Irish Math. Soc. Bulletin **56** *(2005), 53–74*

The Cyclizer Function on Permutation Groups

C. C. FIDDES AND G. C. SMITH

Abstract. Let G be a transitive permutation group acting on a finite set Ω. A cycle c is involved in a permutation g if and only if gc^{-1} fixes all points of $\mathrm{Supp}(c)$. We define a function $Cyc(G)$ which takes the permutation group G to the group generated by the cycles involved in its elements. Let $Cyc^1(G) = Cyc(G)$ and $Cyc^{i+1}(G) = Cyc(Cyc^i(G)))$. It is known that $Cyc^3(G) = Cyc^4(G)$ for all such groups. We investigate and characterize those groups for which $Cyc^2(G) \neq Cyc^3(G)$.

Introduction

In a permutation group each element is a product of disjoint cycles. We say that a cycle c is involved in a permutation g if and only if gc^{-1} fixes all points of $\mathrm{Supp}(c)$. The cyclizer $Cyc(G)$ of a finite permutation group G is the group generated by the cycles involved in G. It is clear that to understand $Cyc(G)$, it suffices to assume that G is a transitive group of degree n. We make this assumption. Let $Cyc^i(G)$ denote the result of performing the cyclizing operation i times, so we have the cyclizer sequence

$$G = Cyc^0(G) \leq Cyc^1(G) \leq \cdots .$$

When $Cyc^{k-1}(G) \neq Cyc^k(G) = Cyc^{k+1}(G)$ we say that G has *cyclizer length* k. This sequence of groups was investigated by Cameron [1] who showed that every finite permutation group has cyclizer length at most 3. If $Cyc(G) = G$, we say that G is cycle-closed. He showed that the non-trivial cycle closed groups are precisely the cyclic groups of prime order and the symmetric groups, both in their natural representations. Cameron posed various problems, including the determination of the (finite transitive permutation) groups G such that $Cyc^2(G) \neq Cyc^3(G)$. We solve this problem.

1. Cameron's Results and Some New Observations

We begin with some general observations. If G is a cycle-closed transitive permutation group of degree n containing a transposition, then G is a symmetric group. Thus any transitive cycle-closed group of even degree is a symmetric group. If a permutation group G is transitive and cycle-closed, then it is prime cyclic or symmetric. For a primitive transitive permutation group G of degree n exactly one of the following applies:

(1) G is prime cyclic,
(2) $Cyc(G) = S_n$,
(3) $Cyc(G) = A_n$.

Note Williamson's lemma:

Lemma 1 (Williamson)**.** *A primitive subgroup of S_n is S_n or A_n whenever it contains an m-cycle for some m satisfying the bound*

$$1 < m \leq (n-m)!$$

In any cyclizer sequence at most three primitive groups can appear. In particular any primitive group will have a cyclizer sequence of length less than three. If a group G is such that $Cyc(G)$ is imprimitive, then G is a p-group. If G is a transitive, imprimitive permutation group such that $Cyc(G)$ is primitive, then $Cyc^2(G)$ is the full symmetric group. For all finite groups G, $Cyc^3(G) = Cyc^4(G)$. If G is a transitive, imprimitive permutation group such that $Cyc(G)$ is imprimitive, then $Cyc^2(G)$ is primitive and moreover contains A_n. Thus if $Cyc(G)$ is imprimitive and G is a 2-group, then $Cyc^2(G)$ is S_n.

Some of this information can be found in Cameron's article [1], or can be easily deduced from his proofs. However, one of these facts is not immediate from Cameron's work, and we supply a justification.

Theorem 2. *If a group G is such that $Cyc(G)$ is imprimitive, then G is a p-group.*

Proof. The group G must be imprimitive, all its blocks be of p-power size for some prime p and blocks only be moved by p-power cycles. Let g be a p^n-cycle involved in an element of G that moves a block Δ_1 (we can assume that $|\Delta_1| = p^{(n-1)}$) and let $\mathrm{Supp}(g) = \Omega$. We will first consider the setwise stabilizer of Ω in G acting on Ω; let this group be H. The set Ω is partitioned into blocks $\Delta_1, \Delta_2, \ldots, \Delta_p$, any element of H that moves these blocks will be known as a *threading* *element*, and elements that fix the blocks setwise will be known as *null elements*. Assume, for contradiction, that H contains an element of order q for some prime $q \neq p$, then this element must be a null element. Let $K \leq H$ be the set of null elements and let Q be a Sylow q-subgroup of H, hence $Q \leq K$. The Frattini argument tells us that $H = N_H(Q) \cdot K$. The group Q is not transitive on Ω and therefore partitions it into more than one Q-orbit. At least one of these orbits is of size one, as q does not divide $|\Omega| = p^n$ and at least one is larger than this as Q is a non-trivial group. Let $h \in H$ be an element of $N_H(Q)$ but not of K. The element h normalizes Q and therefore acts on the Q-orbits, as we have seen these orbits are not of a uniform size and so the group generated by h cannot act transitively on them. This contradicts h being a threading element and therefore no elements of order q can exist. The same argument follows for any $g \in G$ that moves blocks and as G is transitive we can conclude that G does not contain any elements of prime order for primes other than p. $\square$

2. Groups of Degree p^2

We seek finite transitive permutation groups of degree p^2 which have cyclizer length 3. We have already seen that such groups are p-groups, and transitivity gives us that they must be permutation groups of prime power degree. We will begin by looking at p-groups of degree p^2.

Theorem 3. *If G is a transitive p-group of degree p^2 and exponent p, then $Cyc(G)$ is primitive.*

Proof. Let G be such a group. Blocks of $Cyc(G)$ are also blocks of G. Let Δ be a nontrivial block of the group G and α, $\beta \in \Omega$ be such that $\alpha \in \Delta$, $\beta \notin \Delta$. Then, by transitivity, there exists a p-cycle c, involved in an element of G, such that $(\alpha)c = \beta$; this cycle is an element of the group $Cyc(G)$. As c moves p points and $|\Delta|$ is at least p, the set Δ must contain at least one fixed point of c. Call this point γ. We have that $\gamma \in \Delta \cap (\Delta)c$ so $\Delta \cap (\Delta)c \neq \emptyset$ and also $\beta \notin \Delta$ so $\Delta \neq (\Delta)c$, hence Δ is not a block of $Cyc(G)$. The group $Cyc(G)$ can have no nontrivial blocks and so is primitive. $\square$

We can say more than just that $Cyc(G)$ is primitive. Lemma 1 tells us that $Cyc(G)$ is in fact A_{p^2}. So we have the following corollary.

Corollary 4. *If G is a transitive p-group of degree p^2 and exponent p, then $Cyc^2(G) = S_{p^2}$.*

It is a routine matter to verify that the cyclizer of a cyclic group generated by a p^2-cycle is isomorphic to the group C_p Wr C_p.

The group $Cyc^2(\langle g\rangle)$ (where g is a p^2 cycle as above) is a primitive group and is therefore by Lemma 1 either alternating or symmetric. However all cycles involved in $Cyc(\langle g\rangle)$ are cycles of odd length, therefore $Cyc^2(\langle g\rangle) = A_{p^2}$ and $Cyc^3(\langle g\rangle) = S_{p^2}$.

