Conjugate p-elements of Full Support that Generate the Wreath Product Cp wr Cp

Ward, David

2014

MIMS EPrint: **2014.30**

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

Reports available from: http://eprints.maths.manchester.ac.uk/
And by contacting: The MIMS Secretary
School of Mathematics
The University of Manchester
Manchester, M13 9PL, UK

ISSN 1749-9097

Conjugate p-elements of Full Support that Generate the Wreath Product $C_p \wr C_p$

David Ward

Abstract

For a symmetric group $G := \mathrm{Sym}(n)$ and a conjugacy class X of involutions in G, it is known that if the class of involutions does not have a unique fixed point, then - with a few small exceptions - given two elements $a, x \in X$, either $\langle a, x\rangle$ is isomorphic to the dihedral group D_8, or there is a further element $y \in X$ such that $\langle a, y\rangle \cong \langle x, y\rangle \cong D_8$ (P. Rowley and D. Ward, On π-Product Involution Graphs in Symmetric Groups. MIMS ePrint, 2014).

One natural generalisation of this to p-elements is to consider when two conjugate p-elements generate a wreath product of two cyclic groups of order p. In this paper we give a necessary and sufficient condition for this in the case that our p-elements have full support.

1 Introduction

Given a finite group G and a prime p dividing the order of G, the poset $\mathcal{S}_p(G)$ consisting of all non-trivial p-subgroups of G has been the subject of much work. By analysing $\mathcal{S}_p(G)$ together with the subposet $\mathcal{A}_p(G)$ of all non-trivial elementary abelian p-subgroups of G, and their associated order complexes - the respective Brown and Quillen complexes - it is possible to derive results about both the group G and its representations. The complex $\mathcal{S}_p(G)$ was studied by Brown in his paper [9]. Later, Quillen considered these complexes and proved in [18], that the order complexes $|\mathcal{S}_p(G)|$ and $|\mathcal{A}_p(G)|$ were homotopy equivalent, with the homotopy commuting with the underlying G-action.

Brown's motivation for studying the poset $\mathcal{S}_p(G)$ was the calculation of cohomology groups of certain discrete finite groups - the subject of [10]. It is also possible to use homological methods to construct representations for G by considering the Brown and Quillen complexes as simplicial complexes. This was the approach used by Ronan and Smith in [19], [20], [21] and [22].

The rich structure of the conjugacy classes of p-elements in $G := \mathrm{Sym}(n)$, leads to an equally rich structure in the poset $\mathcal{S}_p(G)$. In general the homotopy type of $\mathcal{S}_p(G)$ is still unknown, although in the case that $n = 3p$ it has been determined [25]. In the case that $p = 2$ a section of the poset $\mathcal{S}_p(G)$ involves two conjugate involutions of G generating the dihedral group, D_8, of order 8. A full analysis of this situation was undertaken in [23]. It was seen that if $X = a^G$ - the G-conjugacy class of an involution a, that does not have a unique fixed point - then except in a few small cases, any $x \in X$ either satisfies $\langle a, x\rangle \cong D_8$ or there exists some $y \in X$ satisfying $\langle a, y\rangle \cong \langle x, y\rangle \cong D_8$. This result was obtained

using graphs know as x-graphs. These were basic graphs that indicated the interactions of the disjoint transpositions of conjugate involutions and were first introduce by Bates, Bundy, Perkins and Rowley in [4]. They form part of a rich cornucopia of graphs that may be associated to groups, the study of which allows properties of the groups to be determined. These include commuting involution graphs [4], [5], [6], [13], [17] , [24], local fusion graphs [1], [2] and commuting graphs [3], [8], [15], [16].

There are two natural generalisations of the given result from [23]. The first would consider when two conjugate involutions generate the dihedral group D_{2^m} for $m > 3$. An analysis of x-graphs would by fundamental in such an approach, which would then become a case-by-case analysis of the possible situations that could arise.

An alternative generalisation involves considering D_8 as the wreath product, $C_2 \wr C_2$, of two cyclic groups of order 2. From this viewpoint, a natural generalisation is to consider when two conjugate p-elements of $\mathrm{Sym}(n)$ generate the wreath product $C_p \wr C_p$. In this paper, we consider conjugate p-elements of full support in $\mathrm{Sym}(n)$ that generate this wreath product. To analyse such situations, it would be desirable to form a generalisation of the x-graph. The natural generalisation results in non-planar directed graphs and hence we consider the adjacency matrix of such a graph. Indeed, given conjugate p-elements a and x of full support in $\mathrm{Sym}(n)$, we form suitable matrices A_x^a and A_a^x. Here a will be the standard p-element of G namely $a = (1, 2, \ldots, p)(p+1, \ldots, 2p) \cdots ((r-1)p+1, \ldots, rp)$ where $n = rp$ and we label the p-cycles forming a by $\alpha_i = (p(i-1)+1, \ldots, pi)$ for $i = 1, \ldots, r$. Similarly if x is a G-conjugate of a, then we may label its disjoint p-cycles by $\chi_1, \ldots, \chi_r$. The matrices A_x^a and A_a^x have (i, j) entries given by $|\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_j)|$ and $|\mathrm{supp}(\chi_i^a) \cap \mathrm{supp}(\chi_j)|$ respectively.

Throughout, p will be an odd prime. Our first result considers the case that $n = p^2$. We see that the matrices A_x^a and A_a^x do indeed encode data which we may use to determine when a and x generate the wreath product $W_p := C_p \wr C_p$. This encoding involves circulant matrices and their representer polynomials as defined in Section 2.

Theorem 1.1. *Let $G = \mathrm{Sym}(p^2)$, a be the standard p-element of G and let x be a conjugate of a. Then $\langle a, x\rangle \cong W_p$ precisely when the following two equivalent conditions hold*

(i) $A_x^a = p \cdot Y_\sigma$ for some p-cycle $\sigma \in \mathrm{Sym}(p)$, $A_a^x = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$, $X = 1$ is a simple root of the representer polynomial $f_{A_a^x}(X) \in \mathbb{Z}_p[X]$ and $[a, a^x] = 1$.

(ii) $A_x^a = p \cdot Y_\sigma$ for some p-cycle $\sigma \in \mathrm{Sym}(p)$, $A_a^x = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$, $|\det(A_a^x)|_p = p^2$ and $[a, a^x] = 1$.

(or (i) and (ii) hold with the roles of a and x interchanged).

The second result concerns the case when $n = p^3$. It involves the notions of the block sum matrix, $BS(M)$, of a matrix M and of a reduced representer polynomial as given in Definitions 5.5 and 5.6.

Theorem 1.2. *Let $G = \mathrm{Sym}(p^3)$, a be the standard p-element of G and let x be a conjugate of a. Moreover, suppose that we cannot decompose $a = a_1 \cdots a_p$ and $x = x_1 \cdots x_p$ with a_i, x_i sitting inside a copy of $\mathrm{Sym}(p^2)$ for each i with one*

such pair satisfying the conditions of Theorem 1.1. Then $\langle a, x\rangle \cong W_p$ *precisely when up to a renumbering of the* α_i *the following conditions hold*

(i) $[a, a^{x^i}] = 1$ *for all* $i = 1, \ldots, (p-1)/2$*;*

(ii) A_x^a *is a block matrix having* $p \times p$ *blocks, all of which are zero except for those immediately above the leading diagonal. The non-zero* $p \times p$ *blocks are either equal to* $p \cdot Y_\sigma$ *for some* $\sigma \in \mathrm{Sym}(p)$ *or have every entry equal to* 1*. Moreover,* A_x^a *contains at least one block whose entries are all equal to* 1*; and*

(iii) A_a^x *is a block matrix having* $p \times p$ *blocks each of which is circulant and the diagonal blocks are all equal. Moreover, either*

(c1) $X = 1$ *is a root of multiplicity at least* 2 *of the representer polynomial* $f_{BS(A_a^x)}(X) \in \mathbb{Z}_p[X]$ *but is not a root of the representer polynomial* $f'_{BS(A_a^x)}(X) \in \mathbb{Z}_{p^2}[X]$*; or*

(c2) $X = 1$ *is not a root of the reduced representer polynomial* $g'_{A_a^x}(X) \in \mathbb{Z}_{p^2}[X]$*;*

(or (i)*,* (ii) *and* (iii) *hold - up to a renumbering of the* χ_i *- with the roles of* a *and* x *interchanged).*

Our final result combines Theorems 1.1 and 1.2 to consider the most general setting.

Theorem 1.3. *Let* $r \geq p$*,* $n = rp$ *and* $G = \mathrm{Sym}(n)$*. If* a *is the standard* p*-element of* G *having* G*-conjugacy class* X *and* $x \in X$*, then* $\langle a, x\rangle \cong W_p$ *precisely when for a suitable renumbering of the* α_i *and* χ_j *the following conditions hold*

(i) $[a, a^{x^i}] = 1$ *for* $i = 1, \ldots, (p-1)/2$*;*

(ii) A_x^a *is a block diagonal matrix having blocks* D_1*,* D_2 *and* D_3*, where*

- $D_1 = p \cdot I$ *for some identity matrix* I*;*
- D_2 *is a block diagonal matrix having* $p \times p$ *blocks, where each block has the form* $p \cdot Y_\sigma$ *for some* p*-cycle* $\sigma \in \mathrm{Sym}(p)$*; and*
- D_3 *is a block diagonal matrix having* $p^2 \times p^2$ *blocks having the form of the matrix* A_x^a *from Theorem 1.2.*

(iii) A_a^x *is a block diagonal matrix having blocks* E_1*,* E_2 *and* E_3*, where*

- $E_1 = D_1$*;*
- E_2 *is a block diagonal matrix of the same size as* D_2*, where each block is a* $p \times p$ *circulant matrix having row sum equal to* p*; and*
- E_3 *is a block diagonal matrix of the same size as* D_3*, where each block is a* $p^2 \times p^2$ *block matrix having* $p \times p$ *blocks each of which is circulant and the diagonal blocks are all equal.*

(iv) One of the following holds

- *The representer polynomial* $f_B(X) \in \mathbb{Z}_p[X]$ *of at least one of the circulant blocks,* B*, of* E_2 *has a simple root at* $X = 1$*;*

- *There is at least one block, C, of E_3 such that $X = 1$ is a root of multiplicity at least 2 over $\mathbb{Z}_p$ of the representer polynomial of the block sum matrix $BS(C)$ but $X = 1$ is not a root of the representer polynomial $f'_{BS(C)}(X) \in \mathbb{Z}_{p^2}[X]$;*
- *There is at least one block, C, of E_3 such that $X = 1$ is not a root of the reduced representer polynomial $g'_C(X) \in \mathbb{Z}_{p^2}[X]$.*

(or the conditions $(i) - (iv)$ hold with the roles of a and x interchanged)

This paper is arranged as follows. In Section 2 we define the matrices A_x^a and A_a^x and give some basic results about the wreath product $C_p \wr C_p$. We also introduce the notion of circulant matrices and illustrate a number of properties that they satisfy, which will be used in our subsequent work. Sections 3 and 4 consider the case that $n = p^2$. The former section leads up to a proof of the equivalence of $\langle a, x\rangle \cong W_p$ and part (i) of Theorem 1.1, whilst the latter proves the equivalence of parts (i) and (ii) of the same theorem. The case that $n = p^3$ is considered in Section 5 in which Theorem 1.2 is proved. Due to the technical nature of some of the proofs in Sections 3 and 5, both sections conclude with worked examples highlighting the key steps in the proofs. The paper concludes in Section 6, where Theorem 1.3 is proved.

2 Preliminary Results

Throughout this paper we fix a prime $p \neq 2$ and set $G := \mathrm{Sym}(pr)$ for some $r \geq p$. We consider G to be acting on the set $\Omega := \{1, \ldots, pr\}$ and fix an element $a = \alpha_1\alpha_2 \cdots \alpha_r$ where $\alpha_i = (p(i-1)+1, p(i-1)+2, \ldots, pi)$, which we will sometimes refer to as the *standard p-element of G*. We denote the G-conjugacy class of a by $X = a^G$. Given $x \in X$, it will be useful to denote the disjoint p-cycles forming x by $\chi_1, \ldots, \chi_r$. The χ_i are defined recursively by setting χ_1 to be the p-cycle for which the orbit of 1 under $\langle\chi_1\rangle$ is non-trivial. Assuming that χ_i has been defined for $1 \leq i \leq j$ we then define

$$t_j := \min\{t \in \Omega \mid \text{the orbit of } t \text{ under } \langle\chi_1, \ldots, \chi_j\rangle \text{ is trivial}\}$$

and define χ_{j+1} to be the p-cycle for which the orbit of t_j under $\langle\chi_{j+1}\rangle$ is non-trivial.

For an arbitrary element $g \in G$, we denote the set of fixed points of Ω under $\langle g\rangle$ by $\mathrm{fix}(g)$. The *support* of g, denoted $\mathrm{supp}(g)$, is defined as $\mathrm{supp}(g) := \Omega \setminus \mathrm{fix}(g)$. We shall also use the notation W_p to denote the wreath product $C_p \wr C_p$ of two cyclic groups of order p.

In [23], it was seen that when X was an arbitrary conjugacy class of involutions, then to determine when two conjugate involutions generate the wreath product $W_2 \cong D_8$, we may use graphs known as x-graphs. These graphs essentially considered the intersections of the supports of the transpositions in the decomposition of the involutions. Generalising this from a strictly graph-theoretic viewpoint is impractical. However, consideration of the adjacency matrix of such a generalisation does yield results.

Definition 2.1. *Let $x \in X$ be given. We define the $p \times p$ matrices A_x^a and A_a^x by*

$$(A_x^a)_{i,j} := |\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_j)|$$

and

$$(A_a^x)_{i,j} := |\mathrm{supp}(\chi_i^a) \cap \mathrm{supp}(\chi_j)|\,.$$

As with x-graphs, since the element a is fixed, we suppress it in our notation and denote A_x^a by A_x. The determinant of a matrix B will be denoted by $\det(B)$ and the largest power of p dividing it will be denoted $|\det(B)|_p$.

