The cyclizer function on permutation groups

Fiddes, Ceridwyn

Award date:
2003

Awarding institution:
University of Bath

The Cyclizer Function on Permutation Groups

Submitted by

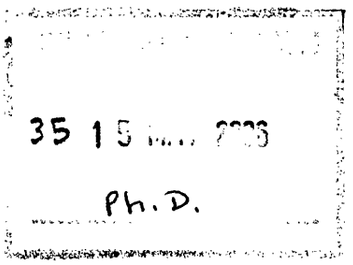
Ceridwyn Fiddes

for the degree of PhD
of the

University of Bath

2003

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346


35 15
Ph.D.

Abstract

Let G be a transitive permutation group acting on a set Ω. A cycle c is involved in a permutation g if and only if gc^{-1} fixes all points of Supp(c). We define a function $Cyc(G)$ which takes the permutation group G to the group generated by all cycles involved in elements of G. A group is called **cycle closed** if it satisfies $Cyc(G) = G$. We will look at the problem of determining the least k such that $Cyc^k(G) = Cyc^{k+1}(G)$ (where $Cyc^1(G) = Cyc(G)$ and $Cyc^{i+1}(G) = Cyc(Cyc^i(G))$) for finite and infinite groups. When Ω is a finite set of size n, it is shown that for all groups other than $C_p := \langle (1, 2, ..., p) \rangle$ for prime p, we have that $Cyc^3(G) = S_n$. Groups such that $Cyc^2(G) \neq S_n$ are characterised. We look at the cyclizer function on certain infinite groups and give examples of cycle closed permutation groups on infinite sets.

Contents

Introduction

In a permutation group each element is a product of disjoint cycles. In this thesis we take the set of cycles that occur in the cycle decomposition of elements of a group and use this set to generate a new group. The inspiration for this came from looking at the set of cycles involved in elements of a group, which is the union of the sets acted on in Parker's Lemma (Theorem 1.4). Chapter 1 recalls standard definitions from group theory and introduces some possibly non-standard notation before formally defining the cyclizer function, which takes a group to the group generated by its cycles. We then begin by looking at transitive finite groups and the sequences produced by repeated applications of the cyclizer function. It is quickly established that all but cyclic groups of prime order in their natural representation produce a sequence of groups terminating with the symmetric group. The question then becomes how long does it take to get to the symmetric group. The number of repeated applications of the cyclizer function is bounded by considering imprimitivity and by noting that the function takes primitive groups to primitive groups. The rest of the consideration of finite groups is concerned with establishing which groups give rise to sequences of maximal length.

For infinite groups the definition of cyclizer needs adjusting to ensure we

get an analogous sequence of groups. We then consider the sequences resulting from an infinite cyclic group and an infinite dihedral group. The thesis ends with some more observations about cyclizers of infinite groups. In the infinite case it has not been possible to bound the length of the sequence.

Some of the results contained in this thesis also appear in a paper by Peter Cameron [2]. I discovered the existence of this paper only after having begun the work contained in this thesis. Unfortunately, on finding the paper I discovered that the work I had completed on finite groups and the first three groups in the cyclizer sequence of the infinite cyclic group had already been published. Subsequent work extended the ideas introduced in Cameron's paper. The paper looks firstly at finite groups, showing that a cycle-closed group can be reached after taking cyclizers at most three times. Cameron then goes on to look at infinite groups, defining four types of cyclizer and giving some analogues of the finite results. The work contained in this thesis was done completely independently except where stated. At the end of his paper Cameron poses several open problems, one of which ("which finite transitive groups G satisfy $Cyc^2(G) \neq Cyc^3(G)$?") is answered by Chapter 3 of this thesis. Another of the open problems is to prove or find a counter example to the conjecture that $Cyc^3(G) = Cyc^4(G)$ for all groups. This thesis and Cameron's paper show that this is true for finite groups and infinite cyclic groups. However this thesis makes no further progress in answering the question, which remains open. Interestingly Cameron notes that this work has an application. A paper [8] by C.Lenart and N.Ray on Hopf algebras quotes and makes use of Theorem 2.3.

The main body of this work is followed by two appendices. The first is an acknowledgement of the substantial role that GAP [4] has played in the research behind this thesis. Although no results depend on them, the calculations performed helped enormously in formulating and checking hypotheses. The second appendix is a short unrelated topic that resulted from a preliminary research project.

