes T_1$ and $Q = B \rtimes T_2$. It is clear that $P, Q \in \mathrm{Syl}_p(S_n)$. Setting $Z := B(T_1 \cap T_2)$ we notice that $Z \le P \cap Q \le P$ and that $|P : Z| = |T_1 : T_1 \cap T_2| = p$. It follows that $Z = P \cap Q$. In fact, assuming for a contradiction that $Z \ne P \cap Q$, we would have $P \cap Q = P$ and hence that $T_1 \le Q \cap S = BT_2 \cap S = T_2$ which is a contradiction. We conclude that $|P \cap Q| = |Z| = |B(T_1 \cap T_2)| = p^{m(\ell)-1}$, as desired.

Finally, to conclude Case 1 we consider $n = 16$ and $p = 2$. Here we can argue similarly unless $k = 1$. Fortunately, it turns out that most Sylow intersections are small. We have verified this special case by choosing random Sylow 2-subgroups by computer.

Case 2: n is not a p-power.
Let $n_1 < n$ be the largest p-power $\le n$. Let $N_1 := \{1, \dots, n_1\}$ and $N_2 := \{n_1 + 1, \dots, n\}$. Let $Y_1 := \mathrm{Sym}(N_1)$ and $Y_2 := \mathrm{Sym}(N_2)$. Then we may assume that $P = P_1 \times P_2$ where $P_1 \in \mathrm{Syl}_p(Y_1)$ and $P_2 \in \mathrm{Syl}_p(Y_2)$. If $p \ge 5$, we can choose $Q_1 \in \mathrm{Syl}_p(Y_1)$ and $Q_2 \in \mathrm{Syl}_p(Y_2)$ inductively such that $Q := Q_1 \times Q_2 \in \mathrm{Syl}_p(S_n)$ with

$$|P \cap Q| = |P_1 \cap Q_1||P_2 \cap Q_2| = p^k.$$

For $p = 3$, we can argue as above except the case $n - n_1 \in \{3, 6\}$ with $k = 1$ needs attention. However, here we can choose $Q_1 \in \mathrm{Syl}_3(Y_1)$ such that $|P_1 \cap Q_1| = 1$, because $n_1 \ge 9$. Hence, we may now assume that $p = 2$. Only the cases $k \in \{1, 2\}$ are problematic. If $n = 12$, we can find P, Q by computer random generation. Consequently, we may assume that $n \ge 17$. Now only the case $n - n_1 = 4$ and $k = 1$ is left. Let $N_1 := \{1, \dots, n_1 + 1\}$. By Lemma 2.6, there exist $P_1, Q_1 \in \mathrm{Syl}_2(\mathrm{Sym}(N_1))$ such that $|P_1 \cap Q_1| = 2$ and P_1 and Q_1 have no common fixed point. Without loss of generality, we may assume that P_1 fixes $n_1 + 1$ and Q_1 fixes n_1. Let $N_2 := \{n_1 + 1, \dots, n\}$ and $N_2' := \{n_1, n_1 + 2, n_1 + 3, n\}$. It is easy to find $P_2 \in \mathrm{Syl}_2(\mathrm{Sym}(N_2))$ and $Q_2 \in \mathrm{Syl}_2(\mathrm{Sym}(N_2'))$ with $P_2 \cap Q_2 = 1$. Now $P = P_1 \times P_2$ and $Q = Q_1 \times Q_2$ are Sylow 2-subgroups of S_n with $|P \cap Q| = 2$. □

Corollary 2.8. *For $n \ge 9$, all possible Sylow-p double coset sizes occur in S_n.*

In Section 5, we further investigate the double cosets of second smallest possible size.

3. Abelian Sylow p-subgroups

For $n = kp$ with $k \in \{1, 2, \dots, p-1\}$, Section 2.1 shows that $P_n \cong (C_p)^k$, where, as before, P_n denotes a Sylow p-subgroup of S_n. Now $p^k \le |P_n x P_n| \le p^{2k}$, and the arguments below show that for $p > 2$:

- All values p^a with $k \le a \le 2k$ occur as sizes of (P_n, P_n)-double cosets.
- Almost all double cosets are of size p^{2k}, so the total number of double cosets is asymptotically $\frac{(kp)!}{p^{2k}}$.
- For p large, the number n_a of double cosets of size p^a is super-exponentially increasing from $n_k = \frac{(p(p-1)^k) \cdot k!}{(pk)!}$ to $n_{2k} = p^{2k}$.

Section 3.1 gives exact formulas, and Section 3.2 gives useful approximations.

3.1. Exact formulas.

Since the case of $k = 1$ was discussed in Example 1.2, we may assume $k \ge 2$ in the following.

Theorem 3.1. *For a prime p and $n = kp$ where $2 \le k \le p-1$, let n_a be the number of Sylow-p double cosets of S_n of size p^a, for each $k \le a \le 2k$. Then*

$$n_a = \frac{1}{p^a} \sum_{j=2k-a}^{k} \big((k-j)p\big)! j! \binom{k}{j}^2 \big(p(p-1)^j\big)(-1)^{j-(2k-a)} \binom{j}{2k-a}. \tag{3.1}$$

Proof. The result will follow from considering the following generating function. Let

$$f_{k,p}(x) = \sum_{i=0}^{k} \#\{\pi \in S_{kp} \mid |C_p^k \cap \pi^{-1} C_p^k \pi| = p^i\} x^i.$$

We claim that

$$f_{k,p}(x) = \sum_{i=0}^{k} \big((k-i)p)\big)! i! \binom{k}{i}^2 \big(p(p-1)(x-1)\big)^i. \tag{3.2}$$