We illustrate these notions with an example. Let $p = 5$ and let a be the standard 5-element of $G := \mathrm{Sym}(25)$. Taking

$$\begin{aligned} x &= \chi_1 \cdot \chi_2 \cdot \chi_3 \cdot \chi_4 \cdot \chi_5 \\ &= (1,22,15,4,5)(2,8,7,19,9)(3,10,14,24,11) \\ &\quad (6,23,25,20,13)(12,18,16,21,17) \end{aligned}$$

in the G-conjugacy class of a, we see that

$$\alpha_1^x = (1,22,8,10,5), \quad \alpha_2^x = (2,14,23,19,7), \quad \alpha_3^x = (3,18,6,24,4),$$
$$\alpha_4^x = (9,13,21,12,16) \quad \text{and} \quad \alpha_5^x = (11,20,17,15,25).$$

Consequently

$$A_x = \begin{pmatrix} 2 & 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 \end{pmatrix}.$$

Similarly

$$\chi_1^a = (1,2,23,11,5), \quad \chi_2^a = (3,9,8,20,10), \quad \chi_3^a = (4,6,15,25,12),$$
$$\chi_4^a = (7,24,21,16,14), \quad \text{and} \quad \chi_5^a = (13,19,17,22,18).$$

This gives rise to the matrix

$$A_a^x = \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 0 & 2 & 2 & 1 & 0 \\ 2 & 0 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 & 2 \\ 1 & 1 & 0 & 1 & 2 \end{pmatrix}.$$

In Section 3 we will be concerned with two specific classes of matrices; permutation matrices and circulant matrices. Indeed, if $\sigma \in \mathrm{Sym}(n)$, then we denote by Y_σ the $n \times n$ permutation matrix defined by

$$(Y_\sigma)_{i,j} = \begin{cases} 1 & \text{if } i\sigma = j; \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

In the case that $\sigma = (1,2,\ldots,n)$, we set $\pi := Y_\sigma$. For a given $n \times n$-matrix A, multiplying A on the left by π cyclically shifts the rows of A down by a row, whilst multiplying by π on the right cyclically shifts the columns of A to the right by a column. Matrices that are invariant under conjugation by π are known as *circulant* matrices. Thus any circulant matrix C satisfies $C_{i,j} = C_{i+k,j+k}$ for

any $k = 1, \ldots, n$ (where we replace $i + k$ (respectively $j + k$) by $i + k - n$ (respectively $j + k - n$) if $i + k > n$ (respectively $j + k > n$)). Consequently a circulant matrix is uniquely determined by its first row, and we denote the circulant matrix

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{pmatrix},$$

by $C = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1})$.

Associated to any circulant matrix $C = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1})$, is the *representer* polynomial $f_C(X)$ in the indeterminant X, given by

$$f_C(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n-1} X^{n-1}.$$

Strictly speaking this is a polynomial with coefficients in the underlying ring of C. However, in this paper the underlying ring of our circulant matrices will be the integers, and it will sometimes be preferable to consider $f_C(X)$ as an element of $\mathbb{Z}_p[X]$ or $\mathbb{Z}_{p^2}[X]$. The following result illustrates this correspondence.

Lemma 2.2. *Let $X = \mathrm{circ}(x_0, \ldots, x_{p-1})$ be an integer circulant matrix. Then* $\det(X) \equiv x_0 + \cdots + x_{p-1} \pmod{p}$.

Proof. Expanding $\det(X)$ gives a series of summands $\alpha_{a_0 \cdots a_{p-1}} x_0^{a_0} x_1^{a_1} \cdots x_{p-1}^{a_{p-1}}$ where $a_0 + \cdots + a_{p-1} = p$ and $a_i \in \mathbb{N}$. Clearly if $a_i = p$ for some i, then the coefficient $\alpha_{a_0 \cdots a_{p-1}}$ is equal to 1 and the corresponding summand of $\det(X)$ is x_i^p. Conversely, consider an occurrence of $x_0^{a_0} \cdots x_{p-1}^{a_{p-1}}$ in the expansion of $\det(X)$ where no a_j is equal to p. Suppose that $x_0^{a_0} \cdots x_{p-1}^{a_{p-1}}$ occurs from the entries $X_{i_1,j_1}, \ldots, X_{i_p,j_p}$ of X. Due to the circular nature of entries of X, it will also occur from the entries $X_{i_1+k,j_1+k}, \ldots, X_{i_p+k,j_p+k}$ for $k = 1, \ldots, p-1$ (where we set $X_{i+p,j}$, $X_{i,j+p}$ and $X_{i+p,j+p}$ equal to $X_{i,j}$ for $i, j = 1, \ldots, p$). Since each a_j is not equal to p, and $p \neq 2$ we conclude that

$$\{X_{i_1+s,j_1+s}, \ldots X_{i_p+s,j_p+s}\} \neq \{X_{i_1+t,j_1+t}, \ldots X_{i_p+t,j_p+t}\}$$

for any distinct $s, t = 0, \ldots, p-1$. Moreover, consideration of the signs of each of these occurrences of $x_0^{a_0} \cdots x_{p-1}^{a_{p-1}}$ shows that they must all be equal. Since there are p such occurrences, we conclude that if $a_j \neq p$ for $j = 0, \ldots, p-1$, then $\alpha_{a_0 \cdots a_{p-1}}$ is divisible by p. Consequently, applying Fermat's Little Theorem we obtain

$$\det(X) \equiv x_0^p + \cdots + x_{p-1}^p \equiv x_0 + \cdots + x_{p-1} \pmod{p}.$$

□

We conclude this section by considering the structure of $W_p \cong \Gamma \rtimes C_p$, where Γ is an elementary abelian p-group of rank p.

Lemma 2.3. *Let p be an odd prime and let G be a group having a normal elementary abelian p-subgroup Γ of index p in G. If $a, x \in G \setminus \Gamma$ satisfy $ord(a) = ord(x) = p$ and $\langle a, x \rangle = G$, then* $\mathrm{rank}(\Gamma) \leq p - 1$.

Proof. Let $a, x \in G \setminus \Gamma$ satisfy the given properties. Since G/Γ is a cyclic p-group, by replacing x by an appropriate power, we may assume without loss of generality that $a\Gamma = x\Gamma$ and hence that the action of a on Γ is equal to the action of x on Γ.

Let $\Delta := \langle a^{-1}x\rangle \times \langle a^{-2}x^2\rangle \times \cdots \times \langle ax^{-1}\rangle$. We note that as $a\Gamma = x\Gamma$ each of $a^{-i}x^i \in \Gamma$ for $i = 1, \ldots, p-1$. Hence $\Delta \subseteq \Gamma$. Conversely, suppose that $y \in \Gamma$. As $y \in W_p = \langle a, x\rangle$, there exist $b_1, \ldots, b_{2n} \in \mathbb{Z}_p$ (for some n) such that

$$y = a^{b_1}x^{b_2}a^{b_3}x^{b_4}\cdots a^{b_{2n-1}}x^{b_{2n}} \tag{2.1}$$

Note that as $G/\Gamma = \langle a\Gamma\rangle = \langle x\Gamma\rangle$, we have the relation $\sum_{i=1}^{2n} b_i \equiv 0 \pmod{p}$.

We now proceed to build y recursively. We assume that y is written in the form (2.1) such that no b_i is zero. In the case that $b_1 = 0$ or $b_{2n} = 0$, an analogous argument holds. Define $y_1 := a^{b_1}x^{-b_1}$. Thus y_1 agrees with y in the first position. Now assume that we have defined $y_i \in \Delta$ for some $i < 2n$ such that $y_i = a^{b_1}x^{b_2}\cdots a^{b_i}x^d$ or $y_i = a^{b_1}x^{b_2}\cdots x^{b_i}a^d$ depending on the parity of i. Here $d := -\sum_{j=1}^{i} b_i$. Thus y_i agrees with y on the first i entries. In the former case define $y_{i+1} := y_i x^{b_{i+1}-d}a^{d-b_{i+1}}$ and in the latter case define $y_{i+1} := y_i a^{b_{i+1}-d}x^{d-b_{i+1}}$. Thus $y_{i+1} \in \Delta$ and y_{i+1} agrees with y in the first $i+1$ positions. Continuing in this way we may define y_i for $i = 1, \ldots 2n$, where each $y_i \in \Delta$. However,

$$y_{2n} = a^{b_1}x^{b_2}a^{b_3}x^{b_4}\cdots a^{b_{2n-1}}x^{b_{2n}}a^{-\sum_{j=1}^{2n} b_i} = y,$$

and hence $y \in \Delta$. We conclude that $\Gamma = \Delta$, from which the result follows immediately. □

Applying Lemma 2.3 to W_p we obtain the following result that we will use in Section 3.

Corollary 2.4. *Let p be an odd prime and let $a, x \in W_p$ be p-elements such that $\langle a, x\rangle = W_p$. Then either $[a, a^{x^i}] = 1$ or $[x, x^{a^i}] = 1$ for all $i = 1, \ldots, p$.*

3 The $n = p^2$ Case

In the next two sections, we prove Theorem 1.1. This theorem reflects the fact that in the wreath product $C_p \wr C_p$, the p copies of C_p are permuted in a p-cycle, and elements within each copy of C_p have a circular orbit.

The proof of Theorem 1.1 can be split into two separate cases. In Subsection 3.1, we will prove the equivalence of $\langle a, x\rangle \cong W_p$ with part (i) of Theorem 1.1. This is proved in Proposition 3.2. Due to the technical nature of the proofs in this subsection, we follow this in Subsection 3.2 with a worked example mirroring the proofs. The equivalence of parts (i) and (ii) of Theorem 1.1 is then proved in Section 4 as Theorem 4.2.

3.1 The Results

We begin by formulating a result relating the conjugation action of x on a to the rank of an elementary abelian p-group.

Lemma 3.1. *Let $G = \mathrm{Sym}(p^2)$, a be the standard p-element of G and let x be a conjugate of a. If $\alpha_1^{x^{j-1}} = \alpha_{1\sigma^{j-1}}^{e_{1\sigma^{j-1}}}$ for some p-cycle $\sigma \in \mathrm{Sym}(p)$, some $e_1, \ldots, e_p \in \mathbb{Z}_p$ and for all $j = 1, \ldots, p$, then the elementary abelian p-group $\Gamma := \langle a^{x^j} | j = 0, \ldots, p-1 \rangle$ has rank p if and only if $e_1^{-1} + \cdots + e_p^{-1} \not\equiv 0 \pmod{p}$.*

Proof. For simplicity of subsequent arguments we define $e_0 := e_p$. Let $d_1, \ldots, d_p \in \mathbb{Z}_p$ be such that

$$\prod_{i=1}^{p} (a^{x^i})^{d_i} = 1. \tag{3.1}$$

As $\alpha_1^{x^{j-1}} = \alpha_{1\sigma^{j-1}}^{e_1\sigma^{j-1}}$, it follows that $a^x = \prod_{j=1}^{p} \alpha_{1\sigma^j}^{e_{1\sigma^{j-1}}^{-1} e_{1\sigma^j}}$. Iterating this we have that $a^{x^2} = \prod_{j=1}^{p} \alpha_{1\sigma^j}^{e_{1\sigma^{j-2}}^{-1} e_{1\sigma^j}}$ and in general $a^{x^i} = \prod_{j=1}^{p} \alpha_{1\sigma^j}^{e_{1\sigma^{j-i}}^{-1} e_{1\sigma^j}}$. Thus we may write (3.1) as

$$\prod_{i=1}^{p} \left(\prod_{j=1}^{p} \alpha_{1\sigma^j}^{e_{1\sigma^{j-i}}^{-1} e_{1\sigma^j}} \right)^{d_i} = 1. \tag{3.2}$$

For ease of notation we will assume without loss of generality that $\sigma = (1, 2, \ldots, p)$. Thus (3.2) becomes

$$\prod_{i=1}^{p} \prod_{j=1}^{p} \alpha_{j+1}^{(e_{j-i+1}^{-1} e_{j+1}) d_i} = \prod_{i=1}^{p} \left(\prod_{j=1}^{p} \alpha_{j+1}^{e_{j-i+1}^{-1} e_{j+1}} \right)^{d_i} = 1. \tag{3.3}$$

It follows that for a fixed $\ell \in \{1, \ldots, p\}$, the exponent of α_ℓ in (3.3) is congruent to $0 \pmod{p}$. Thus we have

$$\sum_{i=1}^{p} (e_{\ell-i}^{-1} e_\ell) d_i \equiv 0 \pmod{p}. \tag{3.4}$$

The equations in (3.4) give rise to a homogeneous system of linear equations with coefficient matrix given by $A = (a_{\ell,i})$, where $a_{\ell,i} = e_{\ell-i}^{-1} e_\ell$. This matrix is invertible if and only if the matrix $B = (b_{\ell,i})$ is invertible, where $b_{\ell,i} = e_{\ell-i}^{-1}$. We may conclude that there is a non-trivial solution to (3.1) precisely when $\det(B) \equiv 0 \pmod{p}$. However, $B = \mathrm{circ}(e_p^{-1}, e_{p-1}^{-1}, \ldots, e_1^{-1})$ and so appealing to Lemma 2.2 we deduce that this occurs precisely when $e_1^{-1} + \cdots + e_p^{-1} \equiv 0 \pmod{p}$. □

Lemma 3.1 underpins the proof of the equivalence of $\langle a, x \rangle \cong W_p$ and part (i) of Theorem 1.1, as it allows us to relate the coefficients of the circulant matrix - A_a^x or A_x - with the base group of the wreath product W_p.