I am deeply indebted to both my supervisor Geoff Smith, for his help and humour, and my partner Daniel Holley, for his encouragement and care (and for trying very hard to remember what a group is). I must also acknowledge Peter Neumann's helpful communication that inspired the proof of Theorem 2.7.

Chapter 1

Definitions and notation

Section 1.1 is an outline of the group theoretic prerequisites to this thesis. The details of this section will be very familiar to anyone with a knowledge of group theory, however the reader is encouraged to read this as some notation may be nonstandard. The reader requiring more details is referred to Dixon [3]. This chapter also introduces some notation from graph theory. We then look at Parker's Lemma and introduce the cyclizer function on permutation groups.

1.1 Permutation groups

A **permutation** π, of a set Ω is a bijection from Ω to itself. Let $\mathrm{Sym}(\Omega)$ denote the set of all bijections on Ω. Composition of functions gives us a binary operation on this set, under which the set $\mathrm{Sym}(\Omega)$ becomes a group, the **symmetric group**. When Ω is finite of size n we may also use the notation S_n for $\mathrm{Sym}(\Omega)$. A permutation $\pi : \Omega \mapsto \Omega$ can be written as a product of disjoint cycles where the occurrence of the cycle $(\alpha_1, \alpha_2, ..., \alpha_n)$ $(\alpha_i \in \Omega)$ in the

cycle decomposition of π tells us that

$$(\alpha_i)\pi = \begin{cases} \alpha_{i+1} \text{ if } i \in \{1, ..., n-1\} \\ \alpha_1 \quad \text{if} \qquad\qquad i = n \end{cases}.$$

Points of Ω occurring in cycles of length 1 are fixed points of the permutation and these cycles are usually omitted from the cycle decomposition. The **support** of a permutation π, written $\text{Supp}(\pi)$, is the set $\{\omega \in \Omega | (\omega)\pi \neq \omega\}$. A cycle with support of size k is a k-cycle. Cycles of length 2 are known as transpositions. Permutations of finite sets (elements of S_n for $n \in \mathbb{N}$) are products of transpositions. A permutation is said to be **even** if it can be written as a product of an even number of transpositions and **odd** if it can be written as the product of an odd number of transpositions. It is well known that permutations cannot be both even and odd. The set of even permutations on n points is a subgroup of S_n, called the **alternating group** and is written A_n. A group G is said to be a **permutation group** on the set Ω if G is a subgroup of $\text{Sym}(\Omega)$. The **degree** of G is the size of the set Ω ($|\Omega|$) (where Ω is a set of minimal size) and the **order** of G is the size of the group ($|G|$).

Let G be any group, then an **action** of G on a set Ω is a map $a : \Omega \times G \mapsto \Omega$ where $a(\omega, g)$ is more commonly written $(\omega)g$. The map a must satisfy the conditions that for all $\omega \in \Omega$ $(\omega)\text{Id} = \omega$ and $(\omega)(gh) = ((\omega)g)h$ for all $g, h \in G$. If such a map exists, then G is said to **act** on Ω and Ω is called a **G-set**. This map yields a homomorphism $\tau : G \to \text{Sym}(\Omega)$ by $(g)\tau : \omega \mapsto (\omega)g$ for all $g \in G$. The image of τ ($\text{Im}(\tau)$) is a subgroup of $\text{Sym}(\Omega)$ and is therefore a permutation group. If τ is injective, then G is isomorphic to the permutation

group $\mathrm{Im}(\tau)$ and is said to act **faithfully** on Ω. All groups are isomorphic to permutation groups and in particular all groups can be made to act faithfully on themselves via $(h)g := h * g$ (where $*$ is group multiplication). This is a faithful action of G on the set of elements of G. This representation of G is the **right regular representation**, regular referring to the fact that for any two points of the set (in this case also the group) there is a unique element of the group taking one to the other. A group can also act on itself via **conjugation**, that is $(h)\ g = g^{-1}\ h\ g$. We will use the notation h^g to mean conjugation of h by g.