First, to prove (3.1) from (3.2): note that the x^{2k-a} coefficient of $f_{k,p}$ is the number of $\pi \in S_{kp}$ such that $|C_p^k \pi C_p^k| = p^a$. If $|C_p^k \pi C_p^k| = p^a$, then there are exactly p^a elements $\sigma \in S_{kp}$ such that $C_p^k \pi C_p^k = C_p^k \sigma C_p^k$ (namely, the set of such σ is the double coset $C_p^k \pi C_p^k$ itself). Hence

$$n_a = \frac{1}{p^a}[x^{2k-a}]f_{k,p}(x) = \frac{1}{p^a} \sum_{j=2k-a}^{k} \big((k-j)p\big)!j!\binom{k}{j}^2 \big(p(p-1)\big)^j (-1)^{j-(2k-a)} \binom{j}{2k-a}.$$

To conclude, we prove that (3.2) holds. Fix k and p and write $f_{k,p}(x) = \sum_i a_i x^i$. Let σ_i be the cycle $\big((i-1)p+1, \dots, ip\big)$. Then a_i counts the number of $\pi \in S_{kp}$ such that the subset $R \subset \{1, 2, \dots, k\}$, of indices r which have the property that there exists another index s with $\pi \sigma_r \pi^{-1} \in \langle \sigma_s \rangle$, has exactly size i. (Here $r, s \in \{1, 2, \dots, k\}$.)

Then the x^i coefficient of $f_{k,p}(x+1)$ is $a_i + a_{i+1}\binom{i+1}{i} + \dots + a_k\binom{k}{i}$ and we want to show that

$$a_i + a_{i+1}\binom{i+1}{i} + \dots + a_k\binom{k}{i} = \big((k-i)p\big)!i!\binom{k}{i}^2 \big(p(p-1)\big)^i. \tag{3.3}$$

The right hand side of (3.3) counts the number of $\pi \in S_{kp}$ together with a distinguished subset $A \subset \{1, \dots, k\}$ of size i such that for each $a \in A$ there exists $b \in \{1, \dots, k\}$ satisfying $\pi \sigma_a \pi^{-1} \in \langle \sigma_b \rangle$. Indeed, concretely choose:

- a pair of subsets $A, B \subset \{1, \dots, k\}$ with $|A| = |B| = i$ – there are $\binom{k}{i}^2$ such choices;
- a bijection $\phi : A \to B$ – there are $i!$ such choices;
- for each $a \in A$ (noting that $|A| = i$), a bijection $r_a : \{(a-1)p+1, \dots, ap\} \to \{(\phi(a)-1)p + 1, \dots, \phi(a)p\}$ such that $r_a \sigma_i r_a^{-1} \in \langle \sigma_{\phi(a)} \rangle$ – there are $p(p-1)$ such choices, for instance by first choosing $r_a((a-1)p+1)$ from one of p possible values, then by choosing $r_a((a-1)p+2)$ from one of $p-1$ possible values, which then determines r_a; and
- a bijection $\tau : \{1, \dots, kp\} \setminus \bigcup_{a \in A}\{(a-1)p+1, \dots, ap\} \to \{1, \dots, kp\} \setminus \bigcup_{b \in B}\{(b-1)p+1, \dots, bp\}$ – notice the domain and codomain of τ each have size $(k-i)p$ so there are $((k-i)p)!$ such choices;

then take π to be defined by the $\{r_a\}_{a \in A}$ and τ, whose domains and codomains both have disjoint unions $\{1, \dots, kp\}$.

On the other hand, the left hand side of (3.3) creates the pair (π, A) as follows: first choose j such that $i \le j \le k$, then take a permutation π counted by a_j, that is, π satisfies $|R| = j$ where

$$R := \{r \in \{1, \dots, k\} \mid \exists\ s,\ \pi \sigma_r \pi^{-1} \in \langle \sigma_s \rangle\},$$

and then choose the distinguished set A to be one of the $\binom{j}{i}$ i-element subsets A of the j-element subset $R \subset \{1, \dots, k\}$. Thus (3.3) holds as desired, and this concludes the proof. ☐

Example 3.2. The first few cases of the generating function considered above are, for example,

- $f_{1,p}(x) = p! + p(p-1)(x-1)$,
- $f_{2,p}(x) = (2p)! + p! \cdot 4p(p-1)(x-1) + 2p^2(p-1)^2(x-1)^2$,
- $f_{3,p}(x) = (3p)! + (2p)! \cdot 9p(p-1)(x-1) + p! \cdot 18p^2(p-1)^2(x-1)^2 + 6p^3(p-1)^3(x-1)^3$.

3.2. **Some approximations.** A glance at the formula (3.1) shows it is not so easy to understand; an alternating sum with factorials and binomial coefficients. The following result gives sharp upper and lower bounds. They show, in a strong sense, that when p is large, most double cosets have size p^{2k}, uniformly in k. This implies that the number of double cosets is asymptotic to $\frac{(kp)!}{p^{2k}}$.

Theorem 3.3. *With notation as above, for all p and $1 \le k \le p-1$ we have that*

$$\frac{(kp)!}{p^{2k}}\left(1 - \frac{1}{(p-2)!}\right) \le n_{2k} \le \frac{(kp)!}{p^{2k}}.$$

Proof. From (3.1),

$$n_{2k} = \frac{1}{p^{2k}} \sum_{j=0}^{k} (-1)^j \big((k-j)p\big)!j!\binom{k}{j}^2 \big(p(p-1)\big)^j. \tag{3.4}$$

Note that the $j = 0$ term in the sum is $(kp)!$. The proof proceeds by showing that the other terms are super exponentially smaller than the $j = 0$ term. For $0 \le j \le k-1$ let

$$\Gamma_j = \big((k-j)p\big)!j!\binom{k}{j}^2\big(p(p-1)\big)^j,$$

so $n_{2k} = \frac{1}{p^{2k}}\sum_{j=0}^{k}(-1)^j\Gamma_j$. We compute

$$\begin{aligned}\frac{\Gamma_{j+1}}{\Gamma_j} &= \frac{\big((k-j)p-p\big)!(j+1)!\binom{k}{j+1}^2\big(p(p-1)\big)^{j+1}}{\big((k-j)p\big)!j!\binom{k}{j}^2\big(p(p-1)\big)^j}\\ &= \frac{(j+1)p(p-1)\left(\frac{k-j}{j+1}\right)^2}{\big((k-j)p\big)\big((k-j)p-1\big)\cdots\big((k-j)p-p+1\big)}\\ &= \frac{p(p-1)(k-j)^2}{(j+1)\big((k-j)p\big)\big((k-j)p-1\big)\cdots\big((k-j)p-p+1\big)}.\end{aligned}$$