Theorem 5. *If G is a transitive p-group of degree p^2 and exponent p^2, then either $G = C_p$ Wr C_p or $Cyc(G) = C_p$ Wr C_p (and hence $Cyc^2(G) = A_{p^2}$ and $Cyc^3(G) = S_{p^2}$).*

Before proving we will look in more detail at the group C_p Wr C_p. The group $W := C_p$ Wr C_p is a Sylow p-subgroup of S_{p^2} and hence contains copies of all p-groups of degree p^2. The base group of this wreath product is $B := \underbrace{C_p \times \cdots \times C_p}_{p \text{ times}}$. The complement group of the wreath product is W/B and is isomorphic to C_p, an abelian group of exponent p. Therefore $W' \leqslant B$ and $W^p \leqslant B$. By Burnside's basis theorem the Frattini subgroup of W is $W'W^p$ which is also a subgroup of B. As $\Phi(W) \leq B$ we have that $Cyc(\Phi(W)) \leqslant Cyc(B) = B \leqslant W$. The group W is not cyclic and can be generated by a p^2-cycle and a p-cycle, hence W is a 2-generator group. Therefore the basis theorem also tells us that any two independent elements (i.e., one is not a power of the other modulo $\Phi(W)$) of $W - \Phi(W)$ will generate W.

As before let g be the p^2-cycle $(0, 1, 2, \ldots, p^2 - 2, p^2 - 1)$, g_0 be the p-cycle $(0, p, 2p, \ldots, (p-1)p)$ and let $W := Cyc(\langle g\rangle) = \langle g, g_0\rangle \cong C_p$ Wr C_p. Recall that g^p was the product of p-cycles $g_0 g_1 \cdots g_d$ where $d = p - 1$. The cycles $g_0, \ldots, g_d$ are all disjoint and therefore commute, the cycle g commutes with the other cycles as follows

$$[g_i, g] = g_i^d\, g_i^g = g_i^d\, g_j \qquad \text{where } j \equiv i + 1 \bmod p.$$

Lemma 6. *All elements of the group W can be written uniquely in the form*

$$g^{\varepsilon_g}\, g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d}$$

where each ε is from the set $\{0, \ldots, d\}$.

Proof. There are p^{p+1} elements of this form and p^{p+1} elements of the group W. It therefore suffices to show that any two elements of this form are indeed distinct elements of W. The supports of the cycles $g_0,\ldots,g_d$ form a block system for our group. The identity element fixes these blocks and therefore if we write the identity element in the form $g^{\varepsilon_g}\, g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}$ we must have that $\varepsilon_g=0$. The cycles $g_0,\ldots,g_d$ are disjoint and so we also have that $\varepsilon_0=\cdots=\varepsilon_d=0$, thus the identity element can only be written in this form as $g^0 g_0^0\cdots g_d^0$.

Assume that $g^{\varepsilon_g}\, g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}=g^{\delta_g}\, g_0^{\delta_0}\cdots g_d^{\delta_d}$, with each ε and δ in $\{0,\ldots,d\}$.

$$\begin{aligned}\mathrm{Id} &= g^{\varepsilon_g}\, g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}\, g_d^{-\delta_d}\cdots g_0^{-\delta_0}\, g^{-\delta_g}\\ &= g^{\varepsilon_g}\, g^{-\delta_g}\, g^{\delta_g}\, g_0^{\varepsilon_0-\delta_0}\ \cdots g_d^{\varepsilon_d-\delta_d}\, g^{-\delta_g}\\ &= g^{\varepsilon_g-\delta_g}\, g_{-\delta_g}^{\varepsilon_0-\delta_0}\ \cdots g_{d-\delta_g}^{\varepsilon_d-\delta_d}\end{aligned}$$

(here the subscripts and powers are taken modulo p) and hence $\varepsilon_g=\delta_g$ and $\varepsilon_i=\delta_i$ for all $i\in\{0,\ldots,d\}$. □

Lemma 7. *The Frattini subgroup of W is the set of elements of the form $g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}$ such that $\sum_{i=0}^d \varepsilon_i\equiv 0 \bmod p$.*

Proof.

$$\begin{aligned}W' &= \langle [g_i,g]=g_i^d\, g_{i+1} \mid i\in\{0,\ldots,d\}\rangle\\ &= \left\{ g_0^{\varepsilon_0}\, g_1^{\varepsilon_1}\ \cdots\ g_d^{\varepsilon_d} \,\middle|\, \textstyle\sum_{i=0}^d \varepsilon_i \equiv 0 \bmod p\right\}\end{aligned}$$

$$\begin{aligned}W^p &= \{w^p \mid w\in W\}\\ &= \left\{ g_0^{p\varepsilon_0}\, g_1^{\sigma}\ \cdots\ g_d^{\sigma} \,\middle|\, \sigma=\textstyle\sum_{i=0}^d \varepsilon_i,\ \ \varepsilon_i\in\{0,\ldots,d\}\right\}\\ &\le W'\end{aligned}$$

Hence $\Phi(W)$ (the Frattini subgroup of W) is

$$W'W^p=\left\{ g_0^{\varepsilon_0}\, g_1^{\varepsilon_1}\ \cdots\ g_d^{\varepsilon_d} \,\middle|\, \sum_{i=0}^d \varepsilon_i\equiv 0 \bmod p\right\}.$$

□

Now we will consider the group generated by the p^2-cycle g and the non-generators of the group W

$$\langle g,\Phi(W)\rangle=\langle g\rangle\Phi(W)=\left\{ g^{\varepsilon_g} g_0^{\varepsilon_0}\, g_1^{\varepsilon_1}\ \cdots\ g_d^{\varepsilon_d} \,\middle|\, \sum_{i=0}^d \varepsilon_i\equiv 0 \bmod p\right\}.$$

Lemma 8. *Elements of* $\langle g\rangle \cdot \Phi(W)$ *of the form*

$$g^{\varepsilon_g}\ g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d}$$

with $\varepsilon_g \neq 0$ *are* p^2*-cycles.*

Proof. The group $\langle g\rangle \cdot \Phi(W)$ has order p^p. The centralizer of a p^2-cycle in $\langle g\rangle\cdot\Phi(W)$ is the group generated by that cycle and so has order p^2. There are therefore p^{p-2} conjugacy classes of p^2-cycles inside $\langle g\rangle\cdot\Phi(W)$. There are $(p-1)p^{p-1}$ elements of the form $g^{\varepsilon_g}\ g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}$ in $\langle g\rangle \cdot \Phi(W)$ (as we have $p-1$ choices of ε_g and p choices each of $\varepsilon_0, \ldots, \varepsilon_{d-1}$ whence ε_d is fixed). It therefore suffices to show that $\langle g\rangle \cdot \Phi(W)$ has $(p-1)p$ conjugacy classes of p^2-cycles.

We will show that the $(p-1)p$ elements of the form $g_0^{-\varepsilon_0} g^{\varepsilon_g} g_0^{\varepsilon_0}$ $(0 \leq \varepsilon_0 \leq d,\ 1 \leq \varepsilon_g \leq d)$ are all in different conjugacy classes of $\langle g\rangle \cdot \Phi(W)$.

First note that $g_0^{-\varepsilon_0} g^{\varepsilon_g} g_0^{\varepsilon_0} = g^{\varepsilon_g} g_{\varepsilon_g}^{-\varepsilon_0} g_0^{\varepsilon_0}$ and so these elements are all in the group $\langle g\rangle \cdot \Phi(W)$. Now assume that $\alpha := g_0^{-\varepsilon_0} g^{\varepsilon_g} g_0^{\varepsilon_0}$ and $\beta := g_0^{-\delta_0} g^{\delta_g} g_0^{\delta_0}$ are conjugate in $\langle g\rangle \cdot \Phi(W)$. So there exists some $\gamma \in \langle g\rangle \cdot \Phi(W)$ such that $\gamma^{-1}\alpha\gamma\beta^{-1} = \mathrm{Id}$. Let $\gamma := g^{\zeta_g}\ g_0^{\zeta_0}\cdots g_d^{\zeta_d}$ with $\sum_{i=0}^{d} \zeta_i \equiv 0 \bmod p$.

$$\begin{aligned}\mathrm{Id} &= \gamma^{-1}\alpha\gamma\beta^{-1} \\ &= g^{-\zeta_g}\ g^{\varepsilon_g}\ g^{\zeta_g}\ g^{-\delta_g}\varphi\end{aligned}$$

for some $\varphi \in \Phi(W)$. Hence $\varepsilon_g = \delta_g$.

