

THE LIE MODULE OF THE SYMMETRIC GROUP

KARIN ERDMANN AND KAI MENG TAN

ABSTRACT. We provide an upper bound of the dimension of the maximal projective submodule of the Lie module of the symmetric group of n letters in prime characteristic p , where $n = pk$ with $p \nmid k$.

1. INTRODUCTION

The Lie module of the symmetric group \mathfrak{S}_n appears in many contexts; in particular it is closely related to the free Lie algebra. One possible approach is to view it as the right ideal of the group algebra $F\mathfrak{S}_n$, generated by the ‘Dynkin-Specht-Wever element’

$$\omega_n := (1 - c_2)(1 - c_3) \cdots (1 - c_n)$$

where c_k is the k -cycle $(1, 2, \dots, k)$. We write $\text{Lie}(n) = \omega_n F\mathfrak{S}_n$ for this Lie module.

It is well-known that $\omega_n^2 = n\omega_n$, so if n is non-zero in F then $\text{Lie}(n)$ is a direct summand of the group algebra and hence is projective. We are interested in this module when F has prime characteristic p and when p divides n . In this case ω_n is nilpotent, and therefore $\text{Lie}(n)$ always has non-projective summands, and its module structure is not well-understood in general.

The module $\text{Lie}(n)$ occurs in the context of algebraic topology, specifically as a homology group of topological spaces related to braid groups, configuration spaces, and Goodwillie towers. Selick and Wu [SW1] relate certain coalgebra decompositions of the tensor algebra to decompositions of the loop suspension of a p -torsion suspension where p is a prime. In this context, one needs to know a maximal projective submodule, called $\text{Lie}^{\max}(n)$, of the Lie module $\text{Lie}(n)$. Since $\text{Lie}(n)$ is a finite-dimensional module, it has a direct sum decomposition of the form $\text{Lie}(n) = \text{Lie}(n)_{pr} \oplus \text{Lie}(n)_{pf}$, unique up to isomorphism, where $\text{Lie}(n)_{pr}$ is projective and $\text{Lie}(n)_{pf}$ does not have any non-zero projective summand. Then $\text{Lie}^{\max}(n)$ is isomorphic to $\text{Lie}(n)_{pr}$. The projective modules for the symmetric groups over positive characteristic are not known, and this is a very difficult open problem. Therefore

Date: June 2009.

2000 Mathematics Subject Classification. 20C30.

The second author thanks the Mathematical Institute, Oxford, for its hospitality during his visit in 2006, during which most of the work appearing here was done, and acknowledges support by MOE’s Academic Research Fund R-146-000-089-112.

one cannot expect to find the module $\text{Lie}^{\max}(n)$ in general. For the applications it would however be good to find upper bounds for the dimension of $\text{Lie}^{\max}(n)$.

When $n = pk$ and p does not divide k , a parametrisation of the indecomposable summands of $\text{Lie}(n)_{pf}$ was given in [ES]. Here we exploit this result to obtain an upper bound for the dimension of $\text{Lie}^{\max}(n)$. The general principle is quite easy. If P is a Sylow p -subgroup of a finite group G , then one may consider the restriction of any FG -module W to FP , which we denote as $\text{Res}_P^G W$. Then $\text{Res}_P^G W_{pr}$ is a direct summand of $(\text{Res}_P^G W)_{pr}$ and therefore

$$\dim W_{pr} \leq \dim (\text{Res}_P^G W)_{pr} \leq \dim W - \dim (\text{Res}_P^G W)_{pf}.$$

Thus, when $G = \mathfrak{S}_n$ and $W = \text{Lie}(n)$, we have

$$\dim \text{Lie}^{\max}(n) \leq (n-1)! - \dim (\text{Res}_P^{\mathfrak{S}_n} \text{Lie}(n))_{pf}.$$

In this paper, we provide in particular a recursive formula for computing $\dim (\text{Res}_P^{\mathfrak{S}_n} \text{Lie}(n))_{pf}$.

We give a brief summary. The main task is, via a Mackey formula, to count certain cosets. The group of interest is a group D , which is a regular subgroup of \mathfrak{S}_{kp} isomorphic to $\mathfrak{S}_p \times \mathfrak{S}_k$. We take it as the subgroup $\Delta_k \mathfrak{S}_p \times \mathfrak{S}_k^{[p]}$ of a wreath product $\mathfrak{S}_p \wr \mathfrak{S}_k$, where $\mathfrak{S}_k^{[p]}$ is a fixed top group, and $\Delta_k \mathfrak{S}_p$ is the diagonal of the base group. The problem reduces to that of counting cosets Dx where $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. This intersection is generated by a fixed-point-free element of order p , and we can take this to be $(\Delta_k \pi)^x = y$ where $y \in P$ and π is the standard p -cycle in \mathfrak{S}_p .

The group P is a direct product of iterated wreath products, and one can reduce the problem to the factors. Write R_m for a Sylow p -subgroup of $\mathfrak{S}_{p^{m+1}}$, then R_m is the semi-direct product of B_m with a cyclic group of order p , where B_m is the direct product of p copies of R_{m-1} with disjoint supports. Then one has to understand x, y with $(\Delta_{p^m} \pi)^x = y \in R_m$. We introduce elements $z_{m,t}$ which conjugate $\Delta_{p^m} \pi$ to fixed-point-free elements in $R_m \setminus B_m$ (here $t \in \mathbb{Z}_p^*$; see Definition 5.3). Let $H \subseteq R_m$ be the elementary abelian p -subgroup generated by the individual cycles of $\Delta_{p^m} \pi$, and let R_m^0 be the subgroup of the base group B_m consisting of the elements which fix the last block of size p^m pointwise. With this we describe now a transversal for the desired cosets.

Firstly, for $m \in \mathbb{Z}_{\geq 0}$, define $Y_m = \{hz_{m,t}b : h \in H, t \in \mathbb{Z}_p^*, b \in R_m^0\}$; then we define recursively

$$X_{p^{-1}} = \emptyset, \quad X_{p^m} := Y_m \cup \prod_{i=1}^p X_{p^{m-1}}[i]$$

where $\prod_{i=1}^p X_{p^{m-1}}[i]$ is the direct product of p copies of the set $X_{p^{m-1}}$ with disjoint supports. Finally, for $d \in \mathbb{Z}^+$, X_d is defined to be the direct product of such sets X_{p^m} , according to the direct factors of a fixed Sylow p -subgroup of \mathfrak{S}_{pd} . Then the set X_{k-1} is a section for the cosets Dx with $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. This gives a recursive formula for the number of these cosets, as well as our upper bound for the dimension of $\text{Lie}^{\max}(kp)$. For fixed p , the size of

X_{k-1} is in the order of $p^{p^{2m}}$ where p^m is the largest power of p occurring in the p -adic expansion of k ; hence our upper bound grows exponentially with k .

We give an outline of this paper. After introducing notation, we reduce in Section 3 the problem of computing $\dim(\text{Res}_P^{\mathfrak{S}_{kp}} \text{Lie}(pk))_{pf}$ to that of computing the number of certain right cosets. In Section 4, we study the Sylow p -subgroup P of \mathfrak{S}_{pk} , and we introduce a combinatorial object called p -composition associated to an element of P . This may be of independent interest. In Section 5, we obtain a ‘good’ subset containing a transversal of the right cosets which we wish to parametrise, and proceed to obtain a transversal in Section 6. We end the paper with a recursive formula for the dimension of $(\text{Res}_P^{\mathfrak{S}_{kp}} \text{Lie}(pk))_{pf}$.

We remark that the same general principle has been used in [CT] to find an upper bound for $\dim(\text{Lie}^{\max}(n))$ in characteristic 2, and where $n \equiv 2 \pmod{4}$. They computed explicitly the projective submodules of $\text{Res}_P^{\mathfrak{S}_n} \text{Lie}(n)$, and obtained a recursive formula for the upper bound. However, it is not clear whether the methods used there can be generalised to other characteristics. Our results here, when specialised to $p = 2$, agree with theirs.

For background on representation theory of finite groups we refer the reader to [B].

2. NOTATIONS

In this section, we introduce the notations to be used throughout this paper.

For $a, b \in \mathbb{Z}_{\geq 0}$ with $a < b$, let

$$\begin{aligned} [a, b] &= \{x \in \mathbb{Z} \mid a \leq x \leq b\}, \\ (a, b] &= \{x \in \mathbb{Z} \mid a < x \leq b\}, \\ [a, b) &= \{x \in \mathbb{Z} \mid a \leq x < b\}. \end{aligned}$$

We denote by \mathfrak{S}_n the group of permutations of the set $[1, n]$. For $m < n$, we identify \mathfrak{S}_m with the subgroup of \mathfrak{S}_n fixing $(m, n]$ pointwise.