A permutation group G is **transitive** if for all $\alpha, \beta \in \Omega$ there exists an element $g \in G$ such that $(\alpha)g = \beta$. If Ω is a G-set, then so is $\Omega^k := \underbrace{\Omega \times \cdots \times \Omega}_{k \text{ times}}$, G acts naturally on Ω^k by

$$(\omega_1, \ldots, \omega_k)g = ((\omega_1)g, \ldots, (\omega_k)g).$$

Let $\Omega^{[k]} \subseteq \Omega^k$ be the set of ordered k-tuples $(\omega_1, \ldots, \omega_k)$ consisting of distinct elements $\omega_i \in \Omega$. If the action of G on $\Omega^{[k]}$ is transitive, then G is said to act **k-transitively** on Ω. Note that k-transitivity implies k'-transitivity for $k' \leq k$.

If a group G acts on a set Ω, then G also acts on the power set of Ω (the set of all subsets of Ω) by $(\Delta)g = \{(\delta)g \mid \delta \in \Delta\}$ for $\Delta \subseteq \Omega$. If for all $g \in G$ the sets $(\Delta)g$ and Δ are either disjoint or equal, then Δ is said to be a **G-block**. Obviously the whole set Ω is a block for all group actions, as are all subsets of size 1, these are trivial blocks. If a group action has no non-trivial blocks,

then it is **primitive**, otherwise G is **imprimitive**. Note that if G acts on a finite set Ω and the action is imprimitive and transitive, then the size of each block must divide the size of Ω, as every block is associated with a system of blocks that partition Ω into sets of equal size. Let $S := \{\Delta_1, \cdots, \Delta_k\}$ be such a system of blocks then there exists a homomorphism from G into a permutation group on S by considering how elements of G move the blocks in S. The image of this homomorphism is labelled G^S.

If $T = \{g_1, \ldots, g_k\}$ is a set of elements of a group G, then $\langle T \rangle$ is the smallest subgroup of G which contains g_i for $i \in \{1, \ldots, k\}$. The elements of T are said to **generate** the group $\langle T \rangle$. For any group G a set of generators for G is a set T such that $\langle T \rangle = G$. A word in the elements $\{g_1, \ldots, g_k\}$ is a string $s_1 \cdots s_l$ where each $s_j = g_i^{\varepsilon_j}$ with $\varepsilon_j \in \mathbb{Z}$. The **commutator** of two elements $g, h \in G$ is the product $g^{-1}\ h^{-1}\ g\ h$ written $[g, h]$. It will be useful to know commutators of generating elements when rewriting words in these generators via $gh = hg[g, h]$. The set of commutators generate a subgroup of G this is the **derived subgroup** and is denoted G'.

The **stabilizer** of a point $\alpha \in \Omega$ is the subgroup of G consisting of all elements which fix α (i.e all $g \in G$ such that $(\alpha)g = \alpha$). This subgroup will be denoted G_α. Similarly we define the point-wise stabilizer of a subset $\Gamma \subseteq \Omega$ to be the group of elements that fix all points of Γ, written G_Γ (so $G_\Gamma = \cap_{\alpha \in \Gamma} G_\alpha$). The set-wise stabilizer of Γ is the group of $g \in G$ such that $(\gamma)g, (\gamma)g^{-1} \in \Gamma$ for all $\gamma \in \Gamma$, and this is written $G_{\{\Gamma\}}$. By ignoring the action G has on points of Ω that are not in the set Γ we can define a map from $G_{\{\Gamma\}}$ to a group acting on Γ, the image of this map is $G^\Gamma_{\{\Gamma\}}$.

For a point $\alpha \in \Omega$ the **orbit** of α, $\mathrm{Orb}(\alpha)$, is the set $\{(\alpha)g \mid g \in G\}$. Orbits under the action of G partition the set Ω. There is a bijective map from the cosets of G_α to $\mathrm{Orb}(\alpha)$ which maps $G_\alpha x$ to $(\alpha)x$ and hence $|\mathrm{Orb}(\alpha)| \cdot |G_\alpha| = |G|$, known as the **orbit-stabilizer theorem**. If G is transitive, the orbit-stabilizer theorem gives the result that $|\Omega| \Big| |G|$.

If G acts on Ω, then there is also a natural action by conjugation on the subgroups of G. If $H \leqslant G$, then the conjugate of H by g is the set

$$H^g := \{g^{-1}hg | h \in H\}.$$

The stabilizer of the group H under this action is called the **normalizer** of H in G and is written $N_G(H)$.