Proposition 3.2. *Let $G = \mathrm{Sym}(p^2)$, a be the standard p-element of G and let x be a conjugate of a. The following are equivalent*

(i) $\langle a, x \rangle \cong W_p$;

(ii) $A_x = p \cdot Y_\sigma$ *for some p-cycle* $\sigma \in \mathrm{Sym}(p)$, $A_a^x = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$, $X = 1$ *is a simple root of the representer polynomial* $f_{A_a^x}(X) \in \mathbb{Z}_p[X]$ *and* $[a, a^x] = 1$ *(or with the roles of a and x interchanged).*

Proof. Throughout the proof we write $a = \alpha_1 \cdots \alpha_p$ as in Section 2. Assume that $\langle a, x\rangle \cong W_p$. By Corollary 2.4 either $[a, a^{x^i}] = 1$ or $[x, x^{a^i}] = 1$ for all $i = 1, \ldots, p$. Without loss of generality assume that $[a, a^{x^i}] = 1$ for all $i = 1, \ldots, p$. An analogous argument can be used in the case that $[x, x^{a^i}] = 1$.

As $[a, a^{x^i}] = 1$, either $\mathrm{supp}(\alpha_i^x) = \mathrm{supp}(\alpha_{i\sigma})$ for each $i = 1, \ldots, p$ and some p-cycle $\sigma \in \mathrm{Sym}(p)$, or $|\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_j)| = 1$ for all i, j. If the former case holds, then $A_x = p \cdot Y_\sigma$. If the latter case holds, then in particular $|\mathrm{supp}(\alpha_1^x) \cap \mathrm{supp}(\alpha_1)| = 1$. It follows that in the disjoint cycle decomposition of x, there exists a cycle whose support contains two elements of $\{1, \ldots, p\}$. By taking appropriate powers of a and x, we deduce that $\mathrm{ord}(a^i x^j) < p^2$ for some $1 \leq i, j \leq p-1$ and hence as $\langle a, x\rangle \cong W_p$, it follows that $\mathrm{ord}(a^i x^j) = p$. Hence

$$1 = (a^i) \cdot (a^i)^{x^{-j}} \cdot (a^i)^{x^{-2j}} \cdots (a^i)^{x^{(1-p)j}}.$$

Thus as the a^{x^m} pairwise commute, they must form an elementary abelian subgroup of order at most p^{p-1}. Moreover, as x acts on this subgroup via conjugation, it would follow that $|\langle a, x\rangle| \leq p^p < p^{p+1} = |W_p|$ and hence $\langle a, x\rangle \ncong W_p$. We conclude that the latter of the two cases cannot hold, and hence $A_x = p \cdot Y_\sigma$. Consequently $\mathrm{supp}(\alpha_i^x) = \mathrm{supp}(\alpha_{i\sigma})$ for each $i \in \{1, \ldots, p\}$.

Since $[a, a^x] = 1$, we conclude that $\alpha_i^x \in \langle \alpha_{i\sigma}\rangle$ for each $i \in \{1, \ldots, p\}$. It follows that $A_a^x = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$ with the sum of the c_i's equal to p. In particular $X = 1$ is a root of the representer polynomial $f_{A_a^x}(X) \in \mathbb{Z}_p[X]$.

Define $\Gamma := \langle a^{x^j} | j = 1, \ldots, p\rangle$. Thus Γ is an elementary abelian p-group of rank p. Moreover $\alpha_1^{x^{j-1}} = \alpha_{1\sigma^{j-1}}^{e_{1\sigma^{j-1}}}$. Define a_i for $i = 1, \ldots, p$ recursively by $a_1 := \min\{i \mid c_i \neq 0\}$ and

$$a_i := \min\left\{ \ell \;\middle|\; \sum_{j=1}^{\ell} j \cdot c_j > \sum_{j=1}^{i-1} a_j \right\}$$

for $i > 1$. As multisets we have that

$$\{a_i \mid i = 1, \ldots, p\} = \{e_i^{-1} \mid i = 1, \ldots, p\}.$$

Appealing to Lemma 3.1 we see that, as Γ has rank p, then $a_1 + \cdots + a_p \not\equiv 0 \pmod{p}$. Consequently

$$f'_{A_a^x}(1) = \sum_{i=0}^{p-1} i \cdot c_i = \sum_{i=1}^{p} a_i \not\equiv 0 \pmod{p},$$

and the representer polynomial of A_a^x has a simple root at $X = 1$ as required.

Conversely, assume that the conditions in (ii) hold. As $A_x = p \cdot Y_\sigma$, it follows that $\mathrm{supp}(\alpha_i^x) = \mathrm{supp}(\alpha_{i\sigma})$. Moreover, as $[a, a^x] = 1$ we have $\alpha_i^x \in \langle \alpha_{i\sigma}\rangle$. Defining $\Gamma := \langle a^{x^i} | i = 1, \ldots, p\rangle$ we deduce that Γ is an elementary abelian p-group upon which $\langle x\rangle$ acts, and $\Gamma \cap \langle x\rangle = \{1\}$. Thus it suffices to prove that $\mathrm{rank}(\Gamma) = p$. However, an analogous argument to that used above involving the a_i, c_i and e_i shows that this is equivalent to proving that $f'_{A_a^x}(1) \not\equiv 0 \pmod{p}$, which holds as $f_{A_a^x}(X)$ has a simple root at $X = 1$. □

We note that all of the conditions in Proposition 3.2 are necessary. Indeed, the necessity of the structure of A_x and A_a^x was evident in the proof of the proposition. However, if $p = 5$ and

$$\begin{aligned} x =&(1,6,11,16,21)(2,7,14,18,25)(3,9,15,17,23)\\ &(4,8,12,20,24)(5,10,13,19,22), \end{aligned}$$

then the matrices A_x and A_a^x are given by

$$A_x = 5 \cdot \pi \qquad \text{and} \qquad A_a^x = \operatorname{circ}(0,2,1,1,1)$$

both of which satisfy the conditions in the proposition. However, in this case $[a, a^x] \neq 1$.

3.2 A Worked Example

To illustrate what is happening in the proofs of Lemma 3.1 and Proposition 3.2, we give an explicit example. Indeed, let $p = 5$ and consider $G = \operatorname{Sym}(25)$, having standard 5-element $a = (1,2,3,4,5)\cdots(21,22,23,24,25) \in G$. Using the computer algebra system MAGMA (see [7] and [11]) we may take a random element, x, of the G-conjugacy class of a that satisfies $\langle a, x\rangle \cong W_5$, namely

$$\begin{aligned} x =&(1,6,11,16,21)(2,9,12,19,22)(3,7,13,17,23)\\ &(4,10,14,20,24)(5,8,15,18,25). \end{aligned}$$

We now consider the methodology from the proofs of Lemma 3.1 and Proposition 3.2 in this specific case.

3.2.1 Lemma 3.1

We have that

$$\begin{aligned} &\alpha_1^x = (6,9,7,10,8) = \alpha_2^3, && \alpha_1^{x^2} = (11,12,13,14,15) = \alpha_3,\\ &\alpha_1^{x^3} = (16,19,17,20,18) = \alpha_4^3, && \alpha_1^{x^4} = (21,22,23,24,25) = \alpha_5,\\ & && \alpha_1^{x^5} = (1,2,3,4,5) = \alpha_1. \end{aligned}$$

Thus - using the notation from Lemma 3.1 - $\sigma = (1,2,3,4,5)$ and $(e_1,e_2,e_3,e_4,e_5) = (1,3,1,3,1)$. Conjugating a by successive powers of x gives

$$\begin{aligned} a^x &= \alpha_1^1\cdot\alpha_2^3\cdot\alpha_3^2\cdot\alpha_4^3\cdot\alpha_5^2 &&= \alpha_1^{e_5^{-1}e_1}\cdot\alpha_2^{e_1^{-1}e_2}\cdot\alpha_3^{e_2^{-1}e_3}\cdot\alpha_4^{e_3^{-1}e_4}\cdot\alpha_5^{e_4^{-1}e_5},\\ a^{x^2} &= \alpha_1^2\cdot\alpha_2^3\cdot\alpha_3^1\cdot\alpha_4^1\cdot\alpha_5^1 &&= \alpha_1^{e_4^{-1}e_1}\cdot\alpha_2^{e_5^{-1}e_2}\cdot\alpha_3^{e_1^{-1}e_3}\cdot\alpha_4^{e_2^{-1}e_4}\cdot\alpha_5^{e_3^{-1}e_5},\\ a^{x^3} &= \alpha_1^1\cdot\alpha_2^1\cdot\alpha_3^1\cdot\alpha_4^3\cdot\alpha_5^2 &&= \alpha_1^{e_3^{-1}e_1}\cdot\alpha_2^{e_4^{-1}e_2}\cdot\alpha_3^{e_5^{-1}e_3}\cdot\alpha_4^{e_1^{-1}e_4}\cdot\alpha_5^{e_2^{-1}e_5},\\ a^{x^4} &= \alpha_1^2\cdot\alpha_2^3\cdot\alpha_3^2\cdot\alpha_4^3\cdot\alpha_5^1 &&= \alpha_1^{e_2^{-1}e_1}\cdot\alpha_2^{e_3^{-1}e_2}\cdot\alpha_3^{e_4^{-1}e_3}\cdot\alpha_4^{e_5^{-1}e_4}\cdot\alpha_5^{e_1^{-1}e_5},\\ a^{x^5} &= \alpha_1^1\cdot\alpha_2^1\cdot\alpha_3^1\cdot\alpha_4^1\cdot\alpha_5^1 &&= \alpha_1^{e_1^{-1}e_1}\cdot\alpha_2^{e_2^{-1}e_2}\cdot\alpha_3^{e_3^{-1}e_3}\cdot\alpha_4^{e_4^{-1}e_4}\cdot\alpha_5^{e_5^{-1}e_5}. \end{aligned}$$

Hence we have confirmed the formula $a^{x^i} = \prod_{j=1}^{p} \alpha_{1\sigma^j}^{e_{1\sigma^{j-i}}^{-1}e_{1\sigma^j}}$ from the proof of the lemma. Consequently, a non-trivial relation between that a^{x^i} will give a

non-trivial solution to $Ax \equiv 0 \pmod{p}$, where the matrix $A = (A_{\ell,j})$ has the form

$$A = \begin{pmatrix} e_5^{-1}e_1 & e_4^{-1}e_1 & e_3^{-1}e_1 & e_2^{-1}e_1 & e_1^{-1}e_1 \\ e_1^{-1}e_2 & e_5^{-1}e_2 & e_4^{-1}e_2 & e_3^{-1}e_2 & e_2^{-1}e_2 \\ e_2^{-1}e_3 & e_1^{-1}e_3 & e_5^{-1}e_3 & e_4^{-1}e_3 & e_3^{-1}e_3 \\ e_3^{-1}e_4 & e_2^{-1}e_4 & e_1^{-1}e_4 & e_5^{-1}e_4 & e_4^{-1}e_4 \\ e_4^{-1}e_5 & e_3^{-1}e_5 & e_2^{-1}e_5 & e_1^{-1}e_5 & e_5^{-1}e_5 \end{pmatrix}.$$

This has a non-trivial solution precisely when the matrix

$$B = \begin{pmatrix} e_5^{-1} & e_4^{-1} & e_3^{-1} & e_2^{-1} & e_1^{-1} \\ e_1^{-1} & e_5^{-1} & e_4^{-1} & e_3^{-1} & e_2^{-1} \\ e_2^{-1} & e_1^{-1} & e_5^{-1} & e_4^{-1} & e_3^{-1} \\ e_3^{-1} & e_2^{-1} & e_1^{-1} & e_5^{-1} & e_4^{-1} \\ e_4^{-1} & e_3^{-1} & e_2^{-1} & e_1^{-1} & e_5^{-1} \end{pmatrix}.$$
$$= \operatorname{circ}(e_5^{-1}, e_4^{-1}, e_3^{-1}, e_2^{-1}, e_1^{-1}) = \operatorname{circ}(1,2,1,2,1)$$

has zero determinant (as the $e_i \in \mathbb{Z}_p$ are invertible). However, by Lemma 2.2 we have that

$$\det(B) \equiv e_5^{-1} + e_4^{-1} + e_3^{-1} + e_2^{-1} + e_1^{-1} \equiv 1+2+1+2+1 \equiv 2 \pmod{5}.$$

Thus there are no non-trivial solutions to $Ax \equiv 0 \pmod{5}$ and hence $\langle a^{x^j} | j = 0, \ldots, 4 \rangle$ has rank 5 - as can easily be verified.

3.2.2 Proposition 3.2

By the work above we have that $[a, a^x] = 1$ and that $\langle a^{x^j} | j = 0, \ldots, 4 \rangle$ is an elementary abelian 5-group of rank 5. Moreover

$$A_x = \begin{pmatrix} 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 5 & 0 & 0 & 0 & 0 \end{pmatrix} = 5 \cdot Y_{(1,2,3,4,5)} \qquad \text{and}$$

$$A_a^x = \begin{pmatrix} 0 & 3 & 2 & 0 & 0 \\ 0 & 0 & 3 & 2 & 0 \\ 0 & 0 & 0 & 3 & 2 \\ 2 & 0 & 0 & 0 & 3 \\ 3 & 2 & 0 & 0 & 0 \end{pmatrix} = \operatorname{circ}(0,3,2,0,0).$$

We define $(c_1, c_2, c_3, c_4) = (3, 2, 0, 0)$, $a_1 = \min\{i | c_i \neq 0\}$ and

$$a_i = \min \left\{ \ell \;\middle|\; \sum_{j=1}^{\ell} j \cdot c_j > \sum_{j=1}^{i-1} a_j \right\}$$

for $i = 2, \ldots, 5$. Thus $(a_1, a_2, a_3, a_4, a_5) = (1, 1, 1, 2, 2)$.

Finally, considering the representer polynomial of A_a^x we have that

$$f'_{A_a^x}(1) \equiv (3+4X)|_{X=1} \equiv 2 \equiv \sum_{i=1}^{5} a_i \not\equiv 0 \pmod 5$$

and hence $X=1$ is a simple root of $f_{A_a^x}(X) \in \mathbb{Z}_5[X]$ as required.