Let $a, b \in \mathbb{Z}^+$. For $\sigma \in \mathfrak{S}_a$, define $\sigma^{[b]} \in \mathfrak{S}_{ab}$ by

$$((i-1)b + j)\sigma^{[b]} = (i\sigma - 1)b + j$$

for all $i \in [1, a]$ and $j \in [1, b]$, so that $\sigma^{[b]}$ permutes the a successive blocks of size b in $[1, ab]$ according to σ . Clearly, the map $\sigma \mapsto \sigma^{[b]}$ is an injective group homomorphism.

For $\tau \in \mathfrak{S}_b$ and $r \in [1, s]$, define $\tau[r] \in \mathfrak{S}_{sb}$ by

$$((i-1)b + j) \tau[r] = \begin{cases} (r-1)b + j\tau, & \text{if } i = r, \\ (i-1)b + j, & \text{otherwise,} \end{cases}$$

for all $i \in [1, s]$ and $j \in [1, b]$, so that $\tau[r]$ acts on the r -th successive block of size b in $[1, sb]$ according to τ , and fixes everything else. Note that as

a permutation on the set $((r-1)b, rb]$, $\tau[r]$ is independent of s (as long as $s \geq r$). As this notation also depends on b (i.e. the degree of the symmetric group in which τ lies), we will specify b when it is unclear from the context what b is.

In addition, define $\Delta_a \tau \in \mathfrak{S}_{ab}$ by $\Delta_a \tau = \prod_{i=1}^a \tau[i]$, so that $\Delta_a \tau$ permutes each of the a successive blocks of size b in $[1, ab]$ simultaneously according to τ . Clearly, the maps $\tau \mapsto \tau[r]$ and $\tau \mapsto \Delta_a \tau$ are injective group homomorphisms.

If $H \subseteq \mathfrak{S}_a$, $K \subseteq \mathfrak{S}_b$ and $r \in \mathbb{Z}^+$, we write

$$\begin{aligned} H^{[b]} &= \{h^{[b]} \mid h \in H\}, \\ K[r] &= \{k[r] \mid k \in K\}, \\ \Delta_a K &= \{\Delta_a k \mid k \in K\}. \end{aligned}$$

We note the following lemma, whose proof is straightforward.

Lemma 2.1. *Let $\sigma \in \mathfrak{S}_a$ and $\tau \in \mathfrak{S}_b$.*

- (1) *If $r \in [1, a]$, then $\tau[r]^{\sigma^{[b]}} = \tau[r\sigma]$.*
- (2) *$\sigma^{[b]}(\Delta_a \tau) = (\Delta_a \tau)\sigma^{[b]}$.*

Assume $n = pk$. Given a set partition of $[1, n]$ into k blocks of size p , we have subgroups D of \mathfrak{S}_n which are isomorphic to $\mathfrak{S}_p \times \mathfrak{S}_k$ where each factor acts regularly: the factor \mathfrak{S}_k permutes the blocks according to \mathfrak{S}_k , and elements of the factor \mathfrak{S}_p act on each block simultaneously, and these two actions commute. Any two such groups are conjugate in \mathfrak{S}_n .

Such a group D can be viewed as a subgroup of a wreath product $\mathfrak{S}_p \wr \mathfrak{S}_k$: let $\mathfrak{S}_k^{[p]}$ be the fixed top group; its centralizer in the base group is the diagonal product $\Delta_k \mathfrak{S}_p$ which is isomorphic to \mathfrak{S}_p , and then one can take $D = \Delta_k \mathfrak{S}_p \times \mathfrak{S}_k^{[p]}$.

One can equally well take D to be the subgroup $\Delta_p \mathfrak{S}_k \times \mathfrak{S}_p^{[k]}$ of $\mathfrak{S}_k \wr \mathfrak{S}_p$ with the analogous construction.

3. THE PROBLEM

Assume F is field of characteristic p , and let $k \in \mathbb{Z}^+$ with $p \nmid k$ and let $n = pk$. Let $D \leq \mathfrak{S}_n$ be a direct product of \mathfrak{S}_p with \mathfrak{S}_k where each factor acts regularly, as described above in Section 2. The p -th symmetrisation of $\text{Lie}(k)$, denoted $S^p(\text{Lie}(k))$, is defined in [ES, §4] as follows. Taking $D = \Delta_p \mathfrak{S}_k \times \mathfrak{S}_p^{[k]}$, then $S^p(\text{Lie}(k))$ is the right ideal of $F\mathfrak{S}_n$ generated by the element $s_p^{[k]} \Delta_p \omega_k$ in FD , where $s_p = \sum_{\sigma \in \mathfrak{S}_p} \sigma \in F\mathfrak{S}_p$ and ω_k is the Dynkin-Specht-Wever element generating $\text{Lie}(k)$. This module is related to $\text{Lie}(n)$ as follows.

Theorem 3.1. [ES, Theorem 10] *Assume $n = pk$ where p does not divide k . Then there is a short exact sequence of right $F\mathfrak{S}_n$ -modules*

$$0 \rightarrow \text{Lie}(n) \rightarrow eF\mathfrak{S}_n \rightarrow S^p(\text{Lie}(k)) \rightarrow 0$$

where e is an idempotent in \mathfrak{S}_n .

As a corollary, we see that $\Omega(S^p(\text{Lie}(k))) \cong \text{Lie}(n)_{pf}$ (where here, and hereafter, Ω is the Heller operator, taking a module to the kernel of its projective cover).

Let Λ_k be the right ideal of FD generated by $s_p^{[k]} \Delta_p \omega_k$. Then $S^p(\text{Lie}(k)) \cong \text{Ind}_D^{\mathfrak{S}_n} \Lambda_k$ as right \mathfrak{S}_n -modules. In our context, we prefer to take D of the form $D = \Delta_k \mathfrak{S}_p \times \mathfrak{S}_k^{[p]}$. Then the module Λ_k has the following description. The action of $\Delta_k \mathfrak{S}_p$ on Λ_k is trivial, while that of $\mathfrak{S}_k^{[p]}$ on Λ_k is equivalent to that of \mathfrak{S}_k on $\text{Lie}(k)$. That is, $\Lambda_k \cong F \boxtimes \text{Lie}(k)$, the outer tensor product.

Let P be a fixed Sylow p -subgroup of \mathfrak{S}_n . By Mackey's formula, we have

$$\begin{aligned} \text{Res}_P^{\mathfrak{S}_n} S^p(\text{Lie}(k)) &\cong \text{Res}_P^{\mathfrak{S}_n} \text{Ind}_D^{\mathfrak{S}_n} \Lambda_k \\ &= \bigoplus_{x \in D/\mathfrak{S}_n \setminus P} \text{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x). \end{aligned}$$

Proposition 3.2.

- (1) If $(\Delta_k \mathfrak{S}_p)^x \cap P = 1$, then $\text{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ is projective.
- (2) If $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, then $\text{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ has no projective summand.

Proof. If $(\Delta_k \mathfrak{S}_p)^x \cap P = 1$, then $\Delta_k \mathfrak{S}_p \cap P^{x^{-1}} = 1$; we claim that in this case $\text{Res}_{D \cap P^{x^{-1}}} \Lambda_k$ is projective, so that (1) follows. To prove the claim, let $Q = D \cap P^{x^{-1}}$, then $\Delta_k \mathfrak{S}_p \cap Q = 1$. If R is a Sylow p -subgroup of $\Delta_k \mathfrak{S}_p$, then all D -conjugates of R lie in $\Delta_k \mathfrak{S}_p$, since $\Delta_k \mathfrak{S}_p$ is normal in D ; thus $R^d \cap Q = 1$ for all $d \in D$. Now, Λ_k is by construction relatively R -projective, so that Λ_k is a direct summand of $\text{Ind}_R^D U$ for some R -module U . It follows that $\text{Res}_Q \Lambda_k$ is a direct summand of $\text{Res}_Q \text{Ind}_R^D U$. But by Mackey's formula, $\text{Res}_Q \text{Ind}_R^D U = \bigoplus_{d \in R/D \setminus Q} \text{Ind}_{R^d \cap Q}^Q (U \otimes x)$. Since $R^d \cap Q = 1$, each summand $\text{Ind}_{R^d \cap Q}^Q (U \otimes x)$ is projective. Thus, $\text{Res}_Q \text{Ind}_R^D U$ and $\text{Res}_Q \Lambda_k$ are projective.

If $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, let $\sigma \in \mathfrak{S}_p$ such that $(\Delta_k \sigma)^x \in (\Delta_k \mathfrak{S}_p)^x \cap P$. Then since $\Delta_k \sigma$ acts trivially on the entire module Λ_k , we see that $\text{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ cannot have any projective summand. \square

In view of Proposition 3.2, let S be the set of all double coset representatives in $D/\mathfrak{S}_n \setminus P$ such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. Then we have

Corollary 3.3. Assume $n = pk$ with $p \nmid k$. Then

$$(\text{Res}_P^{\mathfrak{S}_n} S^p(\text{Lie}(k)))_{pf} \cong \bigoplus_{x \in S} \text{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x).$$

The following is the main result of this section.