An **automorphism** of a group G is an isomorphism $\pi : G \to G$. The automorphisms of G form a group Aut G under composition of functions. An automorphism π is an **inner automorphism** if there exists some $x \in G$ such that $(g)\pi = g^x$ for all $g \in G$. The inner automorphisms form a set Inn G. In fact Inn G is a normal subgroup of Aut G. If $H \leq G$ is invariant under the action of every inner automorphism ($H^x = H$ for all $x \in G$), then H is a **normal** subgroup of G. If H is invariant under all automorphisms of G ($(H)\pi = H$ for all $\pi \in$ Aut G), then the subgroup H is said to be **characteristic** .

If Ω is a infinite set of cardinality λ, then $\mathrm{Sym}(\Omega)$ is a group of order 2^λ. For an infinite cardinal k the **bounded symmetric group**, $BS(\Omega, k)$ on Ω is the group of permutations in $\mathrm{Sym}(\Omega)$ with support of size less than k. The group $BS(\Omega, \aleph_0)$ is the group of permutations with finite support, these

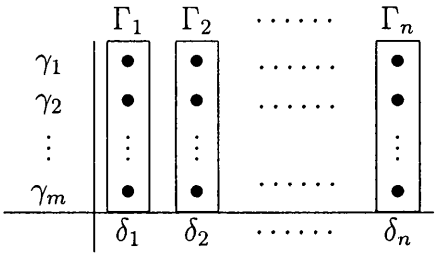


Figure 1.1: *The set* $\Gamma \times \Delta$ *can be thought of as* $|\Delta|$ *copies of* Γ.

permutations are **finitary** permutations and this group is also known as the finitary symmetric group or $FS(\Omega)$. All finitary permutations are either odd or even. The alternating group ($\mathrm{Alt}(\Omega)$) on an infinite set is the subgroup of $FS(\Omega)$ consisting of even permutations.

Let G and H be permutation groups acting on finite sets $\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ and $\Delta := \{\delta_1, \ldots, \delta_n\}$ respectively. The group $B := \underbrace{G \times G \times \cdots \times G}_{n \text{ times}}$ can act on $\Gamma \times \Delta$ by

$$((\gamma_i, \delta_j))(g_1, \ldots, g_n) = ((\gamma_i)g_j, \delta_j).$$

Let $\Gamma_i := \{(\gamma_j, \delta_i) | 1 \leq j \leq m\} \subset \Gamma \times \Delta$ as illustrated in figure 1.1. Each copy of G in B acts on one of the columns in the diagram. The group H also acts on $\Gamma \times \Delta$ (written $H^{\Gamma \times \Delta}$) via

$$((\gamma_i, \delta_j))h = (\gamma_i, (\delta_j)h).$$

in this action H is permuting the Γ_i's ($(\Gamma_i)h = \Gamma_j$ when $(\delta_i)h = \delta_j$). The **wreath product** of G by H, written G Wr H is the group $B \cdot H^{\Gamma \times \Delta}$. The group B is the **base group** of the wreath product, G is called a **base factor** group and H is the **complement** group of the wreath product. The group

G Wr H has a block system, S, of $|\Delta|$ blocks each of size $|\Gamma|$. The action of G Wr H on any one of these blocks is isomorphic to the action of G on Γ and $(G \text{ Wr } H)^S \cong H^\Delta$.

Lemma 1.1. *Wreath products are associative i.e for permutations groups G, H and K $(G\ Wr\ H)\ Wr\ K \cong G\ Wr\ (H\ Wr\ K)$.*

Proof: Let G, H and K be groups acting on sets Γ, Δ and Ω respectively and consider the group $(G \text{ Wr } H) \text{ Wr } K$. This group has a block system $S := \{\Gamma_1, \Gamma_2, ..., \Gamma_n\}$ where $n = |\Delta| \cdot |\Omega|$ and $|\Gamma_i| = |\Gamma|$ for all i such that

$$((G \text{ Wr } H) \text{ Wr } K)^{\Gamma_i}_{\{\Gamma_i\}} \cong G.$$

Now consider the action of the group on the set S. The group $(G \text{ Wr } H)^S$ is isomorphic to H therefore

$$((G \text{ Wr } H) \text{ Wr } K)^S \cong H \text{ Wr } K.$$

So by the above we have that $(G \text{ Wr } H) \text{ Wr } K \cong G \text{ Wr } (H \text{ Wr } K)$. □