Since $(p-1)(k-j) \le (k-j)p - 1$, the ratio is bounded above by

$$\frac{\Gamma_{j+1}}{\Gamma_j} \le \frac{1}{(j+1)\big((k-j)p-2\big)\cdots\big((k-j)p-p+1\big)} \le \frac{1}{(j+1)(p-2)!}. \tag{3.5}$$

It follows that $\Gamma_{j+1} < \Gamma_j$ and that the sum in (3.4) is an alternating sum of decreasing positive terms. Call $S_k = p_{2k} \cdot n_{2k} = \sum_{j=0}^{k}(-1)^j\Gamma_j$, then we have

$$\Gamma_0 - \Gamma_1 \le S_k \le \Gamma_0$$

by taking $j = 0$ in (3.5). Finally,

$$\Gamma_0 - \Gamma_1 = \Gamma_0\left(1 - \frac{\Gamma_1}{\Gamma_0}\right) \ge \frac{\Gamma_0}{(p-2)!}.$$

Thus

$$(kp)!\left(1 - \frac{1}{(p-2)!}\right) \le S_k \le (kp)!,$$

and dividing through by p^{2k} gives the result. □

Remark 3.4. (i) The usual manipulations with alternating sums show S_k is bounded above by $\Gamma_0 - \Gamma_1 + \cdots + \Gamma_{2b}$ and below by $\Gamma_0 - \Gamma_1 + \cdots - \Gamma_{2b+1}$ for any b.

(ii) For $k \le a \le 2k$, (3.1) gives an explicit formula for the quantity n_a. Similar techniques, not developed in detail here, show that the sum in n_a is dominated by the $j = 2k - a$ term. Thus, for $k \le a \le 2k$,

$$n_a \sim \frac{1}{p^a}\big((a-k)p\big)!(2k-a)!\binom{k}{a-k}^2\big(p(p-1)\big)^{2k-a}. \tag{3.6}$$

As a check, when $a = k$ (the smallest possible value for a), we know $n_k = k!(p-1)^k$, and so (3.1) and the computation in Example 1.2 agree.

(iii) The value of n_a falls off extremely rapidly from n_{2k}. Straightforward asymptotics show a super-exponential decrease: letting $u = a - k$ and $b = 2k - a$ and recalling that $k < p$ we observe from (3.6) that

$$\frac{n_a}{n_{2k}} \sim \big(p^2(p-1)\big)^v v!\binom{k}{u}^2\frac{(up)!}{(kp)!} \le p^{4v}\cdot 4^p \cdot \frac{(up)!}{(kp)!} = \left(\frac{p^4}{((k-v)p)^{p/2}}\right)^v \cdot \left(\frac{4}{((k-v)p)^{v/2}}\right)^p,$$

from which we can conclude, for example, that

$$\frac{n_a}{n_{2k}} = o(p^{-p/4}).$$

4. General case

Theorem 1.1 considers $f(n,p) = \mathbb{P}(P_n \cap P_n^x > 1)$ with P_n a Sylow p-subgroup of S_n. We begin by clarifying what probability is being computed. There are three possibilities:

(1) Pick, uniformly at random and independently, two Sylow p-subgroups from the list of all Sylow p-subgroups of S_n, i.e. $\mathrm{Syl}_p(S_n)$.
(2) Fix $P_n \in \mathrm{Syl}_p(S_n)$ and pick, uniformly, a Sylow subgroup from $\mathrm{Syl}_p(S_n)$.
(3) Fix $P_n \in \mathrm{Syl}_p(S_n)$, choose $x \in S_n$ uniformly and consider $P_n \cap P_n^x$.

In all cases, $P_n = P_n^x$ is allowed.

Lemma 4.1. *Under any of (1), (2) and (3), the probability* $\mathbb{P}(P_n \cap P_n^x > 1)$ *is the same.*

Proof. From Sylow's theorems, S_n acts transitively on $\mathrm{Syl}_p(S_n)$ by conjugation. The uniform distribution is invariant under conjugation, so clearly (1) and (2) give the same probability. With P_n fixed, $P_n^{gx} = P_n^x$ if and only if $g \in N_{S_n}(P_n)$. So the uniform distribution on $\mathrm{Syl}_p(S_n)$ assigns probability $\frac{1}{n!}|N_{S_n}(P_n)|$ to each, giving the equality between (2) and (3). □

Throughout, we will use the probabilistic set-up described in (3).

4.1. **Odd primes.** For a prime p, let $x \in S_n$ be an element of order p with fewer than p fixed points. Note that this uniquely defines the conjugacy class of x. Let $f'(n,p)$ be the probability that two random conjugates of x, say x^a and x^b with a,b uniform and independent in S_n both centralize a common element of order p (i.e. the centralizer of $\langle x^a, x^b\rangle$ has order divisible by p). As above, it suffices to consider all pairs x, x^b as b ranges uniformly over all b.

We note:

Lemma 4.2. $f(n,p) \le f'(n,p)$.

Proof. Let P and Q be Sylow p-subgroups of S_n. Let $x \in Z(P)$ have order p and fewer than p fixed points. If $Q = P^y$, then $x^y \in Z(Q)$. If $w \in P \cap Q$ has order p, then w commutes with x and x^y. Letting y range over all elements, the result follows. □

Thus, it suffices to prove the following.