Theorem 3.4. Assume $n = pk$ with $p \nmid k$. We have

$$\dim((\text{Res}_P^{\mathfrak{S}_n} \text{Lie}(n))_{pf}) = (p-1)(k-1)! \sum_{x \in S} [P : D^x \cap P].$$

Proof. Restriction is exact, hence we have a short exact sequence

$$0 \rightarrow \text{Res}_P \text{Lie}(n) \rightarrow \text{Res}_P(eF\mathfrak{S}_n) \rightarrow \text{Res}_P S^p(\text{Lie}(k)) \rightarrow 0.$$

Since $\text{Res}_P(eF\mathfrak{S}_n)$ remains projective as an FP -module, we see that

$$\begin{aligned} (\text{Res}_P \text{Lie}(n))_{pf} &\cong \Omega(\text{Res}_P S^p(\text{Lie}(k))) \\ &\cong \bigoplus_{x \in S} \Omega(\text{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x)) \end{aligned}$$

by Corollary 3.3. To prove the theorem, we show that $\Omega(\text{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x))$ for $x \in S$ is isomorphic to $\text{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \text{Lie}(k)) \otimes x)$ and that $\Omega(F)$ has dimension $p - 1$.

Recall that $\Lambda_k \cong F \boxtimes \text{Lie}(k)$. Since $\text{Lie}(k)$ is a projective $F\mathfrak{S}_k$ -module, we see that $\Omega(\Lambda_k) \cong \Omega(F) \boxtimes \text{Lie}(k)$. Furthermore, $\Omega(F)$ can be described as follows: the natural p -dimensional permutation module of $F\mathfrak{S}_p$ is indecomposable projective and has F as a quotient, so that $\Omega(F)$ is its maximal submodule, of dimension $(p - 1)$. Moreover, $\Omega(F)$ remains indecomposable when restricted to any subgroup of \mathfrak{S}_p of order p . Now, the short exact sequence

$$0 \rightarrow \Omega(F) \boxtimes \text{Lie}(k) \rightarrow P(\Lambda_k) \rightarrow \Lambda_k \rightarrow 0,$$

where $P(\Lambda_k)$ denotes the projective cover of Λ_k , gives the following short exact sequence

$$\begin{aligned} (*) \quad 0 \rightarrow \text{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \text{Lie}(k)) \otimes x) &\rightarrow \text{Ind}_{D^x \cap P}^P(P(\Lambda_k) \otimes x) \\ &\rightarrow \text{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x) \rightarrow 0. \end{aligned}$$

Let $1 \neq \sigma \in \mathfrak{S}_p$ such that $(\Delta_k \sigma)^x \in (\Delta_k \mathfrak{S}_p)^x \cap P$. Then $(\Delta_k \sigma)^x$ acts trivially on $\text{Lie}(k)$, and $\Omega(F)$ is indecomposable as a module for $\langle \Delta_k \sigma \rangle$ (as $\Delta_k \sigma$ has order p) and has dimension $(p - 1)$. It follows that $\text{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \text{Lie}(k)) \otimes x)$ has no projective summand. Thus, from $(*)$, we see that

$$\Omega(\text{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x)) \cong \text{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \text{Lie}(k)) \otimes x)$$

since $\text{Ind}_{D^x \cap P}^P(P(\Lambda_k) \otimes x)$ remains projective. Hence

$$(\text{Res}_P \text{Lie}(n))_{pf} \cong \bigoplus_{x \in S} \text{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \text{Lie}(k)) \otimes x)$$

and the theorem follows. \square

Corollary 3.5. *We have*

$$\dim((\text{Res}_P^{\mathfrak{S}_{kp}} \text{Lie}(kp))_{pf}) = (p - 1)(k - 1)!N,$$

where N is the number of cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.

Proof. Using Theorem 3.4 we must show that $N = N'$ where $N' = \sum_{y \in S} [P : D^y \cap P]$. The index $[P : D^y \cap P]$ is equal to the size of the P -orbit of Dy in the coset space $(\mathfrak{S}_n : D)$, so it is equal to the number of cosets Dx contained in DyP .

Write $D_1 = \Delta_k \mathfrak{S}_p$. If a coset Dx is contained in DyP then $D_1^x \cap P$ is P -conjugate to $D_1^y \cap P$ and hence $D_1^y \cap P \neq 1$ if and only if $D_1^x \cap P \neq 1$. Conversely if Dx is a coset and $D_1^x \cap P \neq 1$ then Dx is contained in one of

the double cosets counted for N' . We sum over all such double cosets, and hence N is equal to the N' . \square

Corollary 3.5 suggests that we should proceed by parametrising the right cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.

4. SYLOW p -SUBGROUPS OF SYMMETRIC GROUPS

The Sylow p -subgroups of \mathfrak{S}_n are direct products of iterated wreath products of cyclic groups of order p . We begin this section with the analysis of these building blocks.

From now on, we denote the distinguished p -cycle $(1, 2, \dots, p)$ of \mathfrak{S}_p by π .

Definition 4.1.

- (1) For each $i \in \mathbb{Z}_{\geq 0}$, let R_i be the subgroup of $\mathfrak{S}_{p^{i+1}}$ generated by $\{\pi^{[p^j]} \mid j \in [0, i]\}$. For convenience, let $R_{-1} = 1$.
- (2) For each $i \in \mathbb{Z}_{\geq 0}$, let $B_i = R_{i-1}[1] \times R_{i-1}[2] \times \cdots \times R_{i-1}[p]$. For convenience, let $B_{-1} = \emptyset$.
- (3) And for each $s \in \mathbb{Z}^+$, let $H_s = \prod_{a=1}^s \langle \pi[a] \rangle$.

Note. For each $i \in \mathbb{Z}_{\geq 0}$ we have $R_i = B_i \times \langle \pi^{[p^i]} \rangle$, and, as a group, R_i is isomorphic to $\underbrace{C_p \wr C_p \wr \cdots \wr C_p}_{(i+1) \text{ times}}$. Also, H_{p^i} is a subgroup of B_i , and it is normal in R_i .

As a next step, we present a ‘canonical form’ for elements in R_i . Let $g \in \mathfrak{S}_n$. We say that a subinterval $(a, b]$ of $(0, n]$ is g -irreducible if and only if g stabilises $(a, b]$ but does not stabilize $(a, a']$ for any $a' with $a < a' < b$. In other words, $(a, b]$ is g -irreducible if and only if g stabilises $(a, b]$, and $(a, b]$ as an ordered set does not have any g -invariant order ideals. Clearly, the set $(0, n]$ is a disjoint union $\cup_{j=1}^s (a_{j-1}, a_j]$ of g -irreducible subintervals, and $g = \prod_{j=1}^s g_j$ where g_j is supported on $(a_{j-1}, a_j]$.$

Below we will describe this factorisation explicitly for elements of R_i . At the same time, we wish to keep track over the supports of the factors; and to label these and we will use the intervals. An example may be found below.

Proposition 4.2. *Suppose that $g \in R_i$, and let $0 = a_0 < a_1 < \cdots < a_s = p^{i+1}$ be such that $(a_{j-1}, a_j]$ is a g -irreducible subinterval for each j ($1 \leq j \leq s$). Then*

- (1) $a_j - a_{j-1}$ is a power of p , dividing a_j , for all $1 \leq j \leq s$;
- (2) $g = \prod_{j=1}^s \gamma_j [a_j / (a_j - a_{j-1})]$ with $\gamma_j \in R_{m_j-1} \setminus B_{m_j-1}$, where $p^{m_j} = a_j - a_{j-1}$, for all $1 \leq j \leq s$.