We note that by considering x as a 5×5 array of the form

$$x = \begin{array}{c} (1,\ 6, 11, 16, 21) \\ (2,\ 9, 12, 19, 22) \\ (3,\ 7, 13, 17, 23) \\ (4, 10, 14, 20, 24) \\ (5,\ 8, 15, 18, 25) \end{array}, \tag{3.5}$$

the image of each entry in the first column of x under the action of a is in the same column, and one row below the original entry. Similarly, for columns $2, 3, 4$ and 5 the action of a corresponds to "descending" by $2, 1, 2$ and 1 rows respectively. Thus the image of 1 under $(ax)^5$ will be in the first column of x in (3.5), but will have descended $2 \equiv 1+2+1+2+1 \equiv \sum_{i=1}^{5} a_i \pmod 5$ rows.

4 An Equivalent Formulation

Our characterisation of $\langle a, x \rangle$ in terms of the matrices A_x and A_a^x given in Section 3 depended on the representer polynomial of a given circulant matrix. However, we may also consider the determinant of the circulant matrix. This characterisation relies on the following well known result regarding the determinant of a circulant matrix.

Theorem 4.1. *[14, Theorem 6] Let $C = \mathrm{circ}(c_0, c_1, \ldots, c_{n-1})$ be a circulant matrix with complex coefficients. Then*

$$\det(C) = \prod_{j=0}^{n-1} \left(\sum_{l=0}^{n-1} c_l \omega^{jl} \right),$$

where $\omega = \exp(2\pi i/n)$.

We now describe this approach using determinants.

Proposition 4.2. *Let $p \geq 3$ be a prime and let $c_1, \ldots, c_{p-1}$ be non-negative integers such that $\sum_{i=1}^{p-1} c_i = p$. Let $C = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$, and let $f_C(X) = \sum_{i=1}^{p-1} c_i X^i \in \mathbb{Z}_p[X]$ be the representer polynomial of C. Then $|\det(C)|_p$ is divisible by p^2 and $|\det(C)|_p$ is divisible by p^3 if and only if $f_C(X) = 0$ or 1 is a root of $f_C(X)$ of multiplicity at least 2.*

Before proceeding to prove Proposition 4.2, we first give three general results that we will require in the proof.

Lemma 4.3. *Let $p \geq 3$ be a prime and $\omega = \exp(2\pi i/p)$ be a primitive p^{th} root of unity. Then $\mathbb{Q} \cap \mathbb{Z}[\omega] = \mathbb{Z}$. In particular, $1/p^i \notin \mathbb{Z}[\omega]$ for $i \geq 1$.*

Proof. We note that $\mathcal{S} = \{1, \omega, \ldots, \omega^{p-2}\}$ is a basis for both $\mathbb{Q}[\omega]$ over $\mathbb{Q}$ and $\mathbb{Z}[\omega]$ over $\mathbb{Z}$. Suppose that $\alpha \in (\mathbb{Q} \cap \mathbb{Z}[\omega]) \setminus \mathbb{Z}$. Then α can be written as a $\mathbb{Z}$-linear combination of elements of $\mathcal{S}$, thus giving two distinct ways of writing α as a $\mathbb{Q}$-linear combination of elements of $\mathcal{S}$ in $\mathbb{Q}[\omega]$. This contradiction gives the result. □

Lemma 4.4. *Let $p \geq 3$ be a prime and let $\omega = \exp(2\pi i/p)$. Then*

(i) $\prod_{j=1}^{p-1}(1 - \omega^{2j}) = p$; *and*

(ii) $\prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j}) = p$.

Proof. Set $h(z) = z^p - 1 = \prod_{j=0}^{p-1}(z - \omega^{2j})$. Differentiating $h(z)$ with respect to z gives

$$pz^{p-1} = h'(z) = \prod_{j=1}^{p-1}(z - \omega^{2j}) + (z-1)\sum_{j=1}^{p-1}\prod_{\substack{i=1 \\ i\neq j}}^{p-1}(z - \omega^{2i}).$$

It follows that $p = h'(1) = \prod_{j=1}^{p-1}(1 - \omega^{2j})$ as required to prove (i).

Part (ii) then follows immediately since

$$\begin{aligned}\prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j}) &= \prod_{j=1}^{p-1}\omega^j(1 - \omega^{(p-2)j}) \\ &= \omega^{p(p-1)/2}\prod_{j=1}^{p-1}(1 - \omega^{(p-2)j}) \\ &= \prod_{j=1}^{p-1}(1 - \omega^{(p-2)j}) = \prod_{j=1}^{p-1}(1 - \omega^{2j}) = p.\end{aligned}$$

□

Lemma 4.5. *Let $p \geq 3$ be a prime. Then*

$$1 + \sum_{i=2}^{p-1}\prod_{j=2}^{i}(1 - j^{-1}) \equiv 0 \pmod{p}. \tag{4.1}$$

Proof. As the elements $(1 - j^{-1})$ for $j = 2, \ldots, p-1$ are the non-zero, non-identity elements of $\mathbb{Z}_p$, it follows that $\prod_{j=2}^{p-1}(1 - j^{-1}) \equiv p - 1 \pmod{p}$. Thus (4.1) is equivalent to proving that $\sum_{i=2}^{p-2}\prod_{j=2}^{i}(1 - j^{-1}) \equiv 0 \pmod{p}$. We will actually prove that

$$1 + \prod_{j=i+1}^{p-i}(1 - j^{-1}) \equiv 0 \pmod{p} \tag{4.2}$$

for all $i = 2, \ldots, (p-1)/2$. This is sufficient to prove the result, since

$$\begin{aligned}\prod_{j=2}^{i}(1 - j^{-1}) + \prod_{j=2}^{p-i}(1 - j^{-1}) &= \prod_{j=2}^{i}(1 - j^{-1})\left(1 + \prod_{j=i+1}^{p-i}(1 - j^{-1})\right) \\ &\equiv 0 \pmod{p},\end{aligned}$$

from which the result follows immediately.

We prove that (4.2) holds by induction on $\ell = (p+1)/2 - i$. When $\ell = 1$, then $i = (p-1)/2$ and so (4.2) becomes $1 + (1 - ((p+1)/2)^{-1}) \equiv 0 \pmod{p}$, which clearly holds since $((p+1)/2)^{-1} \equiv 2 \pmod{p}$. Assume that (4.2) holds for $\ell = (p+1)/2 - k < (p+1)/2$. It follows that

$$\begin{aligned}
1 + \prod_{j=k}^{p-k+1} (1 - j^{-1}) &\equiv 1 + (1 - k^{-1})(1 - (p-k+1)^{-1}) \prod_{j=k+1}^{p-k} (1 - j^{-1}) \\
&\equiv 1 - (1 - k^{-1})(1 - (p-k+1)^{-1}) \\
&\equiv k^{-1} + (p-k+1)^{-1} - k^{-1}(p-k+1)^{-1} \\
&\equiv k^{-1}(p-k+1)^{-1}(p-k+1+k-1) \\
&\equiv 0 \pmod{p}.
\end{aligned}$$

Thus by induction (4.2) holds for all $i = 2, \ldots, (p-1)/2$, as required to complete the proof. □

We are now in a position to prove Proposition 4.2.

Proof of Proposition 4.2: If $c_{p-1} = p$, then the result clearly holds since $\det(C) = p^p$ so is divisible by p^3, whilst $f_C(X) = 0 \in \mathbb{Z}_p[X]$. Thus we may assume that $c_{p-1} \neq p$.

Consider the general form of the determinant of C. As $c_1 + \cdots + c_{p-1} = p$, applying Theorem 4.1 to $C = \mathrm{circ}(0, c_1, \ldots, c_{p-1})$ we have that

$$\begin{aligned}
\det(C) = \prod_{j=0}^{p-1} \Big(& c_1\omega^j + c_2\omega^{2j} + \cdots + c_{p-2}\omega^{(p-2)j} \\
& + (p - c_1 - \cdots - c_{p-2})\omega^{(p-1)j} \Big) \\
= p \cdot \prod_{j=1}^{p-1} \Big(& c_1\omega^j + c_2\omega^{2j} + \cdots + c_{p-2}\omega^{(p-2)j} \\
& + (p - c_1 - \cdots - c_{p-2})\omega^{(p-1)j} \Big) \\
= p^3 \cdot \alpha(C) & \\
+ p^2 \cdot \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j \neq i}}^{p-1} \Big(& c_1\omega^j + \cdots + c_{p-2}\omega^{(p-2)j} \\
& - (c_1 + \cdots + c_{p-2})\omega^{(p-1)j} \Big) \\
+ p \cdot \prod_{j=1}^{p-1} \Big(& c_1\omega^j + \cdots + c_{p-2}\omega^{(p-2)j} - (c_1 + \cdots + c_{p-2})\omega^{(p-1)j} \Big) \\
= p^3 \cdot \alpha(C) + p^2 \cdot \beta(C) + p \cdot \gamma(C) & \qquad (4.3)
\end{aligned}$$

where $\omega = \exp(2\pi i/p)$,

$$\alpha(C) = \sum_{i=1}^{p-1} \sum_{\substack{k=1 \\ k\neq i}}^{p-1} \omega^{-i-k} \prod_{\substack{j=1 \\ j\neq i,k}}^{p-1} \Big(c_1\omega^j + \cdots + c_{p-2}\omega^{(p-2)j} + (p - c_1 - \cdots - c_{p-2})\omega^{(p-1)j} \Big),$$

$$\beta(C) = \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j\neq i}}^{p-1} \Big(c_1(\omega^j - \omega^{(p-1)j}) + \cdots + c_{p-2}(\omega^{(p-2)j} - \omega^{(p-1)j}) \Big)$$

and

$$\gamma(C) = \prod_{j=1}^{p-1} \Big(c_1(\omega^j - \omega^{(p-1)j}) + \cdots + c_{p-2}(\omega^{(p-2)j} - \omega^{(p-1)j}) \Big).$$

We now consider $\beta(C)$ and $\gamma(C)$ in turn.

Claim 1: $\beta(C) = p \cdot \beta'(C)$ for some $\beta'(C) \in \mathbb{Z}[\omega]$.
Proof of Claim 1: Consider the formulation of $\beta(C)$ as:

$$\begin{aligned}
\beta(C) &= \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j\neq i}}^{p-1} \Big(c_1(\omega^j - \omega^{(p-1)j}) + \cdots + c_{p-2}(\omega^{(p-2)j} - \omega^{(p-1)j}) \Big) \\
&= \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j\neq i}}^{p-1} (\omega^j - \omega^{(p-1)j}) \, (\, c_1 + c_2(1 + \omega^{2j} + \cdots + \omega^{(p-1)j} + \omega^j) \\
&\qquad + c_3(1 + \omega^{2j}) + c_4(1 + \omega^{2j} + \cdots + \omega^{(p-1)j} + \omega^j + \omega^{3j}) \\
&\qquad + c_5(1 + \omega^{2j} + \omega^{4j}) + \cdots\cdots + c_{p-2}(1 + \omega^{2j} + \cdots + \omega^{(p-3)j}) \,) \\
&= \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j\neq i}}^{p-1} (\omega^j - \omega^{(p-1)j}) \beta_j(C) \\
&= \sum_{i=1}^{p-1} \omega^{-i} \prod_{\substack{j=1 \\ j\neq i}}^{p-1} (\omega^j - \omega^{(p-1)j}) \prod_{\substack{j=1 \\ j\neq i}}^{p-1} \beta_j(C) \qquad (4.4)
\end{aligned}$$

We have the relation

$$\begin{aligned}
\omega^{p-j} - \omega^j &= (\omega^{p-j-1} - \omega^{j+1})(\omega + \omega^{2j+3} + \cdots + \omega^{2k(j+1)+1} + \cdots + \omega^{-1}) \\
&= (\omega^{p-j-1} - \omega^{j+1})\delta_j \qquad (4.5)
\end{aligned}$$

for $j = 1, \ldots, p-2$. Now $2k(j+1) + 1 \equiv -1 \pmod p$ precisely when $k \equiv -(j+1)^{-1} \pmod p$, and hence there are $1 - (j+1)^{-1} \pmod p$ terms forming the summation in δ_j.

Let $i \in \{1, \ldots, p-2\}$. By (4.5) we have that

$$\omega^{p-1} - \omega = \delta_1 \cdots \delta_{p-i-1}(\omega^i - \omega^{p-i}).$$

Thus (4.4) becomes

$$\beta(C) = \Gamma(C) \prod_{j=1}^{p-2} (\omega^j - \omega^{(p-1)j}) \tag{4.6}$$

where

$$\Gamma(C) := \omega \prod_{j=1}^{p-2} \beta_j(C) + \sum_{i=1}^{p-2} \omega^{-i} \delta_1 \cdots \delta_{p-i-1} \prod_{\substack{j=1 \\ j \neq i}}^{p-1} \beta_j(C).$$

Define $\Gamma(C)(X) \in \mathbb{Z}_p[X]$ to be the polynomial obtained by replacing every occurrence of ω in $\Gamma(C)$ by the indeterminant X. Similarly define $\beta_j(C)(X), \delta_j(X) \in \mathbb{Z}_p[X]$. Since $\beta_j(C)(1) = \beta_i(C)(1)$ for all $i, j = 1, \ldots, p-1$, we may denote this common value by ξ. Moreover, our observation above asserts that

$$\delta_j(1) \equiv 1 - (j+1)^{-1} \pmod{p}.$$

It follows that

$$\begin{aligned}
\Gamma(C)(1) &\equiv \xi^{p-2} + \sum_{i=1}^{p-2} (1 - 2^{-1}) \cdots (1 - (p-i)^{-1}) \xi^{p-2} \\
&\equiv \xi^{p-2} \left(1 + \sum_{i=1}^{p-2} \prod_{j=2}^{p-i} (1 - j^{-1}) \right) \\
&\equiv \xi^{p-2} \left(1 + \sum_{i=2}^{p-1} \prod_{j=2}^{i} (1 - j^{-1}) \right) \\
&\equiv 0 \pmod{p}
\end{aligned}$$

where the last equivalence arises from Lemma 4.5. Consequently, $(X-1)$ is a factor of $\Gamma(C)(X) \in \mathbb{Z}_p[X]$ and hence evaluating $\Gamma(C)(X)$ at $X = \omega$ yields

$$\Gamma(C) = (\omega - 1) F(\omega) + p G(\omega)$$

for some $F(\omega), G(\omega) \in \mathbb{Z}[\omega]$. Substituting into (4.6) gives

$$\beta(C) = \left(\prod_{j=1}^{p-2} (\omega^j - \omega^{(p-1)j}) \right) \left((\omega - 1) F(\omega) + p G(\omega) \right).$$

Finally, as

$$\omega - 1 = (\omega^{p-1} - \omega)(\omega^2 + \omega^4 + \cdots + \omega^{p-1})$$

we may appeal to Lemma 4.4(ii) to get

$$\begin{aligned}\beta(C) &= \left(\prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j})\right)(\omega^2+\omega^4+\cdots+\omega^{p-1})F(\omega) \\ &\quad + p\left(\prod_{j=1}^{p-2}(\omega^j - \omega^{(p-1)j})\right)G(\omega) \\ &= p(\omega^2+\omega^4+\cdots+\omega^{p-1})F(\omega) + p\left(\prod_{j=1}^{p-2}(\omega^j - \omega^{(p-1)j})\right)G(\omega) \\ &= p\beta'(C)\end{aligned}$$

as required. •

Now we consider $\gamma(C)$.