Now we have

$$\begin{aligned}\gamma^{-1} g_0^{-\varepsilon_0} g^{\varepsilon_g} g_0^{\varepsilon_0}\gamma &= g_0^{-\delta_0} g^{\varepsilon_g} g_0^{\delta_0} \qquad \text{and} \\ g_0^{\delta_0}\gamma^{-1} g_0^{-\varepsilon_0} g^{\varepsilon_g} g_0^{\varepsilon_0}\gamma g_0^{-\delta_0} &= g^{\varepsilon_g}.\end{aligned}$$

Therefore $g_0^{\varepsilon_0}\gamma g_0^{-\delta_0} \in \langle g\rangle \leq \langle g\rangle \cdot \Phi(W)$. Rearranging gives

$$g_0^{\varepsilon_0}\gamma g_0^{-\delta_0} = g^{\zeta_g}\ g_0^{\zeta_0}\cdots g_d^{\zeta_d}\ g_{\zeta_g}^{\varepsilon_0}\ g_0^{-\delta_0}$$

and as $\sum_{i=0}^{d} \zeta_i \equiv 0 \bmod p$ we must have that $\varepsilon_0 = \delta_0$. Hence α and β are equal. □

Proof of Theorem 5. Let G be a transitive p-group of degree and exponent p^2 such that $G \neq C_p \mathrm{\ Wr\ } C_p$. The group G contains a p^2-cycle, g. As before let $g^p = g_0 \cdots g_d$. We have $Cyc(G) \geq Cyc(\langle g\rangle) \cong C_p \mathrm{\ Wr\ } C_p$. Once again we will let $W := \langle g, g_0\rangle \cong C_p \mathrm{\ Wr\ } C_p$. As $G \neq W$ and W is a 2-generator group, it must be the case that $G \leq \langle g, \Phi(W)\rangle = \langle g\rangle.\Phi(W)$. Now if x is an element of G, then x must satisfy at least one of the following conditions:

- $x \in \langle g \rangle$,
- $x \in \Phi(W)$,
- $x = g^{\varepsilon_g}.\varphi$ where $\varphi \in \Phi(W)$ and $1 \leq \varepsilon_g \leq d$.

If x falls in to the first or second categories, then we have seen above that all cycles involved in x will be elements of W. If x is in the third category, then x is a p^2-cycle and this cycle is an element of W. Hence $Cyc(G) = W$. $\square$

Corollary 9. *A transitive p-group G of degree p^2 is such that $Cyc^2(G) \neq Cyc^3(G)$ if and only if the exponent of G is p^2.*

3. p-GROUPS OF DEGREE p^n

Let $P_{(p,n)}$ be the group C_p Wr C_p Wr $\cdots$ Wr C_p of degree p^n. When the prime p is unimportant we shall refer to this group as P_n. Similarly we will later define a group M_n which will be denoted as $M_{(p,n)}$ if referring to a particular prime. Then P_n is a Sylow p-subgroup of S_{p^n} and hence contains copies of all transitive p-groups of degree p^n, in particular it contains copies of all G such that $Cyc^2(G) \neq Cyc^3(G)$. As in the previous example we will define a normal form for elements of this group. Let P_n act on p^n points numbered in base p, so for example C_3 Wr C_3 Wr C_3 acts on the points

$$\Omega = \{000, 001, 002, 010, 011, \ldots, 220, 221, 222\}.$$

Let g be a p^n-cycle from $P_{p,n}$ and without loss of generality let it cycle the points in numerical order. In the following let $p - 1 = d$. The element g^p will involve p cycles of length p^{n-1}. Call these cycles $g_0, g_1, \ldots g_d$ and label them so that the point 0 is in the support of g_0, the point 1 is in the support of g_1 and so on. In our example these cycles are

$$\begin{aligned} g_0 &= (000, 010, 020, 100, 110, 120, 200, 210, 220) \\ g_1 &= (001, 011, 021, 101, 111, 121, 201, 211, 221) \\ g_2 &= (002, 012, 022, 102, 112, 122, 202, 212, 222). \end{aligned}$$

Now consider the pth power of the cycle g_i. It involves p cycles of length p^{n-2}. Call these $g_{0i}, g_{1i}, \ldots, g_{di}$ and again label them so that each contains the number by which it is indexed. Returning to the example $g_{01} = (001, 101, 201), g_{11} = (011, 111, 211)$ and $g_{21} = (021, 121, 221)$. This process can be continued until we have p^n p-cycles; each labelled by an $n-1$ digit number. In C_3 Wr C_3 Wr C_3

this process gives one 27-cycle g, three 9-cycles g_0, g_1 and g_2 and nine 3-cycles $g_{00}, \ldots, g_{22}$.

Call a cycle a level k cycle if it is indexed by a k digit number (the cycle g is the level 0 cycle). The level $n-1$ cycles generate the base group of $P_n = C_p \text{ Wr } (C_p \text{ Wr } C_p \text{ Wr } \cdots \text{ Wr } C_p)$. The support of each of these cycles is therefore a P_n-block. The level $n-2$ cycles act on the set of level $n-1$ blocks as a cyclic group of order p and therefore the level $n-1$ and $n-2$ cycles together generate the base group of $P_n = (C_p \text{ Wr } C_p) \text{ Wr } (C_p \text{ Wr } \cdots \text{ Wr } C_p)$. Inductively we can see that the level 0 to level $n-1$ cycles generate P_n and that the support of each cycle is a block under the action of P_n. Let the support of a level k cycle be called a level k block, then the set of level k blocks forms a complete block system for each $k \in \{0, 1, \ldots, d\}$ (where the level 0 block system consists of a single block containing all points). The set of level k blocks will be labelled by Ω_k, so $\Omega_0 = \Omega$ and define Ω_n to be the set of singletons $\{\{\omega\} | \omega \in \Omega\}$. Let $\Delta_j = \text{Supp}(g_j)$ for all $j \in \{0, 1, 2, \ldots, 00, 01, 02, \ldots, d \cdots d\}$ so for example the level 1 block system consists of the blocks $\Delta_0, \Delta_1, \ldots$ and Δ_d.