The **exponent** of a group G is the smallest natural number e such that for all $g \in G$ $g^e = \text{Id}$. Let p be a prime number, a p-group is a group G in which every element has p-power order. Cauchy's theorem [9] tells us that if a prime p divides $|G|$, then G contains an element of order p and therefore also a subgroup of order p. The following theorem shows that G also contains a subgroup of order p^r where p^r is the highest power of p that divides $|G|$. A subgroup of this order is called a **Sylow p-subgroup** of G.

Theorem 1.2. *(Sylow's Theorem). Let G be a finite group and p a prime. Write $|G| = p^r m$ where p does not divide m.*

(i) There is at least one subgroup P of order p^r in G;

(ii) the subgroups of order p^r form a single conjugacy class in G;

(iii) if X is any p-subgroup of G, then $X \leqslant x^{-1}Px$ for some $x \in G$;

(iv) if n is the number of subgroups of order p^r, then $n|m$ and $n \equiv 1 (\mathrm{mod}\ p)$.

Consider the group S_{p^n} which has order $p^n!$. The largest power of p dividing the order of this group is $p^{1+p+p^2+\cdots+p^{n-1}}$. The group

$$P := (\cdots(C_p \text{ Wr } C_p) \text{ Wr } \cdots) \text{ Wr } C_p \leqslant S_{p^n}$$

has order $p^{1+p+p^2+\cdots+p^{n-1}}$ and is therefore a Sylow p-subgroup. All other Sylow p-subgroups are conjugate to P in S_{p^n}, they are therefore isomorphic to P. Hence P contains copies of all p-groups that are subgroups of the symmetric group on p^n points.

Lemma 1.1 shows that wreath products are "associative", hence we can refer to the group C_p Wr C_p Wr $\cdots$ Wr C_p without too much ambiguity.

The following theorem is known as *the Frattini argument.*

Theorem 1.3. *For a group G with a finite normal subgroup H let P be the Sylow p-subgroup of H, then $G = N_G(P) \cdot H$.*

Proof: Let g be an element of G. The conjugate of P by g is a subgroup of H as H is normal, it is therefore a Sylow p-subgroup of H and by Sylow's theorem is a conjugate of P by something in H. So $P^g = P^h$ for some $h \in H$ and hence $gh^{-1} \in N_G(P)$. □

1.2 Graph theory

We will also need a few definitions from graph theory, for further information the reader is referred to [12]. A **graph** is a vertex set V and an edge set E that is a subset of the set of unordered pairs of V. The degree of a vertex v is the size of the set $\{u|\{v,u\} \in E\}$. A **path** in our graph is a sequence of elements from E of the form

$$\{v_0, v_1\}, \{v_1, v_2\}, \{v_2, v_3\}, ..., \{v_{n-1}, v_n\}.$$

If each edge occurs no more than once in a path and the initial vertex v_0 is equal to the final vertex v_n, then the path is called a **circuit**. The **length** of a path or a circuit is the number of edges in the sequence. If for any two vertices v_1 and v_2 there exists a path with v_1 as an initial vertex and v_2 as a final vertex, then the graph is **connected**. The **distance** between the points v_1 and v_2 is the minimum length of a path with initial vertex v_1 and final vertex v_2. We will only be interested in **trees**, that is connected graphs that do not contain any circuits. In particular we will be interested in **regular trees**, these are trees that contain a (distinguished) root vertex of degree p for some prime p, a p-th power number of leaf vertices of degree one and other vertices all of degree $p+1$; in addition to this any two vertices at equal distance from the root must have the same degree. The **height** of a regular tree is the distance from the root vertex to any of the leaf vertices, a regular tree of height zero is the trivial tree consisting of one vertex and no edges. Figure 1.2 shows a regular tree of height two where $p = 3$.