Claim 2: $\gamma(C) = p \cdot \gamma'(C)$ for some $\gamma'(C) \in \mathbb{Z}$.
Proof of Claim 2: We may factorise $\gamma(C)$ as

$$\begin{aligned}\gamma(C) &= \prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j})\,(\,c_1 + c_2(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j) + c_3(1+\omega^{2j}) \\ &\quad + c_4(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j+\omega^{3j}) + c_5(1+\omega^{2j}+\omega^{4j}) + \cdots \\ &\quad \cdots + c_{p-2}(1+\omega^{2j}+\cdots+\omega^{(p-3)j})\,) \\ &= \prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j})\gamma_j(C) \\ &= \prod_{j=1}^{p-1}(\omega^j - \omega^{(p-1)j}) \prod_{j=1}^{p-1}\gamma_j(C) \\ &= p \cdot \prod_{j=1}^{p-1}\gamma_j(C) \qquad (4.7)\end{aligned}$$

where

$$\begin{aligned}\gamma_j(C) = (\,&c_1 + c_2(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j) + c_3(1+\omega^{2j}) \\ &+ c_4(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j+\omega^{3j}) + c_5(1+\omega^{2j}+\omega^{4j}) + \cdots \\ &\cdots + c_{p-2}(1+\omega^{2j}+\cdots+\omega^{(p-3)j})\,)\end{aligned}$$

and the last equality in (4.7) follows from Lemma 4.4(ii). If we consider $\prod_{j=1}^{p-1}\gamma_j(C)$, then by taking s_i to be the coefficient of ω^{ij} in $\gamma_j(C)$ we see that the s_i are non-negative integers and $s_0 = c_1 + \cdots + c_{p-2} = p - c_{p-1}$ is non-zero. Defining $S = \mathrm{circ}(s_0, s_1, \ldots, s_{p-1})$, we see that $\det(S) \in \mathbb{Z}$ and so

$$\prod_{j=1}^{p-1}\gamma_j(C) = \frac{1}{s_0+s_1+\cdots+s_{p-1}}\det(S) \in \mathbb{Q} \cap \mathbb{Z}[\omega].$$

Appealing to Lemma 4.3, we conclude that $\prod_{j=1}^{p-1}\gamma_j(C) \in \mathbb{Z}$ as required to prove Claim 2. •

It follows from (4.3) that

$$\det(C) = p^2\left(p\alpha(C) + p\beta'(C) + \gamma'(C)\right).$$

Since $p\alpha(C) + p\beta'(C) + \gamma'(C) = \det(C)/p^2 \in \mathbb{Q} \cap \mathbb{Z}[\omega] = \mathbb{Z}$, we conclude that $\det(C)$ is divisible by p^2. To complete the proof of the proposition, we make one final claim:

Claim 3: $\gamma'(C) = p \cdot \gamma''(C)$ for some $\gamma''(C) \in \mathbb{Z}[\omega]$ if and only if $X = 1$ is a root of $f_C(X) \in \mathbb{Z}_p[X]$ of multiplicity at least 2.
Proof of Claim 3: First note that $X = 1$ is a root of $f_C(X)$ of multiplicity at least 2 if and only if $X = 1$ is a root of the derivative $f'_C(X)$ of $f_C(X)$. This occurs precisely when $\sum_{i=1}^{p-1} i \cdot c_i \equiv 0 \pmod{p}$. Moreover

$$\begin{aligned}\sum_{i=1}^{p-1} i \cdot c_i &= \sum_{i=1}^{p-2} i \cdot c_i + (p-1)\left(p - \sum_{i=1}^{p-2} c_i\right)\\ &\equiv \sum_{i=1}^{p-2}(i+1)\cdot c_i \pmod{p}\\ &\equiv \sum_{i=1}^{(p-3)/2}\left(2i \cdot c_{2i-1} + (2i+1)\cdot c_{2i}\right) + (p-1)\cdot c_{p-2} \pmod{p}\end{aligned}$$

Thus it suffices to prove that $\gamma'(C)$ has the desired factorisation precisely when

$$\sum_{i=1}^{(p-3)/2}\left(2i \cdot c_{2i-1} + (2i+1)\cdot c_{2i}\right) + (p-1)\cdot c_{p-2} \equiv 0 \pmod{p}.$$

In fact we will prove that

$$\gamma'(C) \equiv \left(\sum_{i=1}^{(p-3)/2}\left(i \cdot c_{2i-1} + \left(i + \frac{p+1}{2}\right)c_{2i}\right) + \frac{p-1}{2}\cdot c_{p-2}\right)^{p-1} \pmod{p} \tag{4.8}$$

We note that

$$\begin{aligned}\gamma'(C) = \prod_{j=1}^{p-1} \big(& c_1 + c_2(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j) + c_3(1+\omega^{2j}) \\ & + c_4(1+\omega^{2j}+\cdots+\omega^{(p-1)j}+\omega^j+\omega^{3j}) \\ & + c_5(1+\omega^{2j}+\omega^{4j})+\cdots+c_{p-2}(1+\omega^{2j}+\cdots+\omega^{(p-3)j})\big) \\ = \prod_{j=1}^{p-1} \big(& (c_1+c_3+\cdots+c_{p-2}+c_2+\cdots+c_{p-3}) \\ & + (c_3+\cdots+c_{p-2}+c_2+\cdots+c_{p-3})\omega^{2j} \\ & + (c_5+\cdots+c_{p-2}+c_2+\cdots+c_{p-3})\omega^{4j} \\ & + \cdots + (c_2+\cdots+c_{p-3})\omega^{(p-1)j} + (c_2+\cdots+c_{p-3})\omega^j \\ & + (c_4+\cdots+c_{p-3})\omega^{3j}+\cdots+c_{p-3}\omega^{(p-4)j}\Big).\end{aligned} \tag{4.9}$$

Now let C' be the circulant matrix $C' = \mathrm{circ}(c'_0,\ldots,c'_{p-1})$ where c'_i is the coefficient of ω^{ij} in the j^{th} factor of (4.9). Then

$$\begin{aligned}\det(C') &= \left(\left(\sum_{i=1}^{(p-3)/2} i\cdot c_{2i-1} + \left(i+\frac{p+1}{2}\right)c_{2i}\right) + \frac{p-1}{2}\cdot c_{p-2}\right)\gamma'(C) \\ &= \lambda\cdot\gamma'(C).\end{aligned} \tag{4.10}$$

There are now two possible cases to consider. First suppose that λ is divisible by p. Then an analogous argument to that used for the matrix C can be used to show that $\det(C')$ is divisible by p^2 (as the coefficient of $\omega^{(p-2)j}$ is zero, and so the matrix is of the required form). Since $\lambda < p^2$, it follows from (4.10) that $\gamma'(C)$ is divisible by p, and hence Claim 3 holds.

Now suppose that λ is not divisible by p. Then (4.8) becomes $\gamma'(C) \equiv 1 \pmod p$ by Fermat's little theorem. Combining (4.10) and Lemma 2.2 we have that $\lambda \equiv \det(C') \equiv \lambda\cdot\gamma'(C) \pmod p$, and hence as $\lambda \not\equiv 0 \pmod p$ it follows that $\gamma'(C) \equiv 1 \pmod p$ as required. This completes the proof of Claim 3. •

To complete the proof of Proposition 4.2 we note that by substituting the results of Claims 1 and 2 into (4.3) we obtain

$$\det(C) = p^3(\alpha(C)+\beta'(C)) + p^2\gamma'(C).$$

If $X=1$ is a root of $f_C(X) \in \mathbb{Z}_p[X]$ of multiplicity at least 2, then by Claim 3 we obtain $\det(C) = p^3(\alpha(C)+\beta'(C)+\gamma''(C))$, and hence appealing to Lemma 4.3 we obtain $|\det(C)|_p \geq p^3$ as required. Conversely, if $X=1$ is not a root of multiplicity at least 2 of $f_C(X)$, then Claim 3 asserts that there is no $\gamma''(C) \in \mathbb{Z}[\omega]$ such that $\gamma'(C) = p\cdot\gamma''(C)$. Thus $\det(C) = p^3(\alpha(C)+\beta'(C)) + p^2\gamma'(C)$ and as $\gamma'(C) \in \mathbb{Z}$, appealing to Lemma 4.3 we obtain that $\det(C) = p^3m + p^2n$ where p and n are coprime. Thus $|\det(C)|_p = p^2$. □

Theorem 1.1 now follows immediately from Propositions 3.2 and 4.2.

5 The $n = p^3$ Case

To consider the case that $G = \mathrm{Sym}(p^3)$, we follow a similar approach to that used in Section 3. We first develop the theoretical results in Subsections 5.1 and 5.2, before giving a worked example for the case that $p = 3$ in Subsection 5.3.

5.1 General Theory

In Section 4 we saw that the multiplicity of $X = 1$ as a root of the representer polynomial of given circulant matrices was important. We begin by noting that the multiplicity is preserved under cyclic shifts of our circulant matrix.

Lemma 5.1. *Let p be a prime and $C := \mathrm{circ}(c_0, c_1, \ldots, c_{p-1})$ be an integer circulant matrix. If $X = 1$ is a root of multiplicity i of $f_C(X) \in \mathbb{Z}_p[X]$, then it is a root of multiplicity i of $f_{\pi^j C}(X) \in \mathbb{Z}_p[X]$ for each $j = 0, \ldots, p-1$.*

Proof. Define $C_j = \pi^{-j} C$ for each $j = 0, \ldots, p-1$. We shall prove that $X = 1$ is a root of multiplicity i of the representer polynomial of each C_j. By assumption the result holds for $j = 0$ and hence assume it holds for $j = k$. We will prove the result holds for C_{k-1}. Indeed

$$\begin{aligned} f_{C_k}(X) &= c_k + c_{k+1}X + \cdots + c_{p-1}X^{p-k-1} + c_0 X^{p-k} + \cdots + c_{k-1}X^{p-1} \\ &= (X-1)^i g(X) \end{aligned}$$

for some $g(X) \in \mathbb{Z}_p[X]$ with $g(1) \not\equiv 0 \pmod{p}$. Thus

$$\begin{aligned} f_{C_{k-1}}(X) &= c_{k-1} + c_k X + \cdots + c_{p-1}X^{p-k} + c_0 X^{p+1-k} + \cdots + c_{k-2}X^{p-1} \\ &= f_{C_k}(X) \cdot X + c_{k-1}(1 - X^p) \\ &= (X-1)^i g(X) \cdot X + c_{k-1}(1-X)^p. \end{aligned}$$

Hence $X = 1$ is a root of multiplicity i of $f_{C_{k-1}}(X)$, and thus by induction of $f_{C_j}(X)$ for each $j = 0, \ldots, p-1$. □

We may use Lemma 5.1 to consider quotients of W_p.

Lemma 5.2. *Let N be a non-trivial normal subgroup of W_p admitting a quotient group Q. Then $\exp(Q) \leq p$.*

Proof. Denote the base group of W_p by Γ, so that $W_p = \Gamma \rtimes C$ where $C = \langle x \rangle$ - a cyclic group of order p. Assume that $\exp(Q) = p^2$, and let $q \in Q$ satisfy $\mathrm{ord}(q) = p^2$. We consider elements of W_p to be ordered pairs of the form (γ, c) for $\gamma \in \Gamma$ and $c \in C$. Thus there exists $\gamma \in \Gamma$ such that $q = (\gamma, x^i)N$ for some $i = 1, \ldots, p-1$. Thus

$$q^p = (\gamma\gamma^{x^{-i}}\gamma^{x^{-2i}} \cdots \gamma^{x^{(1-p)i}}, 1)N = (\gamma\gamma^x\gamma^{x^2} \cdots \gamma^{x^{p-1}}, 1)N \tag{5.1}$$

Moreover, $\gamma\gamma^x\gamma^{x^2} \cdots \gamma^{x^{p-1}} \notin N$ as $\mathrm{ord}(q) = p^2$.

If $N \not\subseteq \Gamma$, then there exists $\gamma_0 \in \Gamma$ such that $(\gamma_0, x^{-i}) \in N$. Consequently

$$q = (\gamma, x^i)(\gamma_0, x^{-i})N = (\gamma\gamma_0^{x^{-i}}, 1)N$$

contradicting the fact that q has order p^2. Thus $N \subseteq \Gamma$.