Theorem 10. *The level* 1 *to level d block systems are the only non-trivial block systems of the action of P_n on the p^n points.*

Proof. Let $\Gamma \subseteq \Omega$ be a block of P_n. Since P_n is a transitive p-group $|\Gamma| = p^k$ for some $k \leqslant n$. The blocks in the set Ω_{n-k} partition Ω into blocks of size p^k. Choose i such that there exists a point $\alpha \in \Gamma \cap \Delta_i$, where $\Delta_i \in \Omega_{n-k}$. The cycle g_i is in the group P_n and therefore Γ is either fixed set-wise or displaced to a disjoint set by this cycle. It can not be the case that $(\Gamma)g_i \cap \Gamma = \emptyset$ (as this would require $|\text{Supp}(g_i)| \geq 2|\Gamma|$, but we know $|\text{Supp}(g_i)| = |\Gamma|$) hence g_i is a permutation of the points of Γ and $\Gamma = \Delta_i$. $\square$

Later we will need to consider the set-wise stabiliser of Δ_0 acting on Δ_0 written

$$P_{n\{\Delta_0\}}^{\Delta_0}.$$

The set-wise stabilizer for each of the level 1 blocks is

$$\underbrace{(C_p \text{ Wr } \cdots \text{ Wr } C_p) \times \cdots \times (C_p \text{ Wr } \cdots \text{ Wr } C_p)}_{p \quad \text{copies}},$$

hence ${P_n}^{\Delta_0}_{\{\Delta_0\}}$ is isomorphic to P_{n-1}. We will also be considering the action of P_n on Ω_{n-1}, written

$$P_n^{\Omega_{n-1}}.$$

This is the complement group of the wreath product

$$P_n = C_p \text{ Wr } (C_p \text{ Wr } \cdots \text{ Wr } C_p),$$

and hence is also P_{n-1}.

It is necessary to know the commutation relations between these cycles as we will then use this information to construct a normal form and to define subgroups of P_n. Distinct cycles from the same level commute as their supports are disjoint. We will begin by looking at commutators in C_3 Wr C_3 Wr C_3 as an example.

$$[g_0, g] = g_0^{-1}\, g_1 = g_0^2\, g_1\, g_{00}^2\, g_{10}^2\, g_{20}^2, \qquad (\text{ as } g_0^{-1} = g_0^2\, g_{00}^2\, g_{10}^2\, g_{20}^2)$$
$$[g_1, g] = g_1^{-1}\, g_2 = g_1^2\, g_2\, g_{01}^2\, g_{11}^2\, g_{21}^2,$$

$$[g_{00}, g_0] = g_{00}^{-1}\, g_{00}^{g_0} = g_{00}^2\, g_{10} \quad \text{and}$$
$$[g_{00}, g] = g_{00}^{-1}\, g_{00}^{g} = g_{00}^2\, g_{01}.$$

Now let g_a and g_b be two of the specified cycles from P_n (a and b are numbers in base p). The commutator will be trivial unless g_a and g_b have supports that intersect. This only happens when a and b are in different levels (so without loss of generality assume that a is an r digit number and b is an s digit number with $r > s$) and when the number b occurs as the last s digits of the number a. When this happens

$$[g_a, g_b] = g_a^{-1}\, g_a^{g_b} = \begin{cases} g_a^d\, g_c & : \text{ when } r = n-1 \\ g_a^d\, g_c\, g_{1a}^d\, g_{2a}^d \cdots g_{da}^d & : \text{ when } r < n-1. \end{cases} \tag{1}$$

If the number a is $a_1\, a_2\, \cdots\, a_s\, a_{s+1}\, \cdots\, a_r$ (each a_i representing a single digit), then c is the number $a_1\, a_2\, \cdots\, a_s\, \tilde{a}_{s+1}\, \cdots\, a_r$ where $\tilde{a}_{s+1} \equiv a_{s+1} + 1 \bmod p$.

Theorem 11. *Each element of P_n can be written in the normal form*

$$g^{\varepsilon_g}\, g_0^{\varepsilon_0}\, g_1^{\varepsilon_1}\, \cdots\, g_d^{\varepsilon_d}\, g_{00}^{\varepsilon_{00}}\, \cdots\cdots\, g_{dd\cdots d}^{\varepsilon_{dd\cdots d}} \tag{2}$$

where all ε's are from the set $\{0, 1 \ldots, d\}$.

Proof. The proof is by induction. We have already seen that this holds for P_2, now assume that it also holds for P_{n-1}. The group P_n has order $p^{1+p+p^2+\cdots+p^{n-1}}$. This is the also the number of elements of the form 2. It therefore suffices to show that two elements of this form written differently really are distinct. Let

$$a := g^{\varepsilon_g}\ g_0^{\varepsilon_0}\ g_1^{\varepsilon_1}\ \cdots\ g_d^{\varepsilon_d}\ g_{00}^{\varepsilon_{00}}\ \cdots\cdots\ g_{dd\cdots d}^{\varepsilon_{dd\cdots d}}$$
$$\text{with each } \varepsilon \in \{0, 1 \dots, d\}$$

$$b := g^{\delta_g}\ g_0^{\delta_0}\ g_1^{\delta_1}\ \cdots\ g_d^{\delta_d}\ g_{00}^{\delta_{00}}\ \cdots\cdots\ g_{dd\cdots d}^{\delta_{dd\cdots d}}$$
$$\text{with each } \delta \in \{0, 1 \dots, d\}$$

and assume that $ab^{-1} = \mathrm{Id}$. Note that if an element of this form (2) is the identity element, then the exponent of every cycle must be zero. Using the commutator from above (1) we can rewrite ab^{-1} so that it starts $g^{\varepsilon_g} g^{-\delta_g} \dots$ and no other occurrences of the cycle g appear in the word. Hence $\varepsilon_g = \delta_g$ and we are left with a word in the cycles g_i such that the exponent of g is zero. This word is an element of the base group $P_{n-1} \times P_{n-1} \times \cdots \times P_{n-1}$. Now considering the element ab^{-1} restricted to each transitive constituent and using the inductive hypothesis we get that $\varepsilon_i = \delta_i$ for all i. $\square$

Let D_n be the subgroup of P_n generated by the commutators of the cycles $g, g_1, \dots g_{d\cdots d}$. Through similar analysis to the case for C_p Wr C_p we can show that D_n is the set of elements which when written in normal form satisfy the following conditions:

$$\varepsilon_g = 0 \text{ and}$$

$$\begin{gathered} \textstyle\sum_{i=0}^{d} \varepsilon_i \equiv 0 \bmod p \\ \textstyle\sum_{i=00}^{dd} \varepsilon_i \equiv 0 \bmod p \\ \vdots \\ \textstyle\sum_{i=0\cdots 0}^{d\cdots d} \varepsilon_i \equiv 0 \bmod p. \end{gathered}$$

The commutator of any two elements from P_n also satisfies these conditions when written in normal form, hence D_n is the derived subgroup. It is also possible to show that the pth power of any element from P_n is in this group, so in fact $D_n = \Phi(P_n)$.

We can use this normal form to define another subgroup of P_n in the following way. Form a subset M_n of P_n by taking all elements which when written in normal form satisfy the following conditions:

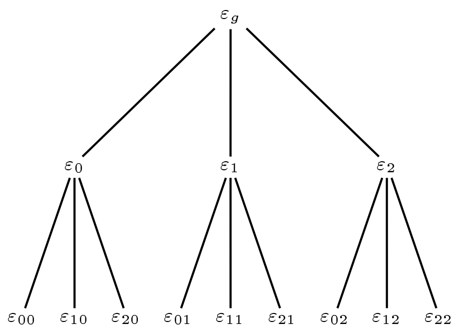
$$\sum_{i=0}^{d} \varepsilon_i \equiv 0 \bmod p$$
$$\sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \bmod p \quad \forall j \in \{0, \ldots, d\}$$
$$\sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \bmod p \quad \forall j \in \{00, \ldots, dd\}$$
$$\vdots$$
$$\sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \bmod p \quad \forall j \in \{0 \cdots 0, \ldots, d \cdots d\}.$$

(Here ij means the digits of i followed by the digits of j.)