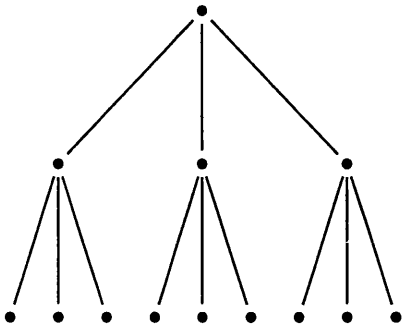


Figure 1.2: *A regular tree.*

A **subtree** of a regular tree is a subset of vertices of the tree such that they and the edges between them also form a regular tree. An **automorphism** of a tree is a map from V to V that preserves distances. An automorphism of a regular tree must preserve the root node and move leaf nodes to other leaf nodes. The automorphism group of a regular tree is $\underbrace{S_p \text{ Wr } S_p \cdots \text{ Wr } S_p}_{h \text{ times}}$ where h is the height of the tree, and is generated by maps that swap pairs of adjacent subtrees of equal height.

The trees that will be considered later are **weighted**, this simply means that each vertex is labelled by some number, in our case labels will be from the integers modulo p.

1.3 Parker's lemma

Let G be a permutation group acting on a set Ω. A cycle c is said to be **involved** in $g \in G$ if gc^{-1} fixes all points of the support of c (i.e a cycle is involved in an element of G if it occurs in the cycle decomposition of that element). Let C_k denote the set of all k-cycles involved in elements of G. Then G acts on the set C_k by conjugation.

Theorem 1.4. *(Parker's Lemma) For a finite group G, let P_k be the number of orbits of the action of G on C_k, and define $c_k(g)$ to be the number of k-cycles involved in g. Then*

$$P_k = \frac{k}{|G|} \sum_{g \in G} c_k(g)$$

Proof: Note that when $k = 1$ this becomes what is known as Burnside's counting lemma. The following proof of Parker's lemma is by double counting in a similar fashion to the proof of Burnside's lemma. Let Γ be the set $\{(c, g) | g \in G, c \text{ is a k-cycle involved in } g\}$ and let

$$\Gamma_c := \{(c, g) | g \in G, c \text{ is involved in } g\}.$$

Then

$$\sum_{g \in G} c_k(g) = |\Gamma| = \sum_{c \in C_k} |\Gamma_c|$$

Now let $C_k = \bigcup_{i=1}^{P_k} C_{k_i}$ where the C_{k_i} are the orbits of C_k.

$$\sum_{c \in C_k} |\Gamma_c| = \sum_{i=1}^{P_k} \sum_{c \in C_{k_i}} |\Gamma_c|$$

An element g is in the stabiliser of c if and only if some power of the cycle c is involved in g. Define a homomorphism

$$\Psi : \text{Stab}(c) \to \langle \gamma \rangle$$

where $\langle \gamma \rangle$ is the cyclic group of order k, by $\Psi(g) = \gamma^j$ if gc^{-j} fixes all points

in the support of c. The homomorphism Ψ is surjective hence the number of elements of G such that $\Psi(g) = \gamma$ is $\frac{|\text{Stab}(c)|}{k}$.

$$\sum_{i=1}^{P_k} \sum_{c \in C_{k_i}} |\Gamma_c| = \sum_{i=1}^{P_k} \sum_{c \in C_{k_i}} \frac{|\text{Stab}(c)|}{k} = \sum_{i=1}^{P_k} \frac{|C_{k_i}|.|\text{Stab}(c)|}{k} = P_k.\frac{|G|}{k}$$

□

The Parker Vector of a group is then defined to be $P(G) = (P_1, P_2, ..., P_n)$. Work has been done to look at what extent the Parker vector determines a group. Daniele Gewurz [5] shows that the Parker vector of A_n belongs uniquely to A_n and that $P(S_n) = P(G)$ for non-symmetric G only when $n = 6$ and $G = PGL(2, 5)$. This thesis will not add to the knowledge of Parker vectors, but it was in considering Parker vectors that the following function arose.

1.4 The cyclizer function

As before, for a permutation group G the set C_k contains all k-cycles involved in elements of G.