If $\Gamma = \langle\alpha_1\rangle \times \langle\alpha_2\rangle \times \cdots \times \langle\alpha_p\rangle$ where $\alpha_i^x = \alpha_{i-1}$ for $i = 2, \ldots, p$ and $\alpha_1^x = \alpha_p$, then from (5.1) we may deduce that

$$1 \neq \gamma\gamma^x\gamma^{x^2}\cdots\gamma^{x^{p-1}} = (\alpha_1\alpha_2\cdots\alpha_p)^j \tag{5.2}$$

for some $j = 1, \ldots, p-1$. Moreover, for any $\delta \in \Gamma$ we have that

$$\delta\delta^x\delta^{x^2}\cdots\delta^{x^{p-1}} \in \langle\alpha_1\alpha_2\cdots\alpha_p\rangle.$$

If there exists $\delta \in N$ such that $\delta\delta^x\delta^{x^2}\cdots\delta^{x^{p-1}} \neq 1$, then q^p is trivial in Q. Thus every $\delta \in N$ must satisfy $\delta\delta^x\delta^{x^2}\cdots\delta^{x^{p-1}} = 1$. Consequently, every $\delta \in N$ has the form

$$\delta = \alpha_1^{c_1}\alpha_2^{c_2}\cdots\alpha_p^{c_p} \tag{5.3}$$

with $c_1 + \cdots + c_p \equiv 0 \pmod{p}$.

Let $\delta \in N\backslash\{1\}$. Thus δ has the form (5.3). Set $C = \mathrm{circ}(c_1, c_2, \ldots, c_p)$ and let $f_C(X) \in \mathbb{Z}_p[X]$ be the corresponding representer polynomial. As $c_1+\cdots+c_p \equiv 0 \pmod{p}$ we have that $X = 1$ is a root of $f_C(X)$. Assume that this root has multiplicity i. Thus $X = 1$ is a root of $f_C^{i-1}(X)$ but is not a root of $f_C^i(X)$. Hence set

$$\lambda := f_C^i(1) = c_{i+1}\cdot\frac{i!}{0!} + c_{i+2}\cdot\frac{(i+1)!}{1!} + \cdots + c_p\cdot\frac{(p-1)!}{(p-1-i)!} \in \mathbb{Z}_p^*.$$

Define d_j for $j = 1, \ldots, p$ by

$$d_{j+1} := \begin{cases} j!/(j-i)! & \text{if } j = i, \ldots, p-1; \text{ and} \\ 0 & \text{otherwise,} \end{cases}$$

so that $\lambda = \sum_{j=1}^p c_j d_j$.

Defining $C_j = \pi^{1-j}C$ for $j = 1, \ldots, p$ we have that $f_{C_1}^i(1) = \lambda$. In fact $f_{C_k}^i(1) = \lambda$ for all $k = 1, \ldots p$. Indeed, by Lemma 5.1 we have that $f_{C_k}^{i-1}(1) = 0$ for each k. Moreover by iterating the calculations in the proof of the lemma we obtain

$$f_{C_k}(X) = f_{C_1}(X)\cdot X^{p-k+1} + (X-1)^p g_k(X)$$

for some $g_k(X) \in \mathbb{Z}_p[X]$. Consequently, $f_{C_k}^i(1) = f_{C_1}^i(1) = \lambda$. We conclude that

$$\begin{pmatrix} c_1 & c_2 & \cdots & c_{p-1} & c_p \\ c_p & c_1 & \cdots & c_{p-2} & c_{p-1} \\ \vdots & \vdots & & \vdots & \vdots \\ c_3 & c_4 & \cdots & c_1 & c_2 \\ c_2 & c_3 & \cdots & c_p & c_1 \end{pmatrix} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{p-1} \\ d_p \end{pmatrix} = \begin{pmatrix} \lambda \\ \lambda \\ \cdots \\ \lambda \\ \lambda \end{pmatrix}.$$

As δ has the form given in (5.3) we see that

$$(\alpha_1\alpha_2\cdots\alpha_p)^\lambda = \prod_{i=1}^p (\delta^{x^{i-1}})^{d_i} \in N.$$

Thus by (5.1) and (5.2), $q^p = N$, contradicting the fact that $\mathrm{ord}(q) = p^2$. Thus the result holds. □

A presentation of W_p was given by Drozd and Skuratovskii.

Theorem 5.3. *[12] The wreath product $C_p \wr C_p$ has a presentation given by*

$$C_p \wr C_p = \langle a, x \,\Big|\, a^p = 1, x^p = 1, [a, a^{x^k}] = 1 \text{ for } 1 \leq k \leq (p-1)/2 \rangle.$$

Combining Corollary 2.4, Lemma 5.2 and Theorem 5.3 we obtain the following result.

Corollary 5.4. *Let G be a group and let $a, x \in G$ be elements of order p. Then $\langle a, x \rangle \cong W_p$ if and only if $\text{ord}(ax) = p^2$ and either*

(i) $[a, a^{x^i}] = 1$ *for* $i = 1, \ldots, (p-1)/2$*; or*

(ii) $[x, x^{a^i}] = 1$ *for* $i = 1, \ldots, (p-1)/2$.

Proof. Assume that $\langle a, x \rangle \cong W_p$. By Corollary 2.4 the desired commutator relations hold. Without loss assume that $[a, a^{x^i}] = 1$ for $i = 1, \ldots, (p-1)/2$. Thus a is in the base group of W_p. Moreover, the base group is defined by $\langle a^{x^i} \mid i = 0, \ldots, p-1 \rangle$ and hence $(ax)^p = a \cdot a^{x^{p-1}} \cdots a^x \neq 1$. Thus $\text{ord}(ax) = p^2$.

Conversely, assume that the commutator relations hold. By Theorem 5.3 we have that $\langle a, x \rangle$ is isomorphic to a quotient of W_p. However, as $\text{ord}(ax) = p^2$ this quotient must be W_p by Lemma 5.2. □

To generalise the results of Sections 3 and 4 we begin by considering conjugate elements of full support in $\text{Sym}(p^3)$. Indeed, let $G := \text{Sym}(p^3)$, $a \in G$ be the standard p-element of G, $X = a^G$ and let $x \in X$. In such a situation the matrices A_x and A_a^x are both $p^2 \times p^2$ matrices. We make the following definition.

Definition 5.5. *Let $r > 1$ be an integer and let M be a $pr \times pr$ matrix. The* block sum matrix *of M, denoted $BS(M)$, is the $p \times p$ matrix given by*

$$(BS(M))_{i,j} := \sum_{v,w=0}^{r-1} M_{i+pv, j+pw}.$$

Given a $pr \times pr$ matrix M, we see that $BS(M)$ is the matrix obtained by partitioning M into $p \times p$ blocks and then forming the formal sum of these blocks. Of particular interest is the case when M can be partitioned into circulant blocks. In this case we see that $BS(M)$ is a circulant matrix.

We shall also consider a variant on the representer polynomial.

Definition 5.6. *Let M be a $pr \times pr$ matrix having $p \times p$ circulant blocks. We define the* reduced representer polynomial *of M to be the polynomial*

$$g_M(X) := g_0 + g_1 X + \cdots + g_{r-1} X^{r-1}$$

where

$$g_i := \sum_{j=0}^{r-1} \sum_{k=1}^{p} M_{jp+1, (j+i)p+k}$$

and $M_{jp+1,(j+i)p+k}$ is replaced by $M_{jp+1,(j+i-r)p+k}$ if $j + i \geq r$.

The reduced representer polynomial of the matrix M in some senses represents the matrix formed by replacing each $p \times p$ circulant block of M by its row/column sum.

5.2 The Results

Before giving a characterisation of which elements of X generate W_p with a, we make the following simple observation. If $\langle a^{x^i} \mid i = 0, \ldots, p-1\rangle$ is an abelian group that is closed under conjugation by x, then

$$(ax)^p = a \cdot a^{x^{p-1}} \cdot a^{x^{p-2}} \cdots a^x.$$

In particular $(ax)^p$ is invariant under conjugation by both a and x and hence by $\langle a, x\rangle$.

We are now in a position to prove Theorem 1.2.

Proof of Theorem 1.2: Assume that $\langle a, x\rangle \cong W_p$ and denote the base group of W_p by Γ. By Corollary 2.4 we either have $\Gamma = \langle a^{x^i} | i = 0, \ldots, p-1\rangle$ or $\Gamma = \langle x^{a^i} | i = 0, \ldots, p-1\rangle$. Without loss of generality assume the former case holds. We will prove that the given conditions hold (an analogous argument may be used to show that in the latter case the conditions hold with the roles of a and x interchanged). By assumption the commutator relations hold and thus it remains to prove the conditions on A_x and A_a^x.

For distinct $i, j \in \{1, \ldots, p^2\}$ such that $\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_j) \neq \emptyset$, we have that $|\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_j)| = 1$ or p. In the latter case the commutator relations assert that $\alpha_i^x \in \langle \alpha_j\rangle$ and this contributes an entry of p in the (i, j) position of A_x and zeros in all other entries of the i^{th} row and j^{th} column. In the former case, we see that there must be distinct $j_1 = j, j_2, \ldots, j_p \in \{1, \ldots, p^2\}$ such that $|\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_{j_\ell})| = 1$ for all $\ell = 1, \ldots, p$. However, the commutator relations then infer that there exist distinct $i_1 = i, i_2, \ldots, i_p \in \{1, \ldots, p^2\}$ such that $\left|\mathrm{supp}(\alpha_{i_k}^x) \cap \mathrm{supp}(\alpha_{j_\ell})\right| = 1$ for all $k, \ell \in \{1, \ldots, p\}$.

If every entry of A_x is equal to 0 or p, then we may decompose $a = a_1 \cdots a_p$ and $x = x_1 \cdots x_p$ with each pair (a_i, x_i) sitting inside a copy of $\mathrm{Sym}(p^2)$. Our assumptions on a and x together with the commutator relations assert that $\langle a_i, x_i\rangle$ is isomorphic to a proper quotient of W_p for each $i = 1, \ldots, p$, and hence the same is true of $\langle a, x\rangle$. We conclude that there is a block of A_x in which every entry is equal to one and up to a suitable renumbering of the α_i, the matrix A_x has the required form.

Since A_x has the given form, it follows that $|\mathrm{supp}(\alpha_i) \cap \mathrm{supp}(\chi_j)| = 0$ or 1 for all $i, j \in \{1, \ldots, p^2\}$. Thus we see that $w \in \mathrm{supp}(\chi_w)$ for $w \in \{1, \ldots, p^2\}$. Setting $q := p^2 - p$, we consider x as

$$x = \begin{array}{ccc} \left(1, 1\cdot\chi_1, \ldots, 1\cdot\chi_1^{p-1}\right) & \cdots & \left(q+1, (q+1)\cdot\chi_{q+1}, \ldots, (q+1)\cdot\chi_{q+1}^{p-1}\right) \\ \left(2, 2\cdot\chi_2, \ldots, 2\cdot\chi_2^{p-1}\right) & \cdots & \left(q+2, (q+2)\cdot\chi_{q+2}, \ldots, (q+2)\cdot\chi_{q+2}^{p-1}\right) \\ \vdots & & \vdots \\ \left(p, p\cdot\chi_p, \ldots, p\cdot\chi_p^{p-1}\right) & \cdots & \left(p^2, (p^2)\cdot\chi_{p^2}, \ldots, (p^2)\cdot\chi_{p^2}^{p-1}\right). \end{array} \tag{5.4}$$

In the subsequent work, we shall refer to the columns of x according to (5.4). By this, we mean that the first column of x is equal to $\{1, 2, \ldots, p\}$, the second column is equal to $\{1\cdot\chi_1, 2\cdot\chi_2, \ldots, p\cdot\chi_p\}$ and so on. We will also refer to the permutation σ_i corresponding to column i. This will be the permutation

defined on column i by a cyclic permuting of the entries. Thus $\sigma_1 = (1, 2, \ldots, p)$, $\sigma_2 = (1 \cdot \chi_1, 2 \cdot \chi_2, \ldots, p \cdot \chi_p)$, and so on.

We consider the structure of A_a^x via the structure of A_x. First suppose that $\mathrm{supp}(\alpha_i^{x^\ell}) = \mathrm{supp}(\alpha_j)$ for some $i = 1, \ldots, p$, $j = 1, \ldots, p^2$ and $\ell = 1, \ldots, p$. As noted above it follows that $\alpha_i^{x^\ell} \in \langle \alpha_j \rangle$, and hence the column of x in (5.4) corresponding to $\alpha_i^{x^\ell}$ will contribute a power of π, say π^r, to one diagonal block of A_a^x. Indeed, this is the only way that a diagonal block of A_a^x can be constructed. Moreover, as there is at least one block of A_x consisting of constant 1s, there exits some $q \in \{1, \ldots, p\}$ such that none of the q^{th}, $(q+p)^{\text{th}}$, $\ldots, (q + (p^2 - p))^{\text{th}}$ columns of x are equal to the support of some α_j. For each such set of columns, the commutator relations then ensure that the combination of the columns add circulant blocks to the matrix A_a^x corresponding to the way that these columns are mapped onto one another by a. It follows that the matrix A_a^x is a block matrix with $p \times p$ circulant blocks. Finally, as there exists at least one set of p columns as defined above, we may use these together with the commutator relations to see that the diagonal blocks of A_a^x must be equal.

It remains to prove that the block sum matrix or the reduced representer polynomial of A_a^x has the desired form. To do this we consider $y := (ax)^p$. The commutator relations ensure that the columns of x in (5.4) are permuted under the action of a and hence the i^{th} column of x in (5.4) is mapped to the $(pr + i)^{\text{th}}$ column of x under y for some value of r. First assume that each column of x is invariant under y. It follows from the commutator relations that $y = \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_{p^2}^{i_{p^2}}$ for some $i_1, \ldots, i_{p^2} \in \{0, \ldots, p-1\}$. However, as y is invariant under conjugation by $\langle a, x \rangle$ we may conclude that the i_j are all equal.