The set M_n is a subgroup of P_n. We can see this by induction on n. Let $m_1 := g^{\varepsilon_g}\ g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d}, m_2 := g^{\delta_g}\ g_0^{\delta_0} \cdots g_d^{\delta_d}$ be elements of the set M_2, then $m_1.m_2^{-1} = g^{\varepsilon_g}\ g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d}\ g_d^{-\delta_d} \cdots g_0^{-\delta_0}\ g^{-\delta_g}$. Using the commutator data (1 top line only) and the fact that $\sum_{i=0}^{d} \varepsilon_i \equiv 0 \bmod p$ and $\sum_{i=0}^{d} \delta_i \equiv 0 \bmod p$ we can see that $m_1.m_2^{-1}$ when rearranged to be in normal form satisfies the conditions above and hence M_2 is a group. Now assume that M_n is a group for all $n \leqslant k-1$ and the elements $m_1 := g^{\varepsilon_g}\ g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d} \cdots g_{d \cdots d}^{\varepsilon_{d \cdots d}}$ and $m_2 := g^{\delta_g}\ g_0^{\delta_0} \cdots g_d^{\delta_d} \cdots g_{d \cdots d}^{\delta_{d \cdots d}}$ are in M_k. Now $g^{-\varepsilon_g} m_1$ and $g^{-\delta_g} m_2$ are (by induction) elements of the group $M_{k-1} \times M_{k-1} \times \cdots \times M_{k-1}$ and hence the element $m_1.m_2^{-1} = g^{\varepsilon_g}\ g^{-\varepsilon_g} m_1 g^{\delta_g}\ g^{-\delta_g} m_2$ is in the set M_k.

P_n **acts on weighted trees.** We can associate the elements of P_n in normal form with weighted regular trees with each vertex corresponding to a cycle from the normal form. An element of P_n written in normal form corresponds to a weighted tree, where the weight of each vertex is the power of the cycle that it represents. Let the root of the tree correspond to the p^n-cycle g. The vertices directly beneath g correspond to the level 1 cycles, beneath those the level 2 cycles and so on, arranged so that the support of a cycle is a subset of the support of the cycles occurring above it. The leaf vertices have weights corresponding to powers of the level $n-1$ cycles.

Example. *Elements of the group C_3 Wr C_3 Wr C_3 can be represented by weighted regular trees of height three. An element in normal form from this group is represented by the tree shown below.*



We will be considering the action of P_n on its set of associated trees. If $\alpha, \beta \in P_n$ and T_α is the tree associated with the element α, then $(T_\alpha)\beta = T_{\alpha\beta}$. It is enough to understand how a single cycle acts on the set of trees, as the action of other elements is equivalent to repeated action of single cycles (the action of the element $g\ g_1$ is obviously equivalent to the action of g followed by the action of g_1). The cycle g_i acts on a tree by rotating the subtree that is rooted at the vertex corresponding to the cycle g_i and increasing the weight of that vertex by one. This rotation is actually a cyclic permutation of the subtrees with root vertices immediately beneath the vertex corresponding to the cycle g_i. Figure 1 shows pictorially the element $gg_0^2g_2g_{00}g_{01}g_{11} \in C_3$ Wr C_3 Wr C_3 (left) and its image under the action of the cycle g_1 (right). The calculation is given below.

$$\begin{aligned} gg_0^2(g_2g_{00}g_{01}g_{11}) * g_1 &= gg_0^2\ g_1g_1^{-1}(g_2g_{00}g_{01}g_{11})g_1 \\ &= gg_0^2g_1g_2g_{00}\ g_1^{-1}(g_{01}g_{11})g_1 \\ &= gg_0^2g_1g_2g_{00}g_{11}g_{21} \end{aligned}$$

For a tree T_α, let $w_\alpha(g_i)$ be the weight of the vertex that corresponds to the cycle g_i. To multiply α by another element β of P_n we can consider the multiplication one cycle at a time starting from level 0 and working down to level $n-1$. This gives the result that

$$w_{\alpha\beta}(g) \equiv w_\alpha(g) + w_\beta(g) \bmod p$$

and if i is a k digit number with the digits $i_1, i_2, \cdots\ i_k$, then

$$w_{\alpha\beta}(g_i) \equiv w_\alpha(g_r) + w_\beta(g_i) \bmod p$$

where r is the k digit number $r_1r_2\cdots r_k$ and $r_k \equiv i_k + w_\beta(g) \bmod p$ and $r_j \equiv i_j + w_\beta(g_{i_{j+1}i_{j+2}\cdots i_k}) \bmod p$ for all other j.

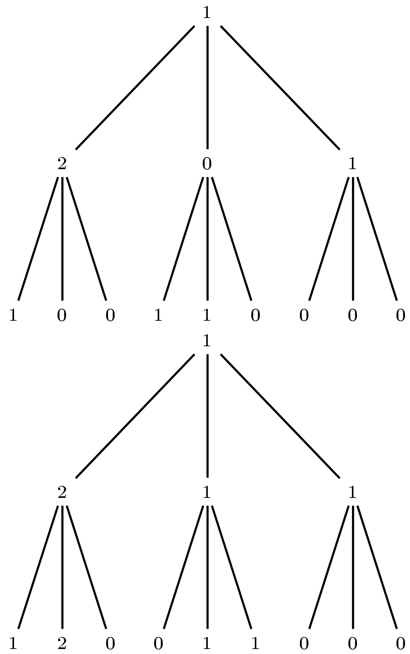


Figure 1

Using this formula and noticing that the identity is associated with the tree where all vertices have zero weight, we get that

$$w_{\alpha^{-1}}(g) \equiv -w_\alpha(g) \bmod p$$

and for i as above

$$w_{\alpha^{-1}}(g_i) \equiv -w_\alpha(g_r) \bmod p$$

where as before r is the k digit number $r_1 r_2 \cdots r_k$ and $r_k \equiv i_k + w_\beta(g)$ and $r_j \equiv i_j + w_\beta(g_{i_{j+1} i_{j+2} \cdots i_k})$ for all other j.

Figure 2 shows the associated trees of an element and its inverse as calculated with the above formula.

Define the *value* of a vertex to be the sum modulo p of the weights of the vertices immediately beneath it, with the stipulation that if a vertex has no branches coming from it (i.e., it is a level $n-1$ vertex), then it has zero value. For an element $\alpha \in P_n$ let $v_\alpha(g_i)$ be the value of the vertex corresponding the cycle g_i in the associated tree T_α.

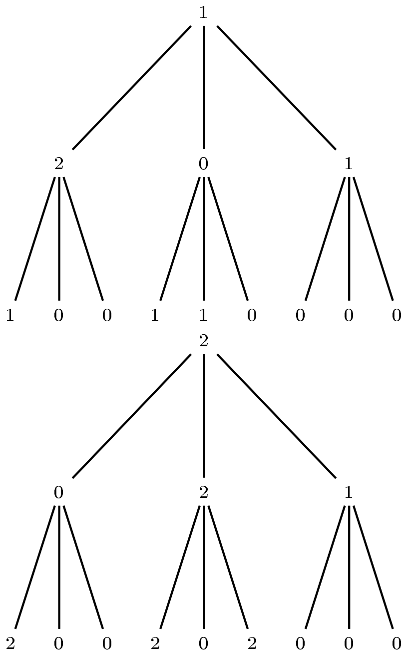


FIGURE 2

Then

$$v_{\alpha\beta}(g) \equiv v_\alpha(g) + v_\beta(g) \bmod p$$

and

$$v_{\alpha\beta}(g_i) \equiv v_\alpha(g_r) + v_\beta(g_i) \bmod p$$

where as above $i = i_1 \cdots i_k$ and r is the k digit number $r_1 r_2 \cdots r_k$ and $r_k \equiv i_k + w_\beta(g)$ and $r_j \equiv i_j + w_\beta(g_{i_{j+1} i_{j+2} \cdots i_k})$ for all other j. From this we get

$$v_{\alpha^{-1}}(g) \equiv -v_\alpha(g) \bmod p$$

and

$$v_{\alpha^{-1}}(g_i) \equiv -v_\alpha(g_r) \bmod p$$

for i and r as before. With this definition the elements of the group M_n are precisely those elements where every vertex has value zero. It can be seen from the above that multiplication and taking inverses preserves this property.