Proof. We prove both statements by induction on i . When $i = 0$, then either $g = 1$, in which case $s = p$ and $a_j = j$ for all $0 \leq j \leq s$, or else $g = \pi^t$ for some $t \in \mathbb{Z}_p^*$, in which case $s = 1$ and so $a_1 = p$. It can easily

be checked that both statements hold in either case. Assume thus $i > 0$. The statements are trivial when $s = 1$. When $s > 1$, then $g \in B_i$, as otherwise $g \in B_i(\pi^{[p^i]})^t$ for some $t \in \mathbb{Z}_p^*$, and then g would not stabilise $(0, a_1]$. Thus, $g = \prod_{j=1}^p g_j[j]$ for some $g_1, g_2, \dots, g_p \in R_{i-1}$. Hence there exist $0 = j_0 < j_1 < \dots < j_p = s$ such that $a_{j_r} = rp^i$ for all $r \in [1, p]$. For each $r \in [1, p]$ and $u \in [0, j_r - j_{r-1}]$, let $b_{r,u} = a_{j_{r-1}+u} - a_{j_{r-1}} = a_{j_{r-1}+u} - (r-1)p^i$. Then $0 = b_{r,0} < b_{r,1} < \dots < b_{r,j_r-j_{r-1}} = a_{j_r} - a_{j_{r-1}} = p^i$, and $(b_{r,u-1}, b_{r,u}]$ is stabilised by g_r while $(b_{r,u-1}, b']$ is not stabilised by g_r for all b' with $b_{r,u-1} < b' < b_{r,u}$. By induction, we conclude that $b_{r,u} - b_{r,u-1}$ is a power of p , say $b_{r,u} - b_{r,u-1} = p^{m_{r,u}}$, and $p^{m_{r,u}}$ divides $b_{r,u}$. Furthermore, $g_r = \prod_{u=1}^{j_r-j_{r-1}} \gamma_{r,u}[b_{r,u}/(b_{r,u}-b_{r,u-1})]$ with $\gamma_{r,u} \in R_{m_{r,u-1}} \setminus B_{m_{r,u-1}}$ for all $u \in [1, j_r - j_{r-1}]$. Since $b_{r,u} \leq p^i$, we see that $b_{r,u} - b_{r,u-1}$ divides $b_{r,u} + (r-1)p^i$. But $b_{r,u} - b_{r,u-1} = a_{j_{r-1}+u} - a_{j_{r-1}+u-1}$ and $b_{r,u} + (r-1)p^i = a_{j_{r-1}+u}$, and hence we proved (1). Part (2) also follows when we define γ_j as $\gamma_{r,j-j_{r-1}}$ if $j \in (j_{r-1}, j_r]$. \square

Example 4.3. Let $p = 3$, and let $g \in B_2 \subseteq R_2 = \langle \pi, \pi^{[p]}, \pi^{[p^2]} \rangle$, with

$$g = \prod_{i=1}^3 g_i[i]$$

where $g_1 = \pi^{[p]}$, g_2 is the product of three disjoint non-trivial powers of π , appropriately shifted, i.e. $g_2 = \pi^{t_1}[1]\pi^{t_2}[2]\pi^{t_3}[3]$ with $t_i \in \mathbb{Z}_p^*$ for all i , and $g_3 = (\pi^{[p]})^2$. Then

$$a_0 = 0, \quad a_1 = p^2, \quad a_2 = p^2 + p, \quad a_3 = p^2 + 2p, \quad a_4 = 2p^2, \quad a_5 = p^3.$$

The normal form for g is then

$$g = \pi^{[p]}[1] \cdot \pi^{t_1}[p+1] \cdot \pi^{t_2}[p+2] \cdot \pi^{t_3}[2p] \cdot (\pi^{[p]})^2[p].$$

We are mainly interested in the elements of R_i having order p . For such elements, the γ_j 's appearing in Proposition 4.2 are conjugate to shifts of powers of the generators of R_i . This is in fact true in a more general setting, which we present below.

Proposition 4.4. *Let G be a group of the form $G = R \langle y \rangle$ where y has order p , with base group B . Let $t \in \mathbb{Z}_p^*$. Then the conjugacy class of y^t contains precisely the elements of G having order p and lying in the coset By^t .*

Thus, the elements of $G \setminus B$ having order p are just the various conjugates of y^t for $t \in \mathbb{Z}_p^*$.

Proof. It suffices to prove the proposition for $t = 1$ since y^t also generates the group $\langle y \rangle$. Let C be the conjugacy class of y , and let $\Gamma = \{g \in By \mid g \text{ has order } p\}$. It is easy to see that $C \subseteq \Gamma$. For the converse, we show that every element of Γ is conjugate to y by a unique element of B' , where B' is the direct product of $p-1$ copies of R , say $B' = R \times \dots \times R \times 1 \subseteq B$. Let $g = by \in \Gamma$, where $b \in B$. Then $g^p = b(yb)(y^2b) \dots (y^{p-1}b)$ (where $xb = xbx^{-1}$). If $b = (r_1, \dots, r_p)$ then the coordinates of g^p are the cyclic

permutations of $r_1 r_2 \dots r_p$. Hence $g^p = 1$ if and only if $r_p = (r_1 r_2 \dots r_{p-1})^{-1}$. This shows that given $r_1, \dots, r_{p-1} \in R$ there is a unique such g of order p . Hence $|\Gamma| \leq |R|^{p-1}$. The set $A := \{(b')^{-1} y b' : b' \in B'\}$ is contained in Γ , and has size $|B'| = |R|^{p-1}$ since the centraliser of y in B' is trivial. It follows that $A = \Gamma$, and $g = (b')^{-1} y b'$ for a unique $b' \in B'$, and the proof is complete. \square

Corollary 4.5 (of proof). *Keep the notations in Proposition 4.4 and its proof. Every element of $G \setminus B$ having order p can be uniquely expressed as $(y^t)^b$ with $b \in B'$ and $t \in \mathbb{Z}_p^*$.*

Take $g \in R_i$ in the normal form as given in Proposition 4.2. We have seen that each irreducible subset of the support of g has size some p -power. We want to keep track of these sizes. In Example 4.3, the sizes are

$$(p^2, p, p, p, p^2).$$

It suffices to label these by the exponents of p , as

$$(2, 1, 1, 1, 2).$$

This suggests the following definition.

Definition 4.6. A p -composition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ is a finite sequence of non-negative integers such that for each $j \in [1, s]$, the partial sum $\sum_{i=1}^j p^{\lambda_i}$ is divisible by p^{λ_j} .

Let $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ be a p -composition. For each $j \in [1, s]$, we will denote these partial sums in the following by

$$\Sigma_j^\lambda := \sum_{i=1}^j p^{\lambda_i}.$$

If $\sum_{i=1}^s p^{\lambda_i} = r$, we say that λ is a p -composition of r .

Example.

- (1) The only p -composition of $p^0 (= 1)$ is $\lambda = (0)$. More generally, when $r < p$, the only p -composition of p^r is $\lambda = (0^r)$, the composition with r parts, each equal to 0.
- (2) There are exactly two p -compositions of $p^1 (= p)$, namely (0^p) , the composition with p parts, each equal to 0, and the composition (1).
- (3) Examples of p -compositions of p^2 are (2) and $\lambda = (1^p)$. There are many more; by Lemma 4.9 (see below) we may substitute for each 1 in λ the p -composition (0^p) , and this gives us refinements of λ .
- (4) More generally, (m) and $\lambda = ((m-1)^p)$ are examples of p -compositions of p^m , and replacing any of the entries $m-1$ in λ by p -compositions of p^{m-1} produces a p -composition of p^m . We will see in Proposition 4.12 that every other p -composition of p^m is obtained in this way.
- (5) If $(\lambda_1, \lambda_2, \dots, \lambda_s)$ is a p -composition of r , and $\lambda_i > 0$ for all i , then $(\lambda_1 - 1, \lambda_2 - 1, \dots, \lambda_s - 1)$ is a p -composition of r/p .
- (6) If λ is a partition (that is, a finite decreasing sequence of non-negative integers), then λ is a p -composition.

Lemma 4.7. *Let $g \in R_i$, and let $0 = a_0 < a_1 < \cdots < a_s = p^{i+1}$ be such that each $(a_{j-1}, a_j]$ is g -irreducible. For each $1 \leq j \leq s$, let $a_j - a_{j-1} = p^{\lambda_j}$. Then $(\lambda_1, \lambda_2, \dots, \lambda_s)$ is a p -composition of p^{i+1} .*

Furthermore, $\lambda_i > 0$ for all $1 \leq i \leq s$ if and only if g is fixed-point-free. If so then $(\lambda_1 - 1, \lambda_2 - 1, \dots, \lambda_s - 1)$ is a p -composition of p^i .

Proof. The first assertion is a reformulation of Proposition 4.2(1). Furthermore, Proposition 4.2(2) shows that the fixed points of g are precisely those a_i such that $a_i - a_{i-1} = 1$, so that (2) follows. \square

Definition 4.8. Let $\lambda = (\lambda_1, \dots, \lambda_s)$ be a p -composition. A *refinement* of λ is a finite sequence $\mu = (\mu_1, \dots, \mu_r)$ of non-negative integers where there exist $0 = i_0 < i_1 < i_2 < \cdots < i_s = r$ such that for each $j \in [1, s]$, $(\mu_{i_{j-1}+1}, \mu_{i_{j-1}+2}, \dots, \mu_{i_j})$ is a p -composition of p^{λ_j} .