We now construct polynomials $f_j(X) \in \mathbb{Z}_p[X]$ for $j = 1, \ldots, p$ recursively. To do this initially set $f_j(X) = 0$ - the zero polynomial. Now consider $((j-1)p+1) \cdot ax$. Redefine $f_j(X)$ to be $f_j(X) := f_j(X) + X^r$ where r is the number of rows descended in (5.4) to go from the entry $((j-1)p+1)$ to the entry $((j-1)p+1) \cdot ax$. Repeat this with $((j-1)p+1)$ replaced by $((j-1)p+1) \cdot (ax)^k$ for $k = 1, \ldots, p-1$. Thus $f_j(X)$ encodes the circulant nature of the action of a on x in the columns of (5.4) corresponding to the orbit of the $((j-1)p+1)^{\text{th}}$ column under the action of $\langle ax \rangle$. We see that the contribution of these columns to $BS(A_a^x)$ is precisely the $p \times p$ circulant matrix for which $f_j(X)$ is the representer polynomial. Moreover, a similar analysis to that used in Section 3 shows that $X = 1$ is a simple root of $f_j(X) \in \mathbb{Z}_p[X]$ precisely when $i_{(j-1)p+1} \not\equiv 0 \pmod{p}$ since

$$f_j'(1) \equiv \begin{cases} 0 & \text{if } i_{(j-1)p+1} \equiv 0 \pmod{p}; \\ i_{(j-1)p+1}^{-1} & \text{otherwise.} \end{cases} \tag{5.5}$$

Considering the representer polynomial of the block sum matrix $BS(A_a^x)$ we see that

$$f_{BS(A_a^x)}(X) = \sum_{j=1}^{p} f_j(X).$$

Since the i_j are all equal, we see that $f'_{BS(A_a^x)}(1) \equiv 0 \pmod{p}$ and $X = 1$ is a root of multiplicity at least two of the representer polynomial of $BS(A_a^x)$.

To obtain the final conclusion we note that as the i_j are all equal, we have that $f_1'(1) = f_2'(1) = \cdots = f_p'(1)$. Combining this with (5.5) we see that $y = 1$

precisely when $f_i'(1) = pk$ for some $k \in \mathbb{N} \setminus \{0\}$ and for all $i = 1, \ldots, p$. This occurs precisely when

$$f'_{BS(A_a^x)}(1) = \sum_{j=1}^{p} f_j'(1) = kp^2.$$

Thus $X = 1$ is a root of $f'_{BS(A_a^x)}(X) \in \mathbb{Z}_{p^2}[X]$ precisely when $y = 1$. Hence as $\langle a, x \rangle \cong W_p$ we conclude that $X = 1$ is not a root of $f'_{BS(A_a^x)}(X) \in \mathbb{Z}_{p^2}[X]$. Hence if the columns of x in (5.4) are invariant under the action of y, then case $(c1)$ holds.

Now assume that the columns of x are not fixed by y. We shall prove that case $(c2)$ must be true. Define block j of x to be the set of columns $jp+1, \ldots, jp+p$ of x in (5.4) for $j = 0, \ldots, p-1$ and consider the matrix A_a^x. Each entry of A_a^x corresponds to the image of a column of x under a. There are two possibilities; either the column i is left invariant under the action of a, or it is mapped onto the column $pr + i$ for some $1 \leq r \leq p-1$. This corresponds to the column being mapped from block j to block $j + r \pmod p$. The former case occurs precisely when a power of π is added to a diagonal block of A_a^x, whilst in the latter case, a power of π is added to an off diagonal block of A_a^x which is r blocks to the right of the leading diagonal. We see that the partial representer polynomial $g_{A_a^x}(X)$ of A_a^x is of the form

$$g_{A_a^x}(X) = g_0 + g_1 X^1 + \cdots + g_{p-1} X^{p-1},$$

where for each $r = 0, \ldots, p-1$ the coefficient g_r is the number of columns i of x in (5.4) that are mapped to the column $i + pr$. Equivalently,

$$g_r = \sum_{j=0}^{p-1} \left| \left\{ i \;\middle|\; \begin{array}{c} \text{column } i \text{ is in block } j \text{ and is mapped to a column in} \\ \text{block } j + r \pmod p \text{ under the action of } a \end{array} \right\} \right|$$

Consider the action of y on the column i of x. This corresponds to applying ax to the column p times. It follows that the action of y is determined by the p successive actions of a. Since each column of x has an orbit of size p^2 under the action of ax, we see that each of the actions of a on the columns of x occurs p times in the action of y on the columns of x. Thus to obtain the number of blocks that column i has passed through in reaching its image under the action of y, we need to sum the number of blocks passed through for each successive action of a. It follows that the total number of blocks passed through by all columns of x under the action of y is

$$p \cdot \sum_{r=0}^{p-1} r \cdot g_r = p \cdot g'_{A_a^x}(1). \tag{5.6}$$

Since y is invariant under the action of x, we see that if column i in block j is mapped to column $i + pr$ in block $j + r \pmod p$ under the action of y, then every column of block j will be mapped to the corresponding column in block $j + r \pmod p$ under the action of y. Hence y simply permutes the blocks of x.

Suppose that block j of x passes through $p \cdot k_j + \ell_j$ blocks under the action of y for some $k_j, \ell_j \in \{0, \ldots, p-1\}$. Since y is invariant under the action of a,

we deduce that the k_j are all equal to some common value say k. It follows that the total number of blocks passed through by all columns of x under the action of y is

$$\sum_{j=0}^{p-1} p \cdot (p \cdot k + \ell_j) = p \left(p^2 k + \sum_{j=0}^{p-1} \ell_j \right). \tag{5.7}$$

Combining (5.6) and (5.7) we obtain

$$g'_{A_a^x}(1) \equiv \sum_{j=0}^{p-1} \ell_j \pmod{p^2}.$$

Finally, we note that $\sum_{j=0}^{p-1} \ell_j \equiv 0 \pmod{p^2}$ precisely when $\ell_j = 0$ for each $j = 0, \ldots, p-1$. Hence $g'_{A_a^x}(1) \equiv 0 \pmod{p^2}$ precisely when the columns of x in (5.4) are fixed by y. Since by assumption the columns of x are permuted by y, we conclude that case $(c2)$ holds.

Conversely assume that the given conditions hold (again the argument for when a and x are interchanged is analogous). By the above we see that $(ax)^p \neq 1$. Combining this with the commutator relations and Corollary 5.4 we obtain that $\langle a, x \rangle \cong W_p$, as required. □

As in Section 3 we note that the conditions given in Theorem 1.2 are all required. As before this is evident in the proof of the theorem for the conditions on the matrices A_x and A_a^x. To see that the commutator relations are all necessary, we note that if $G := \mathrm{Sym}(125)$ and a is the standard 5-element of G, then we may take

$$\begin{aligned} x = &(1,26,51,76,101)(2,27,56,79,106)(3,28,61,77,111)(4,29,66,80,116) \\ &(5,30,71,78,121)(6,41,54,91,117)(7,42,59,94,122)(8,43,64,92,102) \\ &(9,44,69,95,107)(10,45,74,93,112)(11,49,72,83,110)(12,50,52,81,115) \\ &(13,46,57,84,120)(14,47,62,82,125)(15,48,67,85,105)(16,36,68,90,118) \\ &(17,37,73,88,123)(18,38,53,86,103)(19,39,58,89,108)(20,40,63,87,113) \\ &(21,32,70,100,119)(22,33,75,98,124)(23,34,55,96,104)(24,35,60,99,109) \\ &(25,31,65,97,114). \end{aligned}$$

The reader may check that A_x and A_a^x have the required form and $[a, a^x] = 1$. However, $[a, a^{x^2}] \neq 1$.

5.3 A Worked Example

As in Section 3 we follow the technical steps of the proof of Theorem 1.2 in the case of a couple of specific examples. Indeed consider $G := \mathrm{Sym}(27)$ and the following G-conjugates of the standard 3-element a of G,

$$x_1 = \begin{array}{l} (1,10,20)(4,14,22)(7,18,27) \\ (2,13,23)(5,17,25)(8,12,21) \\ (3,16,26)(6,11,19)(9,15,24) \end{array} \tag{5.8}$$

and

$$x_2 = \begin{array}{c}(1,10,22)(4,14,19)(7,12,25)\\(2,13,23)(5,17,20)(8,15,26)\\(3,16,24)(6,11,21)(9,18,27)\end{array}. \tag{5.9}$$

It is easily seen that $\langle a, x_1\rangle \cong \langle a, x_2\rangle \cong W_3$. We shall show that for the pair (a, x_1) conditions (i), (ii) and $(iii)(c1)$ of Theorem 1.2 hold, whilst for the pair (a, x_2) conditions (i), (ii) and $(iii)(c2)$ hold.

(a, x_1) :
As in the proof of Theorem 1.2 we consider the columns of x_1 in (5.8) and note that columns 2, 5 and 8 ensure that the matrix A_{x_1} has a block of constant ones. Indeed

$$A_{x_1} = \left(\begin{array}{ccc|ccc|ccc} 0&0&0&1&1&1&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ \hline 0&0&0&0&0&0&3&0&0\\ 0&0&0&0&0&0&0&3&0\\ 0&0&0&0&0&0&0&0&3\\ \hline 1&1&1&0&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&0 \end{array}\right),$$

whilst

$$A_a^{x_1} = \left(\begin{array}{ccc|ccc|ccc} 0&1&0&0&0&1&0&1&0\\ 0&0&1&1&0&0&0&0&1\\ 1&0&0&0&1&0&1&0&0\\ \hline 0&1&0&0&1&0&0&0&1\\ 0&0&1&0&0&1&1&0&0\\ 1&0&0&1&0&0&0&1&0\\ \hline 0&0&1&0&1&0&0&1&0\\ 1&0&0&0&0&1&0&0&1\\ 0&1&0&1&0&0&1&0&0 \end{array}\right).$$

Consider the representation of x_1 in (5.8) and the element

$$\begin{aligned} y_1 := (ax_1)^3 =& (1,2,3)(4,5,6)(7,8,9)(10,13,16)(11,14,17)\\ &(12,15,18)(19,22,25)(20,23,26)(21,24,27). \end{aligned}$$

Denoting the permutation corresponding to the i^{th} column of x_1 by σ_i we see that

$$y_1 = \sigma_1^{i_1}\cdot\sigma_2^{i_2}\cdot\sigma_3^{i_3}\cdot\sigma_4^{i_4}\cdot\sigma_5^{i_5}\cdot\sigma_6^{i_6}\cdot\sigma_7^{i_7}\cdot\sigma_8^{i_8}\cdot\sigma_9^{i_9},$$

where $i_1 = i_2 = \cdots = i_9 = 1$.

We now define the polynomials $f_j(X) \in \mathbb{Z}_3[X]$ as described in the proof of the theorem. First set $f_1(X) := 0 \in \mathbb{Z}_3[X]$ and consider the orbit of 1 under ax_1. Since $1^{ax_1} = 13$ and 13 is in the second row of x_1 in (5.8), we have "descended" by 1 row. Hence we redefine $f_1(X) := f_1(X) + X^1 = X^1$. As $13^{ax_1} = 22$ and 22

is in the first row of x_1 we have cyclically descended a further 2 rows, and so we set $f_1(X) := f_1(X) + X^2 = X + X^2$. Finally, $22^{ax_1} = 2$ and 2 is in the second row of x_1. Thus we have descended by a further row, and our final polynomial is

$$f_1(X) := f_1(X) + X^1 = 2X + X^2 \in \mathbb{Z}_3[X].$$

By considering the images of the first column of x_1 under the action of $(ax_1)^1$, $(ax_1)^2$ and $(ax_1)^3$ we see that we have accounted for an entry of 1 in each of the circled entries of

$$A_a^{x_1} = \left(\begin{array}{ccc|ccc|ccc} 0 & \textcircled{1} & 0 & 0 & 0 & \textcircled{1} & 0 & 1 & 0 \\ 0 & 0 & \textcircled{1} & \textcircled{1} & 0 & 0 & 0 & 0 & 1 \\ \textcircled{1} & 0 & 0 & 0 & \textcircled{1} & 0 & 1 & 0 & 0 \\ \hline 0 & \textcircled{1} & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & \textcircled{1} & 0 & 0 & 1 & 1 & 0 & 0 \\ \textcircled{1} & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}\right). \tag{5.10}$$

Hence the contribution to the block sum matrix $BS(A_a^{x_1})$ from these columns is

$$\begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix} = \mathrm{circ}(0, 2, 1).$$

This is the matrix for which $f_1(X)$ is the representer polynomial.

Similarly $f_2(X) = 2X + X^2 \in \mathbb{Z}_3[X]$, which accounts for additional entries of 1 in (5.10). This gives

$$A_a^{x_1} = \left(\begin{array}{ccc|ccc|ccc} 0 & \textcircled{1} & 0 & 0 & 0 & \textcircled{1} & 0 & 1 & 0 \\ 0 & 0 & \textcircled{1} & \textcircled{1} & 0 & 0 & 0 & 0 & 1 \\ \textcircled{1} & 0 & 0 & 0 & \textcircled{1} & 0 & 1 & 0 & 0 \\ \hline 0 & \textcircled{1} & 0 & 0 & \textcircled{1} & 0 & 0 & 0 & \textcircled{1} \\ 0 & 0 & \textcircled{1} & 0 & 0 & \textcircled{1} & \textcircled{1} & 0 & 0 \\ \textcircled{1} & 0 & 0 & \textcircled{1} & 0 & 0 & 0 & \textcircled{1} & 0 \\ \hline 0 & 0 & 1 & 0 & \textcircled{1} & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & \textcircled{1} & 0 & 0 & 1 \\ 0 & 1 & 0 & \textcircled{1} & 0 & 0 & 1 & 0 & 0 \end{array}\right). \tag{5.11}$$

Finally, $f_3(X) = 2X+X^2 \in \mathbb{Z}_3[X]$ which contributes a 1 to the remaining entries of (5.11). We note that in general, it is not the case that the $f_i(X) \in \mathbb{Z}_p[X]$ are all equal.