Theorem 4.3. *If* $p \neq 2$, *then* $\lim_{n\to\infty} f'(n,p) = 0$.

The proof of Theorem 1.1 uses the following special case of results of Eberhard and Garzoni [EG21, EG22]. See in particular [EG22, Theorem 1.1].

Theorem 4.4 ([EG22])**.** *Let* $x_n \in S_n$ *be an element of odd order for each* $n \in \mathbb{N}$ *such that the number of fixed points* $F(x_n)$ *satisfies* $F(x_n)/n^{1/2} \to 0$ *as* $n \to \infty$. *Then the probability that two random conjugates of* x_n *generate* A_n *goes to* 1 *as* $n \to \infty$.

Remark 4.5. The probability in Theorem 4.4 can be taken either as the chance that $\langle x_n^a, x_n^b\rangle = A_n$ with $a, b \in S_n$ chosen uniformly and independently, *or* as the chance that two independent uniformly chosen elements of the class of x_n generate A_n. As in Lemma 4.1, they agree.

We also use the following elementary result.

Lemma 4.6. *Let* L *be a subgroup of* $G = S_n$.

(a) If L *acts primitively, then either* L *is cyclic of order* n *with* n *prime or* $C_G(L) = 1$.
(b) If L *acts transitively and* r *is a prime dividing* $|C_G(L)|$, *then* $r \mid n$.

Proof. Suppose $x \in C_G(L)$ has prime order r. Then the orbits of x are permuted by L. If L is primitive, there is only one such orbit. If L is transitive, all orbits must have the same size and the result follows. □

To begin the proof of Theorem 4.3, consider $P \in \mathrm{Syl}_p(A_n)$. Clearly $P \in \mathrm{Syl}_p(S_n)$ since p is odd. Let $z \in Z(P)$ be an element with $r \le p-1$ fixed points where $n = kp + r$. Then the probability that $P \cap P^x \neq 1$, for x uniform in S_n, is at most the probability that there exists a common element centralizing both z and z^x. By Theorem 4.4, this goes to 0 as long as $p/n^{1/2} \to 0$.

If p is fixed, clearly this holds, so it will be assumed that p is increasing. If say $p \log p < n^{1/2}$, the result similarly holds (although we will not use this fact). If $p \mid n$, then $r = 0$ and the result holds. We use the following result to deduce the result from the case $r = 0$.

Lemma 4.7. $f'(n,p) \le \max\{f'(\lambda p, p) \mid 1 \le \lambda \le n/p\}$.

Proof. Let $G = S_n$. We partition the conjugacy class x^G of x into disjoint subsets. If $y \in x^G$, let $H = H_y = \langle x, y\rangle$ and $\Omega = \Omega(y)$ denote the union of all H-orbits of size prime to p. Let $\Delta(\Omega)$ denote the set of conjugates y of x with $\Omega(y)$ a fixed subset.

Note that since x has fewer than p fixed points, H has fewer than p orbits on Ω. Suppose $w \in C_G(H)$ has order p. Then w acts on Ω. Since H has fewer than p orbits, w acts on each H orbit contained in Ω. By Lemma 4.6, w acts trivially on Ω.

Let Ω' be the complement of Ω. If Ω' is empty, then no element of order p centralizes H. Let x' and y' denote the restriction of x and y to Ω' (these are fixed point free permutations on Ω'). Note that as y ranges over $\Delta(\Omega)$, y' ranges uniformly over all fixed point free permutations of order p on Ω'. Since any p-element in $C_G(H)$ acts trivially on Ω, it follows that the probability that x and a random element of $\Delta(\Omega)$ are both centralized by an element of order p is precisely $f'(|\Omega'|, p)$.

The result follows since $|\Omega'| = \lambda p$ for some λ. □

By Theorem 4.4 it follows that $\lim_{p\to\infty} f'(\lambda p, p) = 0$ and Theorem 4.3 follows.

Remark 4.8. The argument shows that Theorem 1.1 holds uniformly in $2 < p \le n$. Using the ideas and results from [EG22], one could prove a more refined version of Lemma 4.7.

4.2. n **even,** $p = 2$**.** In this case $Z = Z(P_n)$ is an elementary 2-group. The same holds for $Z(P_n^x)$. Let $z \in Z$ be an involution with no fixed points. Consider the partition Δ of n into $\frac{n}{2}$ disjoint subsets of size 2 which are the orbits of z. Let A be the elementary abelian 2-subgroup preserving each subset of size 2. We will show that for a random g, the probability that $A \cap A^g \ne 1$ is bounded away from 0 and so also for $P_n \cap P_n^g$.

Note that $g\Delta$ is a random partition of the same sort. Let W be the number of matching pairs in Δ and $g\Delta$. Note that $W \ge 1$ if and only if $A \cap A^g \ne 1$. The arguments in [DHol02, §3] show that, when n is large, W has a limiting Poisson(1/2) distribution

$$\mathbb{P}(W = l) \to \frac{e^{-1/2}\cdot (1/2)^l}{l!} \quad \text{as } n \to \infty.$$

In particular,

$$\mathbb{P}(W > 0) \sim 1 - e^{-1/2} \quad \text{as } n \to \infty,$$

and so the probability that $A \cap A^g \ne 1$ is uniformly bounded away from 0.

4.3. n **odd,** $p = 2$**.** We show that the n even case implies the result for n odd. Choose an involution $z \in Z(P_n)$ with exactly 1 fixed point. Let z^g be a random conjugate of z. Note that $\langle z, z^g\rangle$ is a dihedral group that has exactly 1 orbit of odd size k. If $k < n$, then using the result for $n - k$, we see that the probability that $A \cap A^g \ne 1$ (with A the elementary abelian subgroup preserving each orbit of z) is bounded uniformly away from 0. The result now follows by noting that the probability that zz^g is an n-cycle goes to 0 as $n \to \infty$.

5. Double cosets of size $p|P_n|$

This section gives closed form formulas for the number of p-Sylow double cosets of S_n of second smallest size. The main result is the following.