Definition. *For a finite permutation group G on a finite set of size n, let C be the set of all non-trivial cycles involved in elements of G, so $C := \bigcup_{k=2}^{n} C_k$. The cyclizer of G, written $Cyc(G)$, is the group generated by the elements of C. A group is said to be cycle-closed if $G = Cyc(G)$.*

By repeatedly taking cyclizers we get a sequence of groups.

$$G = G^0 \leq G^1 \leq ... \leq G^k \leq ...$$

where $G^{i+1} = Cyc(G^i)$ (We will usually denote G^i by $Cyc^i(G)$). The group $Cyc^i(G) \leq S_n$ for all i, hence there exists a minimal $k \in \mathbb{N}_0$ such that $Cyc^k(G) = Cyc^{k+1}(G)$ then we say k is the length of the cyclizer sequence for the group G.

Example. *Let G be the cyclic group of order 4 generated by the permutation $(1,2,3,4)$. Then $Cyc(G) = \langle (1,2,3,4), (1,3) \rangle$ the dihedral group on four points. We can then repeat this process to get $Cyc^2(G) = S_4$ and so here the length of the sequence is two.*

$$C_4 \mapsto D_{2.4} \mapsto S_4$$

Two questions arise immediately. Firstly, which finite groups are cycle-closed? And secondly, what is the maximum length of a sequence of cyclizers of a group? Both of these questions will be answered in the following chapters, we will also classify finite groups according to the length of their cyclizer sequence (with the exception of certain 2-groups).

The definition of the cyclizer of a group can be extended to infinite groups. For a group G acting on an infinite set, as in the finite case, let $Cyc(G)$ be the group generated by all cycles involved in elements of G. If G contains elements involving an infinite number of cycles, then $G \not\leq Cyc(G)$, so it is natural to also look at the group $C\widehat{yc}(G) := \langle Cyc(G), G \rangle$. Later we will begin our study of the infinite case by looking at the cyclizer of an infinite cyclic group where the functions Cyc and $C\widehat{yc}$ coincide, and then at other examples of infinite groups.

Chapter 2

Cyclizers of finite groups

Recall that for a finite permutation group G and C the set of all cycles involved in elements of G, $Cyc(G) = \langle C \rangle$. In this chapter we will consider cyclizers of finite groups and answer the two questions posed in the introduction.

1. Which finite groups are cycle-closed?

2. What is the maximum length of a cyclizer sequence?

In this investigation we will consider only transitive groups. It is easily seen that if $G_1, ..., G_m$ are the transitive constituents of G, then

$$Cyc(G) = Cyc(G_1) \times Cyc(G_2) \times \cdots \times Cyc(G_m)$$

and hence G is cycle-closed if and only if all transitive constituents are. Also the length of the associated sequence will be the maximum of the lengths of the sequences of the transitive constituents.

Throughout this chapter G will be a finite transitive permutation group of degree n acting on a set Ω. In this and subsequent chapters reference to "prime cyclic groups" will mean cyclic groups of prime order in their natural representation, that is $\langle(1, 2, ..., p)\rangle$ for some prime p.

2.1 Finite cycle-closed groups

In this section it will be shown that the only finite, cycle-closed, transitive, permutation groups are symmetric or prime cyclic.

Lemma 2.1. *If G is a cycle-closed transitive permutation group of degree n containing a transposition, then G is a symmetric group.*

Proof: Assume that G is a cycle-closed transitive permutation group on $\{1, ..., n\} = \Omega$ which contains a transposition. Without loss of generality we can assume that this transposition is $(1, 2)$. Transitivity of G implies that for all $\alpha \in \Omega$ there exists $\beta \in \Omega$ such that $(\alpha, \beta) \in G$. Let $\alpha \sim \beta$ if $(\alpha, \beta) \in G$ or $\alpha = \beta$, then $\sim$ is an equivalence relation (as $(\alpha, \beta), (\beta, \gamma) \in G$ implies $(\beta, \gamma)(\alpha, \beta)(\beta, \gamma) = (\alpha, \gamma) \in G$). Label the equivalence classes $\Omega_1, .., \Omega_k$. It suffices to show that there is only one equivalence class as then G will contain all transpositions and hence be a symmetric group. Assume for contradiction that $k > 1$. Without loss of generality let $1, 2 \in \Omega_1$ and consider a point $x \in \Omega$ such that x is not in Ω_1. As G is transitive and cycle-closed there is a single cycle element (a permutation involving exactly one nontrivial cycle) $g \in G$ such that $(1)g = x$. Now either $(2)g = 2$ or $(2)g \neq 2$.