Theorem 12. *If $H \leqslant P_n$ such that $Cyc(H) = P_n$, then $H \leqslant M_n$.*

Proof. This is by induction on n. We have already seen that this is the case for groups of degree p^2 so it suffices to show that the inductive step holds. Assume that $H \leqslant P_k$ and $Cyc(H) = P_k$ implies that $H \leqslant M_k$ for all $k \leqslant n-1$. Now let $H \leqslant P_n$ be such that $Cyc(H) = P_n$ hence

$$Cyc(H^{\Delta_0}_{\{\Delta_0\}}) = P_n{}^{\Delta_0}_{\{\Delta_0\}} \cong P_{n-1}$$

but we know from our assumption that this means

$$H^{\Delta_0}_{\{\Delta_0\}} \leqslant M_{n-1}.$$

The group $H^{\Delta_0}_{\{\Delta_0\}}$ is in fact the group generated by the cycles g_a, where a represents a k digit number $(1 \leqslant k \leqslant n-1)$ in base p with the last digit being 0. By considering this and the fact that $H^{\Delta_i}_{\{\Delta_i\}} \leqslant M_{n-1}$ for all $i \in \{0, 1, \ldots, d\}$ we obtain that elements of H written in normal form must satisfy the following conditions:

$$\begin{array}{ll} \sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \pmod{p} & \forall j \in \{0, \ldots, d\} \\ \sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \pmod{p} & \forall j \in \{00, \ldots, dd\} \\ & \vdots \\ \sum_{i=0}^{d} \varepsilon_{ij} \equiv 0 \pmod{p} & \forall j \in \{0\cdots 0, \ldots, d\cdots d\}. \end{array}$$

Finally if we consider $H^{\Omega_{n-1}}$, then we know that

$$Cyc(H^{\Omega_{n-1}}) = P_n^{\Omega_{n-1}} \cong P_{n-1},$$

hence $H^{\Omega_{n-1}} \leqslant M_{n-1}$ and we have the final condition.

$$\sum_{i=0}^{d} \varepsilon_i \equiv 0 \pmod{p}.$$

□

Theorem 13. *If $H \leqslant M_n$ is transitive, then $Cyc(H) = P_n$.*

Before proving this we will first need to show that if an element $h \in M_n$ (when written in normal form) has $\varepsilon_g \neq 0$, then h is a p^n-cycle. Looking at the element

$$h := g^{\varepsilon_g}\, g_0^{\varepsilon_0}\, g_1^{\varepsilon_1} \,\cdots\, g_d^{\varepsilon_d}\, g_{00}^{\varepsilon_{00}} \,\cdots\cdots\, g_{dd\cdots d}^{\varepsilon_{dd\cdots d}}$$

from M_n we see that if $\varepsilon_g = 0$, then h will fix the blocks in Ω_1 set-wise, and therefore cannot be a p^n-cycle. By considering the possible choices for ε_i we can see that the group M_n has order

$p^{1+(p-1)+(p^2-p)+\cdots+(p^{n-1}-p^{n-2})} = p^{p^{n-1}}$ and the number of elements h with $\varepsilon_g \neq 0$ is

$$\left(\frac{p-1}{p}\right) p^{p^{n-1}}.$$

It now suffices to show that the group M_n contains this many p^n-cycles. Let c be a p^n-cycle then the centralizer of c in M_n is $\langle c \rangle$ (we have seen above that commutators of p^n cycles with other elements are non trivial). If we consider the group M_n acting on itself by conjugation, then the centralizer of c is the stabilizer under this action and the orbit is a conjugacy class. The orbit-stabilizer theorem gives us that the conjugacy classes containing c will be of size $p^{p^{n-1}-n}$. Similarly this will be the size of all conjugacy classes containing p^n-cycles.

Lemma 14. *The elements $g, g^2, \cdots g^{p-1}$ are in distinct conjugacy classes of M_n.*

Proof. Assume for contradiction that $g^\alpha = g^r$ where $\alpha \in M_n$ and $r \in \{2, 3, \ldots, p-1\}$. Then

$$g^{(\alpha^n)} = g^{r^n}.$$

Let k be the least integer such that $r^k \equiv 1 (\mathrm{mod}\ p^n)$ (such a k does exist as the Fermat-Euler Theorem [3] gives $r^{\varphi(p^n)} \equiv 1 (\mathrm{mod}\ p)$ where $\varphi(n)$ is the Euler phi function, counting numbers less than and prime to n. On prime powers $\varphi(p^n) = p^n - p^{n-1}$). Now we have

$$g^{(\alpha^k)} = g^{r^k} = g$$

and hence α^k is in the centralizer of g in M_n which is $\langle g \rangle$, but $\alpha \notin \langle g \rangle$. If $\alpha^{k_1} = g$ for $k_1 < k$, then this would contradict our choice of k as minimal such that $r^k \equiv 1 (\mathrm{mod}\ p^n)$, hence $\alpha^k = g$. The element α must therefore be a power of g and this contradicts the assumption that $r \neq 1$. □

There are $(p-1)p^{n-1}$ elements of the form

$$\lambda^{-1} g^{\varepsilon_g} \lambda \tag{3}$$

where $\lambda := g_0^{\varepsilon_0}\, g_{00}^{\varepsilon_{00}}\, g_{01}^{\varepsilon_{00}} \cdots g_{0d}^{\varepsilon_{00}} \cdots\cdots g_{00\cdots 0}^{\varepsilon_{00\cdots 0}}\, g_{00\cdots 1}^{\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots 0}}$

for $\varepsilon_g \in \{1, 2, \ldots, p-1\}$ and all other $\varepsilon \in \{0, 1, 2, \ldots, p-1\}$.

Lemma 15. *Elements of the form* (3) *are members of the group* M_n.

Proof. The element $g_0^{-\varepsilon_0}\ g^{\varepsilon_g}\ g_0^{\varepsilon_0}$ when written in normal form is $g^{\varepsilon_g}\ g_{\varepsilon_g}^{-\varepsilon_0}\ g_0^{\varepsilon_0}$ which is an element of M_2. Assume for induction that the lemma holds for the group M_n for $n \leqslant k-1$. Consider $\lambda^{-1} g^{\varepsilon_g} \lambda$ with λ as above, by induction this is equal to

$$g_{00\cdots 0}^{-\varepsilon_{00\cdots 0}}\ g_{00\cdots 1}^{-\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{-\varepsilon_{00\cdots 0}} g^{\varepsilon_g}\gamma\ g_{00\cdots 0}^{\varepsilon_{00\cdots 0}}\ g_{00\cdots 1}^{\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots 0}}$$

with $g^{\varepsilon_g}\gamma \in M_{k-1}$. Rearranging this we get

$$g^{\varepsilon_g} g_{\varepsilon_g 0\cdots 0}^{-\varepsilon_{00\cdots 0}}\ g_{\varepsilon_g 0\cdots 1}^{-\varepsilon_{00\cdots 0}} \cdots g_{\varepsilon_g 0\cdots d}^{-\varepsilon_{00\cdots 0}} \gamma\ g_{00\cdots 0}^{\varepsilon_{00\cdots 0}}\ g_{00\cdots 1}^{\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots 0}}$$