Lemma 4.9. *A refinement of a p -composition is a p -composition.*

Proof. Let $\mu = (\mu_1, \dots, \mu_r)$ be a refinement of a p -composition $\lambda = (\lambda_1, \dots, \lambda_s)$. Thus, there exist $0 = i_0 < i_1 < i_2 < \cdots < i_s = r$ such that for each $j \in [1, s]$, $(\mu_{i_{j-1}+1}, \mu_{i_{j-1}+2}, \dots, \mu_{i_j})$ is a p -composition of p^{λ_j} . Let $u \in [1, r]$, and let v be such that $u \in (i_{v-1}, i_v]$. Then $\sum_{i=1}^u p^{\mu_i} = \sum_{i=1}^{v-1} p^{\lambda_i} + \sum_{i=i_{v-1}+1}^u p^{\mu_i}$. Since $(\mu_{i_{v-1}+1}, \dots, \mu_{i_v})$ is a p -composition of p^{λ_v} , we see that p^{μ_u} divides $\sum_{i=i_{v-1}+1}^u p^{\mu_i}$. Furthermore, as p^{λ_v} divides $\sum_{i=1}^v p^{\lambda_i}$, and hence $\sum_{i=1}^{v-1} p^{\lambda_i}$, so does p^{μ_u} (as $p^{\mu_u} \leq \sum_{i=i_{v-1}+1}^{i_v} p^{\mu_i} = p^{\lambda_v}$). Thus p^{μ_u} divides $\sum_{i=1}^u p^{\mu_i}$, and we are done. \square

Definition 4.10. Let $r \in \mathbb{Z}^+$, and let $r = \sum_{i=0}^t a_i p^{t-i}$ be its p -adic expansion (where t is the largest positive integer satisfying $p^t \leq r$). The p -composition $(t^{a_0}, (t-1)^{a_1}, \dots, (0)^{a_t})$ with a_0 parts equal to t , a_1 parts equal to $t-1$, and so on, is called the *p -adic p -composition of r* .

Proposition 4.11. *Let $r \in \mathbb{Z}^+$. Every p -composition of r is a refinement of the p -adic p -composition of r .*

Proof. Let $\lambda = (\lambda_1, \dots, \lambda_s)$ be a p -composition of r . The statement is clear for $s = 1$, and by induction, $(\lambda_1, \dots, \lambda_{s-1})$ is a refinement of the p -adic p -composition of Σ_{s-1}^λ . Observe that $p^{\lambda_s} \mid \Sigma_s^\lambda = r$. Let $\sum_{i=0}^t a_i p^{t-i}$ be the p -adic expansion of r (with $a_0 \neq 0$), and let u be the largest integer such that $a_u \neq 0$ (equivalently, u is least integer such that p^{t-u} divides r). Then $u \leq t - \lambda_s$, and hence,

$$\begin{aligned} \Sigma_{s-1}^\lambda &= r - p^{\lambda_s} \\ &= \sum_{i=0}^u a_i p^{t-i} - p^{\lambda_s} \\ &= \sum_{i=0}^{u-1} a_i p^{t-i} + (a_u - 1)(p^{t-u}) + \sum_{i=u+1}^{t-\lambda_s} (p-1)p^{t-i} \end{aligned}$$

is the p -adic decomposition of Σ_{s-1}^λ . Thus, there exists $v \in [1, s)$ such that $(\lambda_1, \dots, \lambda_v)$ is the concatenation of a_0 p -compositions of p^t, \dots, a_{u-1} p -compositions of $p^{t-u+1}, (a_u - 1)$ p -compositions of p^{t-u} , while $(\lambda_{v+1}, \dots, \lambda_s)$ is a p -composition of p^{t-u} , and we are done. \square

Proposition 4.12. *Let $m \in \mathbb{Z}^+$, and let $\lambda = (\lambda_1, \dots, \lambda_s)$ be a p -composition of p^m . If $s > 1$, then λ is a refinement of $((m-1)^p)$.*

Proof. We prove that for $u \in [0, p]$, there exists $i_u \in [0, s]$ such that $\Sigma_{i_u}^\lambda = up^{m-1}$. This is clear for $u = 0$, where $i_u = 0$, and $u = p$, where $i_u = s$. For $u \in (0, p)$, we may assume that we have already found $i_{u-1} \in [0, s]$ such that $\Sigma_{i_{u-1}}^\lambda = (u-1)p^{m-1}$. Let t be the largest index such that $\Sigma_t^\lambda \leq up^{m-1}$. We claim that $\Sigma_t^\lambda = up^{m-1}$ (then we take $i_u = t$). Suppose the contrary that $\Sigma_t^\lambda < up^{m-1}$. Since λ is a p -composition, we have $p^{\lambda_{t+1}}$ dividing $\Sigma_{t+1}^\lambda = \Sigma_t^\lambda + p^{\lambda_{t+1}}$, so that $p^{\lambda_{t+1}}$ divides Σ_t^λ . Since $s > 1$, we have $\lambda_i \leq m-1$ for all $i \in [1, s]$; in particular, $\lambda_{t+1} \leq m-1$, so that $p^{\lambda_{t+1}} \mid (u-1)p^{m-1} = \Sigma_{i_{u-1}}^\lambda$. Therefore $p^{\lambda_{t+1}}$ divides $\Sigma_t^\lambda - \Sigma_{i_{u-1}}^\lambda$, say $\Sigma_t^\lambda - \Sigma_{i_{u-1}}^\lambda = cp^{\lambda_{t+1}}$ with $c \in \mathbb{Z}$. Since $\Sigma_t^\lambda - \Sigma_{i_{u-1}}^\lambda < p^{m-1}$, we have $c < p^{m-1-\lambda_{t+1}}$, so that $c+1 \leq p^{m-1-\lambda_{t+1}}$. Thus $\Sigma_{t+1}^\lambda = (\Sigma_t^\lambda - \Sigma_{i_{u-1}}^\lambda) + \Sigma_{i_{u-1}}^\lambda + p^{\lambda_{t+1}} = (c+1)p^{\lambda_{t+1}} + (u-1)p^{m-1} \leq up^{m-1}$, contradicting the maximality of t . \square

Recall that R_i is an explicit Sylow p -subgroup of $\mathfrak{S}_{p^{i+1}}$, with support $[1, p^{i+1}]$. We will now fix an explicit Sylow p -subgroup of \mathfrak{S}_{pk} . Suppose k has p -adic expansion

$$k = a_0p^t + a_1p^{t-1} + \dots + a_{t-1}p + a_t$$

with $a_i \in [0, p)$, and where $a_0 \neq 0$. Then a Sylow p -subgroup of \mathfrak{S}_{pk} is isomorphic to the direct products of a_i copies of R_i for $i \in [0, t]$, with disjoint supports. We choose our Sylow p -subgroup P of \mathfrak{S}_{pk} by taking first a_0 copies of R_t , then a_1 copies of R_{t-1} (if $a_1 \neq 0$), and so on.

We illustrate this by an example.

Example. Let $n = pk = p^4 + 2p^3 + p$ with $p \geq 3$. We take P with orbits

$$[1, p^4], \quad (p^4, p^4 + p^3], \quad (p^4 + p^3, p^4 + 2p^3], \quad (p^4 + 2p^3, p^4 + 2p^3 + p].$$

The first factor of P is R_3 . The second factor is a shifted copy of R_2 , acting on the next possible block of size p^3 . The support of the first factor R_3 is a p -block of that size, i.e. $[1, p^4]$; therefore the second factor must be $R_2[p+1]$, with support $(p^4, p^4 + p^3]$. Repeating this argument we get

$$P = R_3[1] \times R_2[p+1] \times R_2[p+2] \times R_1[p^3 + 2p^2 + 1].$$

Notice that the numbers $p^4, p^4 + p^3, p^4 + 2p^3, p^4 + 2p^3 + p$ are precisely the partial sums $p\Sigma_i^\kappa$ of the p -adic p -composition $\kappa = (3, 2, 2, 0)$ of k .

The support of the second factor is shifted by $\Sigma_2^\kappa/p^{\kappa_2}$, and the support of the third factor is shifted by $\Sigma_3^\kappa/p^{\kappa_3}$ (note that $\kappa_2 = \kappa_3 = 2$). Finally the support of the fourth factor is shifted by $\Sigma_4^\kappa/p^{\kappa_4} = \Sigma_4^\kappa = k$.

The following gives the precise description of this choice in general.

Definition 4.13. Denote by $\kappa = (\kappa_1, \kappa_2, \dots, \kappa_l)$ the p -adic p -composition of k , and let P be the Sylow p -subgroup of \mathfrak{S}_{pk} chosen as follows:

$$P = P_1 \times P_2 \times \dots \times P_l,$$

where $P_i = R_{\kappa_i}[\Sigma_i^\kappa/p^{\kappa_i}]$ for all i . That is, the i -th factor P_i is a shifted copy of R_{κ_i} , with support being the interval $(p^{\Sigma_{i-1}^\kappa}, p^{\Sigma_i^\kappa}]$.

Note. By our choice of P , the group $R_i[j]$ is contained in P if and only if $1 \leq j \leq k/p^i$.

Notation 4.14. In what follows, we will frequently have expressions of the form $\prod_{i=1}^l x_i[\Sigma_i^\kappa/p^{\kappa_i}]$ and $\prod_{i=1}^l A_i[\Sigma_i^\kappa/p^{\kappa_i}]$ where for each $i \in [1, l]$, x_i and A_i are respectively an element and a subset of $\mathfrak{S}_{p^{\kappa_i+1}}$. Most of the time, the details of the shifts do not play a role. We will therefore use the shorthand notations

$$\prod_{\kappa} x_i \quad \text{and} \quad \prod_{\kappa} A_i$$

to denote these expressions.