Theorem 5.1. *Let p be a prime and $n \in \mathbb{N}$. Suppose the p-adic expansion of n is $\sum_{i=0}^{\infty} a_i p^i$. Let $P_n \in \mathrm{Syl}_p(S_n)$. Then the number of (P_n, P_n)-double cosets in S_n of size $p|P_n|$ is*

$$\begin{cases} \displaystyle\sum_{i=0}^{\infty} a_i a_{i+1} + \sum_{i=2}^{\infty} a_i & \text{if } p = 2,\\[2ex] \displaystyle\frac{|N_{S_n}(P_n) : P_n|}{p} \sum_{i=0}^{\infty} a_{i+1}\left(\binom{p+a_i}{p}(p-1)^{i(p-1)}(p-2)! - 1\right) & \text{if } p > 2. \end{cases}$$

We remark that Theorem 5.1 is proved following a useful lemma for general groups which yields a theorem for the number of maximal size double cosets. Recall from (2.3) that $|N_{S_n}(P_n) : P_n| = \prod_i (p-1)^{ia_i} \cdot a_i!$, when the p-adic expansion of n is $\sum_{i=0}^{\infty} a_i p^i$.

Lemma 5.2. *Let G be a finite group, p be a prime and $P \in \mathrm{Syl}_p(G)$. For $k \in \mathbb{N}$ such that $p^k \le |P|$, let*
$$d(p^k) := \big|\{Q \in \mathrm{Syl}_p(G) : |P : P \cap Q| = p^k\}\big|.$$
Then the number of (P,P)-double cosets in G of size $|P|p^k$ is
$$\frac{d(p^k)}{p^k}|N_G(P) : P|.$$

Proof. Let $g \in G$ and suppose $|PgP| = |P|p^k$. There exist $x_1, \dots, x_{p^k} \in P$ such that $PgP = \bigcup_{i=1}^{p^k} x_i gP$. Setting $Q_i := x_i gPg^{-1}x_i^{-1} \in \mathrm{Syl}_p(G)$, we obtain $|P : P \cap Q_i| = p^k$ for $i = 1, \dots, p^k$. Suppose that $Q_i = Q_j$. Then
$$x_j^{-1}x_i \in N_G(gPg^{-1}) \cap P \le gPg^{-1},$$
because gPg^{-1} is the unique Sylow p-subgroup of $N_G(gPg^{-1})$. Hence, $x_i g \in x_j gP$ and $x_i gP = x_j gP$. Consequently, $i = j$. This shows that each (P,P)-double coset gives rise to p^k Sylow p-subgroups Q of G with $|P : P \cap Q| = p$. Now for each $h \in N_G(P)$ we have
$$|PghP| = |PghPh^{-1}g^{-1}| = |PgPg^{-1}| = |PgP|$$
and $Q_i = x_i ghPh^{-1}g^{-1}x_i^{-1}$. Therefore, each Q arises from $|N_G(P) : P|$ double cosets. □

It is no coincidence that p^k divides $d(p^k)$. In fact, $P \cap Q$ is the stabilizer of Q under the action of P on $\mathrm{Syl}_p(G)$ by conjugation. Hence, $d(p^k)$ is p^k times the number of orbits of size p^k.

For the rest of this section, $G = S_n$.

Lemma 5.3. *Let p be a prime, $n \in \mathbb{N}$ and let $P \in \mathrm{Syl}_p(S_{p^n})$. Then P has a unique maximal subgroup of the form $P_1 \times \ldots \times P_p$, where $N_1 \cup \ldots \cup N_p = \{1, \dots, p^n\}$, $|N_1| = \ldots = |N_p| = p^{n-1}$ and $P_i \in \mathrm{Syl}_p(\mathrm{Sym}(N_i))$ for all $i \in \{1, \dots, p\}$.*

Proof. It is clear that P has such a subgroup $H = P_1 \times \ldots \times P_p$ corresponding to
$$N_i := \{(i-1)p^{n-1} + 1, (i-1)p^{n-1} + 2, \dots, ip^{n-1}\},$$
for instance. Suppose that there is another such subgroup $Q = Q_1 \times \ldots \times Q_p$ corresponding to a partition $M_1 \cup \ldots \cup M_p = \{1, \dots, p^n\}$. Since $P = HQ$, we have that $|H \cap Q| = \frac{1}{p}|H|$. By way of contradiction, suppose that $\{N_1, \dots, N_p\} \ne \{M_1, \dots, M_p\}$. Then at least two of the N_i split into smaller subsets of the form $N_i \cap M_j$. Since the subsets $N_i \cap M_j$ are the orbits of $H \cap Q$, this leads to the contradiction $|H \cap Q| < \frac{1}{p}|H|$. Hence, without loss of generality, $N_i = M_i$ for all $i \in \{1, \dots, p\}$, and $P_i = P \cap \mathrm{Sym}(N_i) = Q_i$ and $H = Q$. □

Lemma 5.4. *Let $n \in \mathbb{N}$ with $n \ge 2$, and let $P \in \mathrm{Syl}_2(S_{2^n})$. Then P has unique maximal subgroup of the form $W \wr V$, where W is a Sylow 2-subgroup of a symmetric group on 2^{n-2} letters and $V \cong C_2^2$ acts regularly on the four copies of W.*

Proof. We have $P = W \wr R \cong (W_1 \times \ldots \times W_4) \rtimes R$ where $\{1, \dots, 2^n\} = N_1 \cup \ldots \cup N_4$, $W_i \in \mathrm{Syl}_2(\mathrm{Sym}(N_i))$ and $R \cong C_2 \wr C_2$ is a Sylow 2-subgroup of $\mathrm{Sym}(\{N_1, \dots, N_4\})$; note that $W = 1$ when $n = 2$. Taking V to be the Klein four-subgroup of R gives us one subgroup $H = W \wr V$ of the desired form.