$$= g^{\varepsilon_g}\gamma g_{\varepsilon_g 0\cdots 0}^{-\varepsilon_{00\cdots 0}}\ g_{\varepsilon_g 0\cdots 1}^{-\varepsilon_{00\cdots 0}} \cdots g_{\varepsilon_g 0\cdots d}^{-\varepsilon_{00\cdots 0}} g_{00\cdots 0}^{\varepsilon_{00\cdots 0}}\ g_{00\cdots 1}^{\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots 0}}$$

which is in the group M_k. □

We will now see that any two elements of this form are not conjugate in M_n. Assume that two elements $\alpha^{-1} g^a \alpha, \beta^{-1} g^b \beta$ of the form (3) are in the same conjugacy class, where

$$\alpha := g_0^{\varepsilon_0}\ g_{00}^{\varepsilon_{00}}\ g_{01}^{\varepsilon_{00}} \cdots g_{0d}^{\varepsilon_{00}} \cdots\cdots g_{00\cdots 0}^{\varepsilon_{00\cdots 0}}\ g_{00\cdots 1}^{\varepsilon_{00\cdots 0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots 0}} \quad \text{and}$$

$$\beta := g_0^{\delta_0}\ g_{00}^{\delta_{00}}\ g_{01}^{\delta_{00}} \cdots g_{0d}^{\delta_{00}} \cdots\cdots g_{00\cdots 0}^{\delta_{00\cdots 0}}\ g_{00\cdots 1}^{\delta_{00\cdots 0}} \cdots g_{00\cdots d}^{\delta_{00\cdots 0}}.$$

Then there exists some $\gamma \in M_n$ such that

$$\beta\gamma^{-1}\alpha^{-1} g^a \alpha\gamma\beta^{-1} = g^b.$$

The proof of Lemma 14 gives us that $a = b$ and $\alpha\gamma\beta^{-1} \in \langle g \rangle$ and hence $\gamma = \alpha^{-1} g^c \beta$ for some $c \leqslant p^n$.

The element γ is in the group M_n and hence all vertices of its associated tree have zero value. From above we have that

$$\begin{aligned} 0 = v_\gamma(g) \quad &= v_{\alpha^{-1}\ g^c \beta}(g) \\ &\equiv v_{\alpha^{-1}}(g) + v_{g^c}(g) + v_\beta(g) \ (\bmod p) \\ &\equiv -\varepsilon_0 + 0 + \delta_0 \ (\bmod p) \end{aligned}$$

and hence $\varepsilon_0 = \delta_0$.

Now let i be a $k-1$ digit number

$$\begin{aligned} v_{\alpha^{-1}\ g^c}(g_i) \quad &\equiv v_{\alpha^{-1}}(g_r) + v_{g^c}(g_i) \ (\bmod p) \qquad \forall i \\ &\equiv -\underbrace{\varepsilon_{0\cdots 0}}_{k \text{ zeros}} + 0 \ (\bmod p) \end{aligned}$$

(here r is as defined just after Figure 1, however in the tree corresponding to α^{-1}, the value of all level $k-1$ vertices is the same) therefore

$$\begin{aligned} 0 = v_\gamma(g_i) &= v_{\alpha^{-1}\ g^c\beta}(g_i) \\ &\equiv v_{\alpha^{-1}\ g^c}(g_r) + v_\beta(g_i) \pmod p \\ &\equiv -\underbrace{\varepsilon_{0\cdots0}}_{k\text{ zeros}} + \underbrace{\delta_{0\cdots0}}_{k\text{ zeros}} \pmod p \end{aligned}$$

and hence $\underbrace{\varepsilon_{0\cdots0}}_{k\text{ zeros}} = \underbrace{\delta_{0\cdots0}}_{k\text{ zeros}}$ for all $k \in \{1, \ldots, n\}$. So we have $\alpha = \beta$.

We have now shown that all elements of the form 3 are in distinct conjugacy classes, hence there are at least $p^{n-1}(p-1)$ conjugacy classes. This gives at least

$$p^{n-1}(p-1)p^{p^{n-1}-n} = \left(\frac{p-1}{p}\right)p^{p^{n-1}}$$

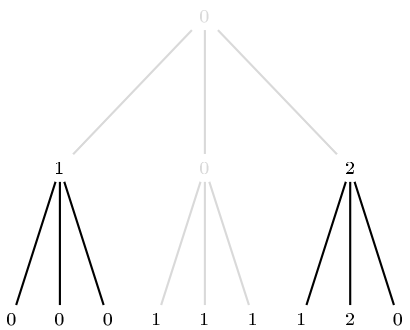
p^n-cycles in M_n and therefore all h with $\varepsilon_g \neq 0$ must be p^n-cycles.

Lemma 16. $Cyc(M_n) = P_n$.

Proof. The p^n-cycle g is an element of M_n and we therefore have $P_n \leq Cyc(M_n)$. It suffices to prove that if α is an element of M_n, then all cycles involved in α are elements of P_n. Let

$$\mathrm{Id} \neq \alpha = g^{\varepsilon_g}\ g_0^{\varepsilon_0}\ g_1^{\varepsilon_1}\ \cdots\ g_d^{\varepsilon_d}\ g_{00}^{\varepsilon_{00}}\ \cdots\cdots\ g_{dd\cdots d}^{\varepsilon_{dd\cdots d}} \in M_n.$$

If $\varepsilon_g \neq 0$, then the above argument tells us that α is a p^n-cycle, which is clearly in P_n as α is. Let T_α be the tree associated with α. If $w_\alpha(g)(:= \varepsilon_g) = 0$, then remove the top vertex and all adjacent edges from T_α. Next look at the level 1 vertices and again remove any that have weight zero along with their adjacent edges. Any level 1 vertices with non zero weight are now roots of subtrees of T_α, all vertices beneath these cannot now be removed. Continue to remove vertices of weight zero until T_α has been partitioned into subtrees each of which has a root of non-zero weight.



The tree shown, T_α, is composed of five subtrees, two of height 1 and three of height 0. The element α is the product of the elements associated with these subtrees.

As these subtrees are disjoint and each have a root of non-zero weight they correspond to disjoint single cycles in M_n. Now the element α is the product of these disjoint cycles, as each one is an element of M_n they are also elements of P_n and we are done. $\square$

Proof of Theorem 13. If H is transitive, then there is some $h \in H$ such that when h is written in normal form, the power of g is non zero. Other cycles in the normal form fix the blocks of Ω_1. By the above argument this element h is then a p^n-cycle. The cyclizer of the cyclic group $\langle h \rangle$ is P_n hence $Cyc(H) \geqslant P_n$. We have already seen that $Cyc(H) \leqslant P_n$ and so they must be equal. $\square$

Theorem 17. *If H is a transitive p-group of degree p^n and $Cyc(H) \neq P_n$, then $|Cyc(H)|$ is even. This means that $Cyc^2(H)$ is a primitive group containing a transposition and is therefore S_{p^n}.*

Before proving this it will be useful to note the following. If G is a transitive group with a non-trivial block system consisting of blocks $\Delta_1, \Delta_2, \ldots, \Delta_n$, then let G^{Δ} denote the action of G on the set $\{\Delta_i | 1 \leqslant i \leqslant n\}$. There is an obvious surjective homomorphism from G onto G^{Δ} and hence $|G^{\Delta}| \mid |G|$. It is well known that the order of a stabilizer divides the order of the group. Also note that $Cyc(G^{\Delta}) = Cyc(G)^{\Delta}$. Similarly if a group G acts on Ω and $\Gamma \subset \Omega$, then $Cyc(G_{\{\Gamma\}}) = Cyc(G)_{\{\Gamma\}}$.