Similarly if $\lambda = (\lambda_1, \dots, \lambda_s)$ is a p -composition then we write

$$\prod_{\lambda} x_i = \prod_{i=1}^s x_i[\Sigma_i^\lambda/p^{\lambda_i}]$$

(where $x_i \in \mathfrak{S}_{p^{\lambda_i+1}}$).

5. FINDING RIGHT COSET REPRESENTATIVES

We will now analyse the right cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, and where from now, P will always denote the Sylow p -subgroup of \mathfrak{S}_{pk} as in Definition 4.13. Our aim in this section is to find a good subset $X_k \subseteq \mathfrak{S}_{pk}$ such that

- $(\Delta_k \mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$;
- if $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, then there exists $y \in X_k$ such that $Dx = Dy$.

When $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, this is a non-trivial p -group conjugate to a subgroup of $\Delta_k \mathfrak{S}_p$, and hence it is generated by a fixed-point-free element y of \mathfrak{S}_{pk} of order p . Clearly we can replace x by elements of the form dx for $d \in D$ without altering the right coset Dx . Taking d suitably in $\Delta_k \mathfrak{S}_p \subseteq D$ will allow us to have $y = (\Delta_k \pi)^x$ in P . Such x takes orbits of $\Delta_k \pi$ to orbits of y , and the order in which these orbits appear can be controlled by modifying with $d \in \mathfrak{S}_k^{[p]}$. The following makes this precise.

Proposition 5.1. *Let κ and P be as in Definition 4.13. Let $x \in \mathfrak{S}_{pk}$ such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. Then for each $r \in [1, l]$ there exists $x_r \in \mathfrak{S}_{p^{\kappa_r+1}}$ such that*

- $\prod_{\kappa} x_j \in Dx$;
- $(\Delta_{p^{\kappa_r}} \pi)^{x_r} \in R_{\kappa_r}$.

Proof. Let $1 \neq y \in (\Delta_k \mathfrak{S}_p)^x \cap P$, say $y = (\Delta_k g)^x$ for some p -cycle $g \in \mathfrak{S}_p$. Then $g = \pi^\tau$ for some $\tau \in \mathfrak{S}_p$; and by replacing x with $(\Delta_k \tau)x \in Dx$ we may assume $g = \pi$.

Since $y \in P = P_1 \times \cdots \times P_l$, we have $y = \prod_{r=1}^l y_r$ where for each r , $y_r \in P_r = R_{\kappa_r}[\Sigma_r^\kappa/p^{\kappa_r}]$. As $\prod_{r=1}^l y_r = (\Delta_k \pi)^x = \prod_{i=1}^k (\pi[i])^x$, there exists $\sigma \in \mathfrak{S}_k$ permuting the cycles of $\Delta_k \pi$ such that, for each $r \in [1, l]$, we have $\prod_{i=\Sigma_{r-1}^\kappa+1}^{\Sigma_r^\kappa} \pi[i\sigma]^x = y_r$. Recall that $\prod_{i=1}^k \pi[i\sigma] = (\Delta_k \pi)^{\sigma^{[p]}}$, so by replacing x with $\sigma^{[p]}x \in Dx$, we may assume that

$$((\Delta_{p^{\kappa_r}} \pi)[\Sigma_r^\kappa/p^{\kappa_r}])^x = y_r \in P_r = R_{\kappa_r}[\Sigma_r^\kappa/p^{\kappa_r}]$$

for all $r \in [1, l]$. Thus x preserves the orbits of P and we can write $x = \prod_{r=1}^l z_r$, where $z_r \in \mathfrak{S}_{p^{\kappa_r+1}}[\Sigma_r^\kappa/p^{\kappa_r}]$ for all r , and $y_r = ((\Delta_{p^{\kappa_r}} \pi)[\Sigma_r^\kappa/p^{\kappa_r}])^{z_r}$. The proposition follows by defining x_r to be the element of $\mathfrak{S}_{p^{\kappa_r+1}}$ such that $x_r[\Sigma_r^\kappa/p^{\kappa_r}] = z_r$. \square

This shows in particular that we can take x so that it respects the direct factors of P . We have the following refinement, which concentrates on a fixed factor of P . The proof is analogous to that of Proposition 5.1.

Proposition 5.2. *Suppose that $(\Delta_{p^m} \pi)^x \in R_m$ for some $x \in \mathfrak{S}_{p^{m+1}}$. Then there exist a p -composition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ of p^m , and elements $x_r \in \mathfrak{S}_{p^{\lambda_r+1}}$ for all $r \in [1, s]$ such that*

- $\prod_\lambda x_r \in \mathfrak{S}_{p^m}^{[p]} x$;
- $(\Delta_{p^{\lambda_r}} \pi)^{x_r} \in R_{\lambda_r} \setminus B_{\lambda_r}$.

Proof. By Proposition 4.2 and Lemma 4.7, there exist a p -composition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ of p^m , and elements $\gamma_r \in R_{\lambda_r} \setminus B_{\lambda_r}$ for $r \in [1, s]$, such that $(\Delta_{p^m} \pi)^x = \prod_\lambda \gamma_r$. Thus there is some $\sigma \in \mathfrak{S}_{p^m}$ such that $(\prod_{i=\Sigma_{r-1}^\lambda+1}^{\Sigma_r^\lambda} \pi[i\sigma])^x = \gamma_r[\Sigma_r^\lambda/p^{\lambda_r}]$ for all $r \in [1, s]$. By replacing x by $\sigma^{[p]}x \in \mathfrak{S}_{p^m}^{[p]} x$, we may assume that

$$((\Delta_{p^{\lambda_r}} \pi)[\Sigma_r^\lambda/p^{\lambda_r}])^x = \gamma_r[\Sigma_r^\lambda/p^{\lambda_r}]$$

for all r . Thus $x = \prod_{r=1}^s z_r$, where $z_r \in \mathfrak{S}_{p^{\lambda_r+1}}[\Sigma_r^\lambda/p^{\lambda_r}]$, and

$$\gamma_r[\Sigma_r^\lambda/p^{\lambda_r}] = ((\Delta_{p^{\lambda_r}} \pi)[\Sigma_r^\lambda/p^{\lambda_r}])^{z_r}.$$

The Proposition follows by defining x_r to be the element of $\mathfrak{S}_{p^{\lambda_r+1}}$ such that $x_r[\Sigma_r^\lambda/p^{\lambda_r}] = z_r$. \square

We now find good coset representatives for these x_r , and we start by defining distinguished elements which will conjugate $\Delta_{p^m} \pi$ to $(\pi^{[p^m]})^t$.

Definition 5.3. For $t \in \mathbb{Z}_p^*$ and $m \in \mathbb{Z}_{\geq 0}$, define $z_{m,t} \in \mathfrak{S}_{p^{m+1}}$ by

$$((i-1)p+j)z_{m,t} := i + \overline{(t(j-1))}p^m \quad (i \leq p^m, j \leq p).$$

Here, and hereafter, given an integer x , we write \bar{x} for the residue of x (mod p) with $0 \leq \bar{x} < p$.

For example, if $m = 0$ then $z_{0,t}$ normalizes the group $\langle \pi \rangle$ (see Lemma 5.4 below), and $z_{0,1} = 1$.

Note. It will be convenient to describe $z_{m,t}$ by making use of the natural faithful action of \mathfrak{S}_n on standard tableaux. We take tableaux with p^m rows and each row of length p , i.e. of shape (p^{p^m}) . Then $z_{m,1}$ is the element of $\mathfrak{S}_{p^{m+1}}$ which sends the tableau

$$\begin{array}{cccc} 1 & 2 & \cdots & p \\ p+1 & p+2 & \cdots & 2p \\ \vdots & \vdots & & \vdots \\ p^m-p+1 & p^m-p+2 & \cdots & p^m+1 \end{array} \quad \text{to} \quad \begin{array}{cccc} 1 & p^m+1 & \cdots & (p-1)p^m+1 \\ 2 & p^m+2 & \cdots & (p-1)p^m+2 \\ \vdots & \vdots & & \vdots \\ p^m & 2p^m & \cdots & p^{m+1} \end{array}.$$

We denote the first tableau by T , and the second one by \tilde{T} , and we will use these notations later.

In general, $z_{m,t}$ sends T to the tableau

$$\begin{array}{cccc} 1 & \bar{t}p^m+1 & \cdots & \overline{(t(p-1))p^m+1} \\ 2 & \bar{t}p^m+2 & \cdots & \overline{(t(p-1))p^m+2} \\ \vdots & \vdots & & \vdots \\ p^m & (\bar{t}+1)p^m & \cdots & \overline{(t(p-1)+1)p^m} \end{array}$$

which is obtained from \tilde{T} by permuting the columns according to $z_{0,t}$.