To prove uniqueness, we use a counting argument. The number of partitions of $\{1, \dots, 2^n\}$ into four subsets of size 2^{n-2} each is
$$\frac{2^n!}{(2^{n-2}!)^4 4!}.$$
The number of Sylow 2-subgroups of S_{2^k} is the $2'$-part of $2^k!$, call it t_k. Therefore, the number of subgroups of S_{2^n} of the form $W := W_1 \times \ldots \times W_4$ where each W_i is a Sylow 2-subgroup of a symmetric group on 2^{n-2} letters, is
$$\frac{2^n!}{(2^{n-2}!)^4 4!} \cdot t_{n-2}^4 = \frac{t_n}{3}.$$
The Sylow 2-subgroups of S_{2^n} containing W correspond one-to-one to the three Sylow 2-subgroups of S_4 (permuting the W_i). Since t_n is the number of Sylow 2-subgroups of S_{2^n}, each Sylow 2-subgroup P of S_{2^n} contains a unique subgroup of the form W. Finally, there is only one way to extend W to $W \wr V$ where V permutes the W_i regularly. □

Proof of Theorem 5.1. We write $G = S_n$ and $P = P_n$ for short. There exists a partition
$$\{1, \ldots, n\} = N_1 \cup \ldots \cup N_s$$
and $P_i \in \mathrm{Syl}_p(\mathrm{Sym}(N_i))$ such that $P = P_1 \times \ldots \times P_s$, where $s := \sum_{i=0}^{\infty} a_i$. By Lemma 5.2, it suffices to determine the number of $Q \in \mathrm{Syl}_p(G)$ such that $|P : P \cap Q| = p$. In this case $R := P \cap Q$ is a radical subgroup of G, i. e. P is the largest normal p-subgroup of $N_G(P)$. The radical p-subgroups of symmetric groups were classified by Alperin–Fong [AP90, (2A)]; see also [F20] for corrections.

It turns out that there is a refined partition $M_1 \cup \ldots \cup M_t$ of $\{1, \ldots, n\}$ where each M_i is a subset of some N_j, and $R_i \le \mathrm{Sym}(M_i)$ such that $R = R_1 \times \ldots \times R_t$. Moreover, each R_i is an iterated wreath product of the form $A_1 \wr \ldots \wr A_k$, where every $A_j \cong C_p^{e_j}$ (for some $e_j \in \mathbb{N}$) is elementary abelian and acts regularly on its support. (Note the case $k = 0$ i.e. $R_i = 1$ is allowed.) Hence, $|M_i| = p^{e_1 + \ldots + e_k}$ and
$$\log_p |R_i| = e_1 p^{e_2 + \ldots + e_k} + e_2 p^{e_3 + \ldots + e_k} + \ldots + e_k \le p^{e_1 + \ldots + e_k - 1} + p^{e_2 + \ldots + e_k - 1} + \cdots + p^{e_k - 1},$$
since $e_i \le p^{e_i - 1}$ (with equality if and only if $e_i = 1$ or $p = e_i = 2$). Thus
$$\log_p |R_i| \le \sum_{i=0}^{e_1 + \cdots + e_k - 1} p^i = \sum_{j=1}^{\infty} \left\lfloor \frac{|M_i|}{p^j} \right\rfloor = \log_p(|M_i|!).$$
Since $|P : R| = p$, we conclude that *either* $e_1 = \ldots = e_k = 1$, *or* $p = 2$ and $e_1 = \ldots = e_{k-1} = 1$ and $e_k = 2$.

Suppose first that $p > 2$. Then each R_i is a Sylow p-subgroup of the symmetric group on its support. This means that $N_i = M_i$ and $R_i = P_i$ for all but one i. For $i \ge 0$, we have a_{i+1} choices to fix a factor P_j of P such that $|N_j| = p^{i+1}$. The only way to decompose N_j into some M_k is to take p disjoint subsets each of size p^i, say $N_j = M_{k_1} \cup \ldots \cup M_{k_p}$. By Lemma 5.3, the M_{k_l} are uniquely determined up to order by the wreath structure of P_j. Since $P_r = R_r$ for all $r \ne j$, we have $a_i + p$ sets M_l of size p^i in total. Each Sylow p-subgroup Q containing R combines p of those M_l to one set of size p^{i+1}. We have $\binom{p+a_i}{p}$ possibilities to choose those sets M_l. For ease of notation, suppose that $M = M_1 \cup \ldots \cup M_p$ have been chosen. Now we need to count how many Sylow p-subgroups of $S_M := \mathrm{Sym}(M)$ contain $R_M := R_1 \times \ldots \times R_p$ with $R_i \in \mathrm{Syl}_p(\mathrm{Sym}(M_i))$. Each such Sylow p-subgroup P_M lies inside $N_{S_M}(R_M) \cong (R_1 \rtimes C_{p-1}^i) \wr S_p$. On the other hand, $N_{S_M}(P_M) \cong P_M \rtimes C_{p-1}^{i+1}$. Hence, the number of Sylow p-subgroups of S_M containing R_M is
$$|N_{S_M}(R_M) : N_{S_M}(P_M)| = \frac{(p-1)^{ip} p!}{(p-1)^{i+1} p} = (p-1)^{i(p-1)}(p-2)!.$$
For each choice of N_j there is just one refined partition $M = M_1 \cup \ldots \cup M_p$ leading to $Q = P$. This possibility needs to be subtracted. This proves the theorem for $p > 2$.