The final step of the proof of Theorem 1.2 considers the representer polynomials $f_1(X), f_2(X), f_3(X) \in \mathbb{Z}_3[X]$ and $f_{BS(A_a^x)}(X) \in \mathbb{Z}_9[X]$. We see that $f_j'(1) = 1 = i_j^{-1} \in \mathbb{Z}_3$ for all j, as given in (5.5). Moreover, considering

$f'_j(X) \in \mathbb{Z}_9(X)$ we have that $f'_j(1) = 4$ for all j. Consequently

$$f'_{BS(A_a^{x_1})}(1) = \sum_{j=1}^{3} f'_j(1) = 3 \neq 0 \in \mathbb{Z}_9$$

and case $(c1)$ holds.

(a, x_2) :
As with x_1, we see that columns 2, 5 and 8 of x_2 in (5.9) ensure that A_{x_2} has the desired form, namely

$$A_{x_2} = \left(\begin{array}{ccc|ccc|ccc} 0&0&0&1&1&1&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ 0&0&0&1&1&1&0&0&0\\ \hline 0&0&0&0&0&0&1&1&1\\ 0&0&0&0&0&0&1&1&1\\ 0&0&0&0&0&0&1&1&1\\ \hline 0&3&0&0&0&0&0&0&0\\ 3&0&0&0&0&0&0&0&0\\ 0&0&3&0&0&0&0&0&0 \end{array}\right),$$

whilst

$$A_a^{x_2} = \left(\begin{array}{ccc|ccc|ccc} 0&2&0&0&0&1&0&0&0\\ 0&0&2&1&0&0&0&0&0\\ 2&0&0&0&1&0&0&0&0\\ \hline 0&0&0&0&2&0&0&1&0\\ 0&0&0&0&0&2&0&0&1\\ 0&0&0&2&0&0&1&0&0\\ \hline 1&0&0&0&0&0&0&2&0\\ 0&1&0&0&0&0&0&0&2\\ 0&0&1&0&0&0&2&0&0 \end{array}\right).$$

In this case we see that

$$\begin{aligned} y_2 := (ax_2)^3 =& (1,5,8)(2,6,9)(3,4,7)(10,17,15)(11,18,13)\\ & (12,16,14)(19,25,24)(20,26,22)(21,27,23) \end{aligned}$$

and so clearly y_2 does not fix the columns of x_2 in (5.9). We thus consider the blocks of columns of x_2 in (5.9), where block 0 is given by the first three columns, block 1 by the middle three columns and block 2 by the final three columns. Denoting the columns of x_2 by $c_1, \ldots, c_9$ we see that the action of a on the columns of x_2 is given by $c_2 \mapsto c_5$, $c_5 \mapsto c_8$, $c_8 \mapsto c_2$ and $c_i \mapsto c_i$ for $i = 1, 3, 4, 6, 7, 9$. It follows that there are six columns whose image under a stays in the same block, meaning that $g_0 = 6$. The remaining three columns are mapped from block i to block $i + 1 \pmod 3$ for some $i = 0, 1, 2$. Hence $g_1 = 3$ and $g_2 = 0$.

Considering the reduced representer polynomial of $A_a^{x_2}$ we have that

$$g_{A_a^{x_2}}(X) = \sum_{j=0}^{2} g_i X^i = 6 + 3X.$$

Moreover we see that the columns of x_2 in (5.9) are permuted under the action of ax_2 in the following cyclic manner

$$c_1 \mapsto c_2 \mapsto c_6 \mapsto c_4 \mapsto c_5 \mapsto c_9 \mapsto c_7 \mapsto c_8 \mapsto c_3 \mapsto c_1.$$

It follows that column i is mapped under y_2 to column $i+3$ (or $i-6$ if $i+3>9$) and in doing so passes through a single block of x_2. Thus using the notation of (5.7) we have that $k_j = 0$ and $\ell_j = 1$ for all $j = 0, 1, 2$.

Consequently the total number of blocks passed through by all columns of x_2 under the action of y_2 is

$$9 = 3 \cdot g'_{A_a^{x_2}}(1)$$

and

$$g'_{A_a^{x_2}}(1) \equiv 3 \equiv \sum_{j=0}^{2} \ell_j \pmod 9.$$

In particular $g'_{A_a^{x_2}}(1) \not\equiv 0 \pmod 9$ and case $(c2)$ holds.

6 The General Case

We now consider the most general setting that $G := \mathrm{Sym}(n)$ for some $n \geq p^2$ and let

$$a = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots (p(r-1)+1, p(r-1)+2, \ldots, pr) \in G$$

for some $r \geq p$. As previously we set $X := a^G$ and consider $x \in X$. Denote the p-cycles forming a (respectively x) by $\alpha_1, \ldots, \alpha_r$ (respectively $\chi_1, \ldots, \chi_r$). We note that if $\langle a, x\rangle \cong W_p$, then $|\mathrm{supp}(\alpha_i) \cap \mathrm{supp}(\chi_j)| = 0, 1$ or p for each $i, j \in \{1, \ldots, r\}$.

Before considering the most general situation, we look at the case that $\mathrm{supp}(a) = \mathrm{supp}(x)$ and prove Theorem 1.3.

Proof of Theorem 1.3: Assume that $\langle a, x\rangle \cong W_p$. Without loss of generality assume that a is in the base group of W_p. We will show that the given conditions hold true (if x is in the base group, then an analogous argument may be used to show that the conditions hold with the roles of a and x interchanged). The commutator relations follow immediately.

First consider the case that $\mathrm{supp}(\alpha_i) = \mathrm{supp}(\chi_j)$ for some $i, j \in \{1, \ldots, r\}$. This results in matrix entries $(A_x)_{i,i} = (A_a^x)_{j,j} = p$. By a suitable renumbering of the α_i and χ_j, we may assume that such a situation arises for pairs (α_i, χ_i) with $i = 1, \ldots, m$ for some m. This gives the diagonal block D_1 of A_x and E_1 of A_a^x. It follows that for all other α_i we have $\mathrm{supp}(\alpha_i^x) \cap \mathrm{supp}(\alpha_i) = \emptyset$.

If $\alpha_i^{x^\ell} \in \langle \alpha_{i_\ell} \rangle$ for $\ell = 1, \ldots, p$ and for some i_ℓ, then we may consider these α_{i_l} and the χ_j that share their common support as lying inside a copy of $\mathrm{Sym}(p^2)$. Thus we may apply the results of Section 3 to obtain the general structures of D_2 and E_2. In all other cases, we use a similar approach to find a subset $I \subset \{1, \ldots, r\}$ of size p^2 such that $\prod_{i \in I} \alpha_i$ and $\prod_{i \in I} \chi_i$ are conjugate elements of full support inside a copy of $\mathrm{Sym}(p^3)$. The results of Section 5 then give the

structures of D_3 and E_3. The final condition on one of the blocks of E_2 or E_3 then follows from the fact that ax has order p^2 and the results of Sections 3 and 5.

Conversely, assume that the conditions in Theorem 1.3 hold (again the argument for when a and x are interchanged is analogous). By Corollary 5.4 it remains to check that ax has order p^2. Suppose that D_1 is an $m_1 \times m_1$ matrix, D_2 is a $pm_2 \times pm_2$ matrix and D_3 is a $p^2m_3 \times p^2m_3$ matrix for some m_1, m_2 and m_3. Define $a_1 = \alpha_1 \cdots \alpha_{m_1}$,

$$\begin{aligned} a_{2,i} &= \alpha_{m_1+p(i-1)+1} \cdots \alpha_{m_1+p(i-1)+p} && \text{for } i = 1, \ldots, m_2, \text{ and} \\ a_{3,j} &= \alpha_{m_1+pm_2+p^2(j-1)+1} \cdots \alpha_{m_1+pm_2+p^2(j-1)+p^2} && \text{for } j = 1, \ldots, m_3. \end{aligned}$$

Define $x_1, x_{2,1}, \ldots, x_{2,m_2}, x_{3,1}, \ldots, x_{3,m_3}$ analogously. We see that the pair (a_1, x_1) corresponds to the blocks D_1 and E_1 of A_x and A_a^x, each pair $(a_{2,i}, x_{2,i})$ corresponds to a block of D_2 and its associated block in E_2, whilst every pair $(a_{3,j}, x_{3,j})$ corresponds to blocks of D_3 and E_3. Moreover, since for each pair (a_*, x_*) we have $\mathrm{supp}(a_*) = \mathrm{supp}(x_*)$ and $[a_*, a_*^{x_*^i}] = 1$, it suffices to check that for one such pair, the element $a_*x_* \in \mathrm{Sym}(\mathrm{supp}(a_*))$ has order p^2. However, this follows immediately from condition (iv) and the results of Sections 3 and 5. Thus $\langle a, x \rangle \cong W_p$. □

In the general setting, we note that by the preceding arguments we must have that $|\mathrm{supp}(a) \cap \mathrm{supp}(x)|$ is divisible by p. Thus the above result will still hold if $n = pr + s$ for some $s < p$. However this is not the case in general, since if we no longer require $\mathrm{supp}(a) = \mathrm{supp}(x)$, the condition that a and x are G-conjugate becomes weaker. Indeed, if we consider $G = \mathrm{Sym}(p^2)$, we have that W_p is embedded into G using the generators $a = (1, 2, \ldots, p)$ and

$$x = (1, p+1, \ldots, p(p-1)+1)(2, p+2, \ldots, p(p-1)+2) \cdots (p, 2p, \ldots, p^2).$$

However, we may also use x and y to generate W_p, where

$$\begin{aligned} y = (1, 2, \ldots, p)(p+1, p+2, \ldots, 2p) \cdots \\ \cdots (p(p-2)+1, p(p-2)+2, \ldots, p(p-1)). \end{aligned}$$

If we now relax our assumption that $\mathrm{supp}(a) = \mathrm{supp}(x)$ and move into $G := \mathrm{Sym}(p(p+1))$, we see that taking $x \in G$ as above and

$$\overline{y} = y \cdot (p^2+1, p^2+2, \ldots, p(p+1)),$$

we have that $\langle x, \overline{y} \rangle \cong W_p$. However, it is clear that the generation of W_p results from the elements $x, y \in \mathrm{Sym}(p^2) \hookrightarrow G$. It follows that although x and $\overline{y}$ are G-conjugate, this conjugation is in some sense artificial. Consequently, producing a theorem such as Theorem 1.3 would not be realistic in the most general setting.

Acknowledgement. The author would like to thank their supervisor, Peter Rowley, for his guidance throughout this research.

References

[1] J. Ballantyne *On local fusion graphs of finite Coxeter groups.* J. Group Theory, 16(2013),595–617.

[2] J. Ballantyne, N. Greer and P. Rowley *Local Fusion Graphs for Symmetric Groups*. J. Group Theory, 16(2013),35–49.

[3] C. Bates, D. Bundy, S. Hart and P. Rowley *A Note on Commuting Graphs for Symmetric Groups*. Electron. J. Combin., 16(2009).

[4] C. Bates, D. Bundy, S. Perkins and P. Rowley *Commuting involution graphs for symmetric groups*. J. Algebra, 266(2003),133–153.

[5] C. Bates, D. Bundy, S. Perkins and P. Rowley *Commuting involution graphs for finite Coxeter groups*. J. Group Theory, 6(2003),461–476.

[6] C. Bates, D. Bundy, S. Perkins and P. Rowley *Commuting Involution Graphs in Special Linear Groups*. Comm. Algebra, 32(2004),4179–4196.

[7] W. Bosma and J.Cannon *Discovering Mathematics with Magma: Reducing the Abstract to the Concrete*, Volume 19 of Algorithms and Computation in Mathematics. Springer, 2006.

[8] J.R. Britnell and N. Gill *Perfect commuting graphs*. ArXiv e-prints, 1309.2237, 2013.

[9] K.S. Brown *Euler Characteristics of Groups: The p-Fractional Part*. Invent. Math., 29(1975),1–5.

[10] K.S. Brown *High dimensional cohomology of discrete groups*. Proc. Nat. Acad. Sci. U.S.A., 73(1976),1795–1797.

[11] J. Cannon, C. Playoust and W. Bosma *Algebraic Programming with Magma: An Introduction to the Magma Categories*. Springer, 2007.

[12] Y. Drozd and R.V. Skuratovskii *Generators and Relations for Wreath Products*. Ukrainian Math. J., 60(2008),1168–1171.

[13] A. Everett *Commuting Involution Graphs for 3-Dimensional Unitary Groups*. Electron. J. Combin., 18(2011)

[14] I. Kra and S. Simanca *On circulant matrices*. Notices Amer. Math. Soc., 59(2012),368–377.

[15] G.L. Morgan and C.W. Parker *The diameter of the commuting graph of a finite group with trivial centre*. J. Algebra, 393(2013),41–59.

[16] C.W. Parker *The commuting graph of a soluble group*. Bull. Lond. Math. Soc., 45(2013),839–848.

[17] S. Perkins *Commuting involution graphs for* $\tilde{A}_n$. Arch. Math., 86(2006),16–25.

[18] D. Quillen *Homotopy Properties of the Poset of Nontrivial p-Subgroups of a Group*. Adv. Math., 28(1978),101–128.

[19] M.A. Ronan *Duality for Presheaves on Chamber Systems and a Related Chain Complex*. J. Algebra, 121(1989),263–274.

[20] M.A. Ronan and S.D. Smith *Sheaves on Buildings and Modular Representations of Chevalley Groups.* J. Algebra, 96(1985),319–346.

[21] M.A. Ronan and S.D. Smith *Universal Presheaves on Group Geometries and Modular Representations.* J. Algebra, 102(1986),133–154.

[22] M.A. Ronan and S.D. Smith *Computation of* 2*-modular sheaves and representations for* $L_4(2), A_7, 3S_6,$ *and* M_{24}. Comm. Algebra, 17(1989),1199–1237.

[23] P. Rowley and D. Ward *On* π*-Product Involution Graphs in Symmetric Groups.* MIMS ePrint, 2014.

[24] M.R. Salarian *Characterizing some small simple groups by their commuting involution graphs.* Southeast Asian Bull. Math., 35(2011),467–474.

[25] J. Shareshian *Hypergraph matching complexes and Quillen complexes of symmetric groups.* J. Combin. Theory Ser. A, 106(2004), 299-314.