Lemma 5.4. *Let $z_{m,t}$ be as above.*

- (1) *We have $\pi[i]^{z_{m,t}} = (i, p^m+i, \dots, (p-1)p^m+i)^t$ for $i \in [1, p^m]$. Thus, $(\Delta_{p^m}\pi)^{z_{m,t}} = (\pi^{[p^m]})^t$.*
- (2) *For $s, t \in \mathbb{Z}_p^*$ we have $(\Delta_{p^m}z_{0,t}) \cdot z_{m,s} = z_{m,ts}$.*

Proof. For the first part, consider the tableaux T and $Tz_{m,t}$ above. The rows of T are the cycles of $\Delta_{p^m}\pi$, and the rows of $Tz_{m,t}$ are the cycles of $(\pi^{[p^m]})^t$. The standard formula for conjugation gives the statement. The second part follows from a direct verification using the definition of $z_{m,t}$. \square

We still concentrate on a factor R_m of P . When $\Delta_{p^m}\pi$ is conjugated, we need to take care of its centraliser in $\mathfrak{S}_{p^{m+1}}$. This is the group $H_{p^m} \rtimes \mathfrak{S}_{p^m}^{[p]}$ (and this explains why in the following the group $\mathfrak{S}_{p^m}^{[p]}$ appears). In particular we should expect factors from H_{p^m} occurring as well.

We denote by R_m^0 the subgroup of B_m consisting of elements which fix the last block of p^m elements pointwise, i.e.

$$R_m^0 = \prod_{i=1}^{p-1} R_{m-1}[i]$$

Proposition 5.5. *Suppose that $(\Delta_{p^m}\pi)^x \in R_m \setminus B_m$ for some $x \in \mathfrak{S}_{p^{m+1}}$. Then there exist unique $t \in \mathbb{Z}_p^*$, $h \in H_{p^m}$ and $b \in R_m^0$ such that*

$$hz_{m,t}b \in \mathfrak{S}_{p^m}^{[p]} x.$$

Proof. Since $(\Delta_{p^m}\pi)^x$ lies in $R_m \setminus B_m$ and has order p , we apply Corollary 4.5. Hence there exist unique $t \in \mathbb{Z}_p^*$ and $b \in R_m^0$ such that $(\Delta_{p^m}\pi)^x = ((\pi^{[p^m]})^t)^b$.

Thus

$$(\Delta_{p^m}\pi)^x = ((\pi^{[p^m]})^t)^b = (\Delta_{p^m}\pi)^{z_{m,t}b},$$

and so $z_{m,t}bx^{-1}$ lies in the centraliser of $\Delta_{p^m}\pi$ in $\mathfrak{S}_{p^{m+1}}$, which is $H_{p^m} \times \mathfrak{S}_{p^m}^{[p]}$. Hence, there exists a unique $h \in H_{p^m}$ such that $hz_{m,t}b \in \mathfrak{S}_{p^m}^{[p]}x$. \square

Propositions 5.1, 5.2 and 5.5 suggests the following definition for the desired coset representatives.

Definition 5.6. Let $d \in \mathbb{Z}^+$. For a p -composition $\lambda = (\lambda_1, \dots, \lambda_s)$ of d , define

$$X_\lambda := \{h \prod_{\lambda} (z_{\lambda_r, t_r} b_r) \mid h \in H_d, t_r \in \mathbb{Z}_p^*, b_r \in R_{\lambda_r}^0 \text{ for all } r \in [1, s]\}$$

and then set

$$X_d := \bigcup_{\lambda} X_\lambda.$$

For $m \in \mathbb{Z}_{\geq 0}$, we define the subset Y_m of $\mathfrak{S}_{p^{m+1}}$ by

$$Y_m = \{hz_{m,t}b \mid h \in H_{p^m}, t \in \mathbb{Z}_p^*, b \in R_m^0\}.$$

For example $Y_0 = \{hz_{0,t} : h \in \langle \pi \rangle, t \in \mathbb{Z}_p^*\}$ which is the normaliser of $\langle \pi \rangle$ in \mathfrak{S}_p . We have also a recursive description:

Lemma 5.7.

(1) Let $m \in \mathbb{Z}_{\geq 0}$. Then

$$X_{p^m} = Y_m \cup \prod_{i=1}^p X_{p^{m-1}}[i]$$

(disjoint union, and where $X_{p^{-1}} = \emptyset$).

(2) Let $k \in \mathbb{Z}^+$, with p -adic p -composition $\kappa = (\kappa_1, \dots, \kappa_l)$. Then

$$X_k = \prod_{\kappa} X_{p^{\kappa_i}}.$$

Proof. These follow from Propositions 4.12 and 4.11, and Lemma 4.9. \square

We can now state the main theorem of this section.

Theorem 5.8. Let P be as in Definition 4.13. Let $x \in \mathfrak{S}_{pk}$ such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. Then there exist $x_0 \in X_k$ such that $x_0 \in Dx$.

Proof. This follows from Propositions 5.1, 5.2 and 5.5, and Lemma 5.7(2). \square

We note that the converse of Theorem 5.8 also holds.

Lemma 5.9. We have $(\Delta_k \mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$.

Proof. By the definition of the z_{λ_r, t_r} , the conjugate $(\Delta_k \pi)^y$ belongs to P . \square

6. UNIQUENESS

We have seen in the previous section that $(\Delta_k \mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$, and if $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, then there exists $x_0 \in X_k$ such that $Dx_0 = Dx$. However, x_0 need not be unique. For example, instead of x_0 , one may choose $(\Delta_k \pi)x_0$ which also lies in X_k .

In this section, we will construct a subset of X_k which contains a unique element from each right coset Dx satisfying $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.

We begin with the observation that such a subset can be chosen to be contained in X_{k-1} .

Proposition 6.1. *Let $k \in \mathbb{Z}^+$ with $p \nmid k$. Then $X_{k-1} \subseteq X_k$. Furthermore, if $x \in X_k$, then there exists $y \in X_{k-1}$ such that $Dx = Dy$.*

Proof. Let $\kappa = (\kappa_1, \kappa_2, \dots, \kappa_l)$ be the p -adic p -composition of k . Since $p \nmid k$, we see that $\kappa_l = 0$, and $(\kappa_1, \dots, \kappa_{l-1})$ is the p -adic p -composition of $(k-1)$. Thus, $X_k = X_{k-1} \times X_1[k]$ by Lemma 5.7(2).

The first assertion now follows as $1 (= z_{0,1})$ belongs to X_1 .

For the second part, we have $x = a \cdot x'[k]$ where $a \in X_{k-1}$ and $x' = hz_{0,t}$ with $h \in H_1$ and $t \in \mathbb{Z}_p^*$. Let u be the inverse of t in \mathbb{Z}_p^* . Then $z_{0,u}$ is the inverse of $z_{0,t}$ by Lemma 5.4(2). Define $y := \Delta_{k-1}(z_{0,u}h^{-1})a$. Then $y \in Dx$ since $\Delta_k(z_{0,u}h^{-1}) \in D$ and

$$\Delta_k(z_{0,u}h^{-1})x = \Delta_{k-1}(z_{0,u}h^{-1})a \cdot (z_{0,u}h^{-1}x')[k] = y.$$

Furthermore, $y \in X_{k-1}$; to see this, note that $\Delta_{k-1}z_{0,u}$ normalises H_{k-1} and use Lemma 5.4(2). \square

Before we continue, we make the following observation:

Lemma 6.2. *Let $m \in \mathbb{Z}_{\geq 0}$, and let $k \in \mathbb{Z}^+$ with p -adic p -composition $(\kappa_1, \dots, \kappa_l)$. Then*

- (1) $\mathfrak{S}_{p^m}^{[p]} \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] = \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$;
- (2) $\mathfrak{S}_k^{[p]} \cap \prod_{\kappa} \mathfrak{S}_{p^{\kappa_i+1}} = \prod_{\kappa} \mathfrak{S}_{p^{\kappa_i}}^{[p]}$.

Proof. Note first that $\mathfrak{S}_{p^m}^{[p]}$ consists *precisely* of the permutations of $\mathfrak{S}_{p^{m+1}}$ which, in the natural action, induce row permutations on the tableau T . Suppose that $\sigma^{[p]} \in \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$ for some $\sigma \in \mathfrak{S}_{p^m}$. Then $\sigma^{[p]}$ leaves each successive block in $[1, p^{m+1}]$ of size p^m invariant. Thus, on the tableau T , $\sigma^{[p]}$ leaves each of the p sub-tableaux consisting of p^{m-1} successive rows of T invariant setwise, so that $\sigma^{[p]} \in \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$. This shows $\mathfrak{S}_{p^m}^{[p]} \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] \subseteq \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$. The converse clearly holds, since $\mathfrak{S}_{p^{m-1}}^{[p]} \subseteq \mathfrak{S}_{p^m}$ and

$$\prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i] = \left(\prod_{i=1}^p \mathfrak{S}_{p^{m-1}}[i] \right)^{[p]} \subseteq \mathfrak{S}_{p^m}^{[p]}.$$

This proves part (1). Part (2) is similar. \square

Proposition 6.3. *Let $k \in \mathbb{Z}^+$ such that $p \nmid k$, with p -adic p -composition $\kappa = (\kappa_1, \kappa_2, \dots, \kappa_l)$. For each $i \in [1, l]$, let $x_i, y_i \in X_{p^{\kappa_i}}$. Let $x_l = y_l = 1$, and let $x = \prod_{\kappa} x_i$ and $y = \prod_{\kappa} y_i$. The following statements are equivalent:*

- (1) $\mathfrak{S}_{p^{\kappa_i}}^{[p]} x_i = \mathfrak{S}_{p^{\kappa_i}}^{[p]} y_i$ for all $i \in [1, l]$;
- (2) $\mathfrak{S}_k^{[p]} x = \mathfrak{S}_k^{[p]} y$;
- (3) $Dx = Dy$.