Finally, let $p = 2$. The subgroups Q constructed above also exist here. The corresponding number simplifies to $\sum a_i a_{i+1}$ since $a_i \in \{0, 1\}$. Let $i \ge 2$ be such that $a_i = 1$. Without loss of generality, let $|N_i| = 2^i$. Let $P_i \le \mathrm{Sym}(N_i)$ be the corresponding factor of P. By Lemma 5.4, P_i has a unique maximal subgroup $R_i \cong W \wr V = W^4 \rtimes V$ such that W is a Sylow 2-subgroup of some $S_{2^{i-2}}$ and $V \cong C_2^2$ permutes the conjugates of W regularly. Since $N_{\mathrm{Sym}(N_i)}(R_i) \cong W \rtimes S_4$, the Sylow 2-subgroups Q containing R_i correspond one-to-one to the three Sylow 2-subgroups of S_4. One of them equals P. So for each i with $a_i = 1$, we obtain one (additional) double coset of size $2|P|$. This yields the second sum $\sum_{i \ge 2} a_i$ in the formula. □

From the proofs of Lemma 5.2 and Theorem 5.1, one can extract an algorithm to construct the double cosets of size $p|P_n|$.

6. Remarks and problems

Our original goal was to "understand the Sylow-p double cosets of S_n". We approach this by counting; how many double cosets are there and what are their sizes? There is still much that is not known. For example, when $p = 2$ then Theorem 1.1(b) shows that $f(n, 2)$ is bounded away from 0. We believe in fact that equality holds, although we do not know the limiting distribution for $|P_n \cap P_n^x|$. It is further natural to ask:

- Are there 'nice labels' for the double cosets?

- What are the structure constants when multiplying double cosets?
- Over a field of characteristic p, the Hecke algebra
$$\mathcal{H}_n(k) = L_k(P_n \setminus S_n/P_n) = \mathrm{End}_{S_n}(\mathbb{1}_{P_n}^{S_n})$$
is not semisimple. As mentioned in the introduction, when p is odd, we know from [GL18, Corollary B] that the number of irreducible representations of $\mathcal{H}_n(k)$ is equal to $|\mathcal{P}(n)|$, the number of partitions of n, whenever n is not a power of p (barring small exceptions when $p = 3$ and $n \leq 10$). Conversely, if $n = p^\ell$ for some $\ell \in \mathbb{N}$ then $\mathcal{H}_n(k)$ admits exactly $|\mathcal{P}(n)|-2$ irreducible representations.

  Moreover, in a recent (unpublished) manuscript, Giannelli and Law were able to completely describe those irreducible characters χ of S_n such that $[\chi, (\mathbb{1}_{P_n})^{S_n}] = 1$. This result, together with [CR81, Chapter 11D], allows us to determine the exact number of 1-dimensional representations of $\mathcal{H}_n(k)$ and therefore to compute the k-dimension of its abelianisation.

But, can we say more? Does $\mathcal{H}_n(k)$ have some kind of nice structure? For instance, is it Frobenius or quasi-Frobenius? (See [CR62] for background on quasi-Frobenius algebras.) For the roughly parallel problems for finite groups G with a split BN-pair, there *are* nice answers to these additional questions.

- The Yokonuma algebra [Y67] gives a nice description of $U \setminus G/U$, closely tied to Bruhat decompositions.
- At least in type A and elsewhere [KMS23], there are useful descriptions of the structure constants.
- The work of Tinberg [T80] summarised in the introduction shows that $L_k(U \setminus G/U)$ *is* Frobenius (among many other things).

All we want is to let $q \to 1$ in type A(!). Moreover, work of Kessar–Linckelmann suggests that there is trouble even in the simplest case $C_p \leq S_p$. They find $L_k(C_p \setminus S_p/C_p)$ is Frobenius for $p \in \{3, 5\}$ but not quasi-Frobenius for $p \geq 7$ [KL25]. This paper develops general tools for studying properties such as self-injectivity for Hecke algebras for general groups over general fields.

We would like a more quantitative version of Theorem 1.1, along the lines of Section 4. We would like analogues of the counting theorems for n_a for the case of general n.

References

[AP90] J. L. Alperin and P. Fong, Weights for symmetric and general linear groups, *J. Algebra* **131** (1990), 2–22.

[BD24] L. Bartholdi and P. Diaconis, An algorithm for uniform generation of unlabeled trees (Pólya trees), with an extension of Cayley's formula, `arXiv:2411.17613 [math.CO]`.

[Car72] R. W. Carter, *Simple groups of Lie type,* Pure and applied mathematics **28**, Wiley, 1972.

[Car85] R. W. Carter, *Finite groups of Lie type,* Wiley, 1985.

[Cur70] C. W. Curtis, *Modular representations of finite groups with split* (B, N)*-pairs,* Lecture Notes in Mathematics **131**, Springer, 1970.

[Cur99] C. W. Curtis, *Pioneers of representation theory: Frobenius, Burnside, Schur, Brauer,* History of Mathematics **15**, American Mathematical Society, Providence, 1999.

[CR62] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras,* Interscience, New York, 1962.

[CR81] C. W. Curtis and I. Reiner, *Methods of representation theory: with applications to finite groups and orders, vol. 1*, John Wiley & Sons, New York, 1981.

[DHol02] P. Diaconis and S. Holmes, Random walks on trees and matchings, *Electron. J. Probab.* **7** (2002), 1–17.

[DHow25] P. Diaconis and M. Howes, Random sampling of contingency tables and partitions: two practical applications of the Burnside process, *Technical report*, Department of Statistics, Stanford University.

[DMal21] P. Diaconis and M. Malliaris, Complexity and randomness in the Heisenberg groups (and beyond). *N. Z. J. Math.* **52** (2021), 403–426.

[DRS23] P. Diaconis, A. Ram and M. Simper, Double coset Markov chains, *Forum Math. Sigma* **11**:e2 (2023), 1–45.

[DSi22] P. Diaconis and M. Simper, Statistical enumeration of groups by double cosets, *J. Algebra* **607** (2022), 214–246.

[DZ23] P. Diaconis and Z. Zhong, Hahn polynomials and the Burnside process, *Ramanujan J.* **61** (2023), 567–595.

[DZ25] P. Diaconis and Z. Zhong, Counting the number of group orbits by marrying the Burnside process with importance sampling, `arXiv:2507.11731 [math.PR]`.