Proof. Assume that $H \leqslant P_n$ but $Cyc(H) \neq P_n$, then H contains some element involving a cycle c which is not an element of P_n. If a cycle c is involved in an element of P_n, then it is a p^k-cycle for some k. If it also does not break any of the block systems on P_n, then in particular it does not break the blocks of size p^k in the the block system Ω_{n-k}. Therefore $\mathrm{Supp}(c) = \Delta_i$ for some $n-k$ digit i and c must be a power of the cycle g_i and is therefore an element of the group P_n. It follows from this that our cycle c which is involved in an element of P_n but not itself in the group P_n, must break at least one of the block systems $\Omega_1, \ldots, \Omega_{n-1}$.

Choose r to be the least number such that $\Omega_0, \Omega_1, \ldots, \Omega_r$ are all block systems of $Cyc(H)$ but Ω_{r+1} is not, and let $r+s$ be the least number greater than r such that Ω_{r+s} *is* a block system of $Cyc(H)$ (note that r and s do exist as Ω_0 and Ω_n are trivially block systems). Now we consider the group $Cyc(H)_{\{\Delta_i\}}^{\Omega_{r+s}|_{\Delta_i}}$ for a fixed $\Delta_i \in \Omega_r$, where $\Omega_{r+s}|_{\Delta_i}$ is the set of $\Delta_j \in \Omega_{r+s}$ such that $\Delta_j \subset \Delta_i$.

Note. This group is the set-wise stabiliser of a level r block Δ_i, acting the set of level $r+s$ blocks that are subsets of Δ_i. Hence it has degree p^s. The only non-trivial blocks this group could have, would correspond to non-trivial P_n-blocks from levels $r+1$ to $r+s-1$, but we have chosen r and s so that this cannot happen, hence this group is primitive. The group H is a p-group, therefore the subgroup $H_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i}$ is also a p-group and hence contains an element which involves a p-cycle. This p-cycle is in $Cyc(H_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i}) = Cyc(H)_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i}$.

By Lemma 1 primitive groups of degree p^s with $s \geqslant 2$ which contain a p-cycle are either alternating or symmetric. The group $Cyc(H)_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i}$ is the cyclizer of a p-group, it is primitive and contains a p-cycle, therefore

$$Cyc(H)_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i} \cong A_{p^s}$$

The important point is that the order of this group is even. Now we can see that

$$2 \mid |A_{p^s}| = |Cyc(H)_{\{\Delta_i\}}^{\Omega_{r+s}|\Delta_i}| \mid |Cyc(H)_{\{\Delta_i\}}| \mid |Cyc(H)|$$

and we are done. □

If $H \leqslant C_3$ Wr C_3 Wr C_3 and $Cyc(H) \neq C_3$ Wr C_3 Wr C_3, then there are three cases. Either Ω_1 is not a block system in $Cyc(H)$ or Ω_2 is not a block system of $Cyc(H)$ or neither of them are. In the first case $Cyc(H) = A_9$ Wr C_3, second $Cyc(H) = C_3$ Wr A_9 and third $Cyc(H) = A_{27}$. Obviously in all cases $Cyc^2(H) = S_{27}$.

Corollary 18. *Up to isomorphism of permutation groups, the finite groups G for which $Cyc^2(G) \neq Cyc^3(G)$ are precisely the transitive subgroups of the groups M_n for $n \in \mathbb{N}, n \geqslant 2$.*

4. CLASSIFICATION OF FINITE GROUPS

We are now in a position to classify finite transitive groups, other than 2-groups, according to the length of their cyclizer sequence. We will also see why the classification of 2-groups is an open problem.

Primitive groups. From §1 we have that the cyclizer of a primitive group that is not prime cyclic is S_n or A_n. A primitive group of even order must contain an element that involves a transposition hence its cyclizer is S_n. A non-prime cyclic primitive group, G, of odd order will only involve cycles of odd length and hence $Cyc(G) = A_n$, it follows that $Cyc^2(G) = S_n$.

We have shown that a primitive group has a cyclizer sequence of length 1 if it has even order and length 2 if it has odd order.

Imprimitive groups (other than p-groups). By Theorem 2 if G is imprimitive but not a p-group, then $Cyc(G)$ is primitive. Hence if $|G|$ is even, then $Cyc(G)$ contains a transposition and is S_n by Lemma 1. If $|G|$ is odd, then $Cyc(G) \leq A_n$ and by §1, $Cyc^2(G) = S_n$.

So an imprimitive group, which is not a p-group has a cyclizer sequence of length 1 if it has even order and of length 2 if it has odd order (as with primitive groups).

p-groups (for p an odd prime). §2 gives us that a p-group G has a cyclizer sequence of length 3 if and only if it is a transitive subgroup of the group M_n. If $G \not\leq M_n$ then it has a cyclizer sequence of length two as $Cyc(G) \leq A_{p^n}$.

So a p-group G of degree p^n (with p odd) has a cyclizer sequence of length 3 if it is a transitive subgroup of the group $M_{(p,n)}$ and of length 2 otherwise.

2-groups. If G is a 2-group, then either $Cyc(G) = S_n$ or $Cyc(G)$ is imprimitive and $Cyc^2(G) = S_n$ as it is primitive and contains a transposition. We are now required to determine when $Cyc(G)$ is imprimitive. Through a similar argument to that in §2 we can see that $Cyc(G) = C_2 \text{ Wr } C_2 \cdots \text{ Wr } C_2$ when G is a subgroup of $M_{(2,n)}$ for some n. However these are not the only groups to have $Cyc(G)$ imprimitive. For example the group of quarternions in its right regular representation has the following cyclizer sequence.

$$Q \mapsto C_2 \text{ Wr } S_4 \mapsto S_8.$$

In order to complete this classification we need to answer the following question.

For which imprimitive groups G is $Cyc(G)$ also imprimitive?

In other words we want to know which imprimitive G have a system of non-trivial blocks that is respected by all cycles involved in elements of the group. We leave this as an open question and hence the classification is not quite complete.

We summarize the classification information in Figure 3.

Cyclizer length	*Groups*
0	• C_p for p prime • S_n
1	• Primitive groups of even order • Imprimitive groups of even order *(except certain 2-groups)*
2	• Primitive groups of odd order • Imprimitive groups of odd order except those specified in §2 • 2-groups G such that $Cyc(G) \neq S_n$
3	• p-groups ($p \neq 2$) as specified in §2

FIGURE 3. *A partial classification of groups according to the length of their cyclizer sequence*

ACKNOWLEDGEMENT

Some of this work forms part of [2]. At the time, Ceri Fiddes was supported by a Departmental Studentship from the Mathematics Department of the University of Bath.

REFERENCES

[1] P. J. Cameron, Cycle-closed permutation groups, Journal of Algebraic Combinatorics (1996), 315–322.
[2] C. C. Fiddes, The cyclizer function on permutation groups, Ph.D thesis, University of Bath, 2003.
[3] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, Oxford University Press (1979).
[4] A. G. Williamson, On primitive permutation groups containing a cycle, Math. Z. 130 (1973), 159–162.

Geoff Smith,
Department of Mathematics,
University of Bath,
Claverton Down,
Bath BA2 7AY, UK