Proof. (1) \Rightarrow (2) and (2) \Rightarrow (3) follow from the fact that

$$\prod_{\kappa} \mathfrak{S}_{p^{\kappa_i}}^{[p]} \subseteq \mathfrak{S}_k^{[p]} \subseteq D.$$

(3) \Rightarrow (1): Suppose that $Dx = Dy$. Then there exist $\sigma \in \mathfrak{S}_k$ and $\tau \in \mathfrak{S}_p$ such that

$$(*) \quad \sigma^{[p]}(\Delta_k \tau) \prod_{\kappa} x_i = \prod_{\kappa} y_i.$$

This gives

$$\sigma^{[p]} = \prod_{\kappa} (y_i x_i^{-1} (\Delta_{p^{\kappa_i}} \tau)^{-1}) \in \prod_{\kappa} \mathfrak{S}_{p^{\kappa_i+1}},$$

so that $\sigma^{[p]} \in \prod_{\kappa} \mathfrak{S}_{p^{\kappa_i}}^{[p]}$ by Lemma 6.2(2). Thus, for each $i \in [1, l]$ there exists $\sigma_i \in \mathfrak{S}_{p^{\kappa_i}}$ such that $\sigma^{[p]} = \prod_{\kappa} \sigma_i^{[p]}$. Putting this into (*), we get, for all $i \in [1, l]$,

$$\sigma_i^{[p]}(\Delta_{p^{\kappa_i}} \tau) x_i = y_i.$$

When $i = l$, we have $\sigma_l = 1$ since $\kappa_l = 0$, and hence $\tau = 1$, since $x_l = y_l = 1$. Thus, we have, for $i \in [1, l]$,

$$y_i = \sigma_i^{[p]} x_i \in \mathfrak{S}_{p^{\kappa_i}}^{[p]} x_i.$$

□

In view of Proposition 6.3, our problem reduces to determining the necessary and sufficient conditions for $\mathfrak{S}_{p^m}^{[p]} x = \mathfrak{S}_{p^m}^{[p]} y$ where $x, y \in X_{p^m}$.

Recall that X_{p^m} is a disjoint union of Y_m and $\prod_{i=1}^p X_{p^{m-1}}[i]$ (Lemma 5.7(2)). We consider these two sets separately.

Proposition 6.4. *Let $m \in \mathbb{Z}^+$ and for each $i \in [1, p]$, let $x_i, y_i \in X_{p^{m-1}}$. The following statements are equivalent:*

- (1) $\mathfrak{S}_{p^m}^{[p]}(\prod_{i=1}^p x_i[i]) = \mathfrak{S}_{p^m}^{[p]}(\prod_{i=1}^p y_i[i])$.
- (2) $\mathfrak{S}_{p^{m-1}}^{[p]} x_i = \mathfrak{S}_{p^{m-1}}^{[p]} y_i$ for all $i \in [1, p]$.

The proof of this is straightforward, using Lemma 6.2(1). It remains to consider the right cosets $\mathfrak{S}_{p^m}^{[p]} x$ where $x \in Y_m$.

Proposition 6.5. *Let $m \in \mathbb{Z}_{\geq 0}$. Suppose that there exist $x \in X_{p^m}$ and $y \in Y_m$ such that $\mathfrak{S}_{p^m}^{[p]} x = \mathfrak{S}_{p^m}^{[p]} y$. Then $x = y$.*

Proof. We have $y = \tau^{[p]}x$ for some $\tau \in \mathfrak{S}_{p^m}$. Since $y \in Y_m$, we have $(\Delta_{p^m}\pi)^y \in R_m \setminus B_m$, and since $\tau^{[p]}$ centralises $\Delta_{p^m}\pi$ we have

$$(\Delta_{p^m}\pi)^x = (\Delta_{p^m}\pi)^y \in R_m \setminus B_m.$$

We claim that $x \in Y_m$. If not, then $x \in \prod_{i=1}^p X_{p^{m-1}}[i] \subseteq \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$, say $x = \prod_{i=1}^p x_i[i]$, and then $(\Delta_{p^m}\pi)^x = \prod_{i=1}^p (\Delta_{p^{m-1}}\pi)^{x_i}[i] \in \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$, a contradiction since $(R_m \setminus B_m) \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] = \emptyset$. Thus $x \in Y_m$ and hence $x = y$ by the uniqueness result of Proposition 5.5. \square

Theorem 6.6. *Let $k \in \mathbb{Z}^+$ with $p \nmid k$. Then X_{k-1} is a transversal of the right cosets Dx satisfying $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.*

Proof. This follows from Propositions 6.1, 6.3, 6.4 and 6.5. \square

Corollary 6.7.

- (1) *Let $m \in \mathbb{Z}_{\geq 0}$, and let $a_m = |X_{p^m}|$. Then a_m satisfies the following recurrence relation (where $a_{-1} = 0$):*

$$a_m = a_{m-1}^p + p^{2p^m-1}(p-1).$$

- (2) *Let $k \in \mathbb{Z}^+$ such that $p \nmid k$, with p -adic p -composition $(\kappa_1, \dots, \kappa_l)$. Then the number of right cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$ equals $\prod_{i=1}^{l-1} a_{\kappa_i}$.*

Proof. From the uniqueness of Proposition 5.5, we have

$$|Y_m| = |H_{p^m}| |\mathbb{Z}_p^*| |R_{m-1}|^{p-1} = p^{2p^m-1}(p-1)$$

(note that $|R_{m-1}| = p^{\frac{p^m-1}{p-1}}$). The corollary thus follows from Lemma 5.7(1,2) and Theorem 6.6. \square

From Corollaries 3.5 and 6.7, we have

$$\dim((\text{Res}_P \text{Lie}(kp))_{pf}) = (p-1)(k-1)! \prod_{i=1}^{l-1} a_{\kappa_i},$$

where $(\kappa_1, \dots, \kappa_l)$ is the p -adic p -composition of k . Since

$$\prod_{i=1}^{l-1} a_{\kappa_i} \geq a_{\kappa_1} \geq p^{2p^{\kappa_1}-1}(p-1) > p^{\frac{2k}{p}-1}(p-1)$$

(note that $p^{\kappa_1+1} > k$), we see that $\prod_{i=1}^{l-1} a_{\kappa_i}$, and hence $\dim((\text{Res}_P \text{Lie}(kp))_{pf})$, grows exponentially with k .

Remark. Selick and Wu [SW2] computed explicitly $\text{Lie}^{\max}(6)$ and $\text{Lie}^{\max}(8)$ in characteristic two. In particular, they showed that $\text{Lie}^{\max}(6)$ has dimension 96, which is also the upper bound computed by our recurrence formula.

REFERENCES

- [B] D. J. Benson, 'Representations and cohomology I: Basic representation theory of finite groups and associative algebras', *Cambridge Studies in Advanced Mathematics* **30**, Cambridge University Press, Cambridge, 1991.
- [CT] F. Cohen, K. M. Tan, 'An upper bound for $\dim(\text{Lie}^{\max}(n))$ ', unpublished, 2002.
- [ES] K. Erdmann, M. Schocker, 'Modular Lie powers and the Solomon descent algebra', *Math. Z.* **253** (295–313), 2006.
- [SW1] P. Selick, J. Wu, 'Natural coalgebra decomposition of tensor algebras and loop suspensions', *Mem. Amer. Math. Soc.* **148**, 2000.
- [SW2] P. Selick, J. Wu, 'Some calculations for $\text{Lie}(n)^{\max}$ for low n ', *J. Pure Appl. Algebra* **212** (2570–2580), 2008.

(K. Erdmann) MATHEMATICAL INSTITUTE, 24–29 ST GILES', OXFORD, OX1 3LB, UNITED KINGDOM.

E-mail address: `erdmann@maths.ox.ac.uk`

(K. M. Tan) DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF SINGAPORE, 2, SCIENCE DRIVE 2, SINGAPORE 117543.

E-mail address: `tankm@nus.edu.sg`