[EG21] S. Eberhard and D. Garzoni, Random generation with cycle type restrictions, *Algebr. Comb.* **4**(1) (2021), 1–25.

[EG22] S. Eberhard and D. Garzoni, Probability of generation by random permutations of given cycle type, `arXiv:2205.07573 [math.GR]`.

[F20] P. Fong, The Alperin weight conjecture for symmetric and general linear groups revisited, *J. Algebra* **558** (2020), 395–410.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.14.0*, 2024, (https://www.gap-system.org).

[Gia21] E. Giannelli, McKay bijections for symmetric and alternating groups, *Algebra Number Theory* **15**(7) (2021), 1809–1835.

[GL18] E. Giannelli and S. Law, On permutation characters and Sylow p-subgroups of $\mathfrak{S}_n$, *J. Algebra* **506** (2018), 409–428.

[GJ02] L. Goldberg and M. Jerrum, The Burnside process converges slowly, *Comb. Probab. Comput.* **11**(1) (2002), 21–34.

[GO96] A. Granville and K. Ono, Defect zero p-blocks for finite simple groups, *Trans. Amer. Math. Soc.* **348** (1996), 331–347.

[Gre78] J. A. Green, On a theorem of H. Sawada, *J. London Math. Soc.* (2) **18** (1978), 247–252.

[JK81] G. James and A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics and its Applications, vol. 16, Addison-Wesley Publishing Co., Reading, Mass., 1981.

[J93] M. Jerrum, Uniform Sampling Modulo a Group of Symmetries Using Markov Chain Simulation, in J. Friedman (ed.) *Expanding Graphs, Proceedings of a DIMACS Workshop*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **10**, DIMACS/AMS, 1993 (pp. 37–47).

[Kal48] L. Kaloujnine, La structure des p-groupes de Sylow des groupes symétriques finis, *Ann. Sci. École Norm. Sup.* (3) **65** (1948), 239–276.

[Kel03] T. Keller, Orbits in finite group actions, in C. M. Campbell, E. F. Robertson, G. C. Smith (eds.) *Groups St Andrews 2001 in Oxford*, London Mathematical Society Lecture Note Series **305**, Cambridge University Press, 2003 (pp. 306–331).

[Kle05] A. Kleshchev, *Linear and projective representations of symmetric groups,* Cambridge Tracts in Mathematics, Cambridge University Press, 2005.

[KL25] R. Kessar and M. Linckelmann, On some Hecke algebras for p-blocks of finite groups algebras, *preprint*.

[KMS23] R. Kessar, G. Malle and J. Semeraro, The principal block of a $\mathbb{Z}_l$-spets and Yokonuma type algebras, *Algebra Number Theory* **17**:2 (2023), 397–433.

[L00] A. Legendre, *Théorie des Nombres,* Firmin Didot Frères, fourth edition, 1900.

[M04] M. Meo, The mathematical life of Cauchy's group theorem, *Hist. Math.* **31** (2) (2004), 196–221.

[N98] G. Navarro, *Characters and Blocks of Finite Groups,* London Mathematical Society Lecture Note Series **250**, Cambridge University Press, 1998.

[OEIS23] R. Stanley, A360808, Number of double cosets of the Sylow 2-subgroup of the symmetric group S_n, 2023, https://oeis.org/A360808.

[O94] J. B. Olsson, *Combinatorics and representations of finite groups*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, Heft 20, 1994.

[Ren24] P. Renteln, Counting Sylow double cosets in the symmetric group, *Discrete Math.* **347** (10) (2024), 114109.

[Ric69] F. Richen, Modular representations of split (B, N)-pairs, *Trans. Am. Math. Soc.* **140** (1969), 435–460.

[Saw77] H. Sawada, A characterization of modular representations of finite groups with split (B, N)-pairs, *Math. Z.* **155** (1977), 29–42.

[Sta99] R. P. Stanley, *Enumerative Combinatorics, volume 2,* Cambridge Studies in Advanced Mathematics **62**, Cambridge University Press, 1999.

[Suz82] M. Suzuki, *Group theory I,* Springer Berlin, Heidelberg, 1982.

[T80] N. Tinberg, Modular representations of finite groups with unsaturated split (B, N)-pairs, *Can. J. Math.* **32**(3) (1980), 714–733.

[W16] M. Wildon, Sylow subgroups of symmetric groups, 2016, https://wildonblog.wordpress.com/2016/11/27/sylow-subgroups-of-symmetric-groups/.

[Y67] T. Yokonuma, Sur la structure des anneaux de Hecke d'un groupe de Chevalley fini, *C. R. Acad. Sci. Paris Ser. I Math.* **264** (1967), 344–347.

[ZM96] V. I. Zenkov and V. D. Mazurov, On the intersection of Sylow subgroups in finite groups, *Algebra i Logika* **35**(4) (1996), 424–432.

(P. Diaconis) Department of Mathematics, Stanford University, 390 Jane Stanford Way, Stanford, 94305, California, USA
Email address: diaconis@math.stanford.edu

(E. Giannelli) Dipartimento di Matematica e Informatica U. Dini, Viale Morgagni 67/a, Firenze, Italy
Email address: eugenio.giannelli@unifi.it

(R. Guralnick) Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA
Email address: guralnic@usc.edu

(S. Law) School of Mathematics, Watson Building, University of Birmingham, Edgbaston, Birmingham B15 2TT, UK
Email address: s.law@bham.ac.uk

(G. Navarro) Departament de Matemàtiques, Universitat de València, 46100 Burjassot, València, Spain
Email address: gabriel@uv.es

(B. Sambale) Institut für Algebra, Zahlentheorie und Diskrete Mathematik, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany
Email address: sambale@math.uni-hannover.de

(H. Spink) Department of Mathematics, University of Toronto, 40 St. George St., Toronto, ON, Canada
Email address: hunter.spink@utoronto.ca