If $(2)g = 2$, then $g^{-1}(1, 2)g = (x, 2) \in G$ hence $x \in \Omega_1$ giving a con-

tradiction. Otherwise $g = (1, x, .., 2, ..)$, $(1, x, 2, ...)$ or $(1, x, ..., 2)$. Now let $h = g(1, 2)$ and we get that $h = (1, x, ...)(2, ...)$, $(1, x)(2, ...)$ or $(1, x, ...)$ respectively. In each case let $h\prime$ be the cycle of h that moves the point 1 then $h\prime$ is a single cycle element taking 1 to x and fixing 2, so now we get a contradiction as before using $h\prime$ instead of g. □

Corollary 2.2. *Any transitive cycle-closed group of even degree is a symmetric group.*

Theorem 2.3. *If a permutation group G is transitive and cycle-closed, then it is prime cyclic or symmetric.*

Proof: Let G be a cycle-closed transitive permutation group, proof follows by induction on the degree of G. For $n = 1, 2$ or 3 G is automatically prime cyclic or symmetric. Assume that the theorem holds for all groups of degree less than n and consider G a transitive, cycle-closed, permutation group on $\{1, ..., n\} = \Omega$. As G is cycle-closed all point stabilisers G_α for $\alpha \in \Omega$ are also cycle-closed although not necessarily transitive. By induction G_1 is the direct product of prime cyclic or symmetric groups. One of three situations occur.

- One of the transitive constituents of G_1 is S_m for some $m \geq 2$ hence G contains a transposition and therefore by Lemma 2.1 $G = S_n$.

- The stabiliser G_1 is trivial. Then the stabiliser of each point is trivial and therefore all elements of G move all points of Ω. The group G involves only n-cycles hence n is prime and G is an n-group. But $G \leq S_n$ so $|G| = n$ and G is a prime cyclic group.

- The stabiliser G_1 is the direct product of prime cyclic groups and trivial groups but is not itself trivial. If any of these cyclic groups are of order 2, then the lemma applies and G is symmetric, so assume that none is. Each stabiliser partitions Ω into transitive components, each component corresponding to a prime cycle from the direct product (As G_i is conjugate to G_j for all $i, j \in \Omega$ the transitive partitions corresponding to each stabiliser will be of the same shape). Assume for contradiction that G_1 partitions Ω into *more* than two transitive constituents. One of these must be $\{1\}$, consider also the largest component and without loss of generality assume that this is $\{2, .., p+1\}$ where p is prime. The partition that G_2 imposes on Ω must be the same as G_1 except on the points $\{1, 2, ..., p+1\}$ where the partition must be$\{2\}\{1, 3..., p+1\}$. The group G therefore contains two p-cycles, one with support $\{2, .., p+1\}$ and another with support $\{1, 3, ..., p+1\}$. Both these p-cycles are elements of the group G_{p+2}, which exists by assumption. Thus $\{1, ..., p+1\}$ is a subset of a transitive constituent of G_{p+2}, contradicting the choice of p as the size of the largest constituent. Therefore G_i has only two transitive constituents, one of which is $\{i\}$ and the other containing p points for p an odd prime. The stabilisers G_i are odd prime cyclic for all i, thus G has even degree and is symmetric by Corollary 2.2. □

2.2 Bounds on the length of a cyclizer sequence

The previous section has shown that for any transitive permutation group which is not symmetric or prime cyclic there exists a sequence of groups

$$G = G^0 < G^1 < \cdots < G^k$$

such that $G^i = Cyc^i(G)$ and $G^i \neq G^{i+1}$ for all i. We know that G^k is symmetric or prime cyclic, but as a prime cyclic group has no nontrivial subgroups $G^k = S_n$ where n is the degree of G. In this section we are interested in finding a bound on k i.e. finding some N such that $Cyc^{N+1}(G) = Cyc^N(G)$ for all finite groups G.

2.2.1 Primitivity

Let $\Delta \subseteq \Omega$ be a non trivial block of the action of $Cyc(G)$ on Ω. The group G is a subgroup of $Cyc(G)$ and so Δ is also a block under the action of G. We have that primitivity of G implies primitivity of $Cyc(G)$. Therefore either the groups in the sequence are all primitive or there exists some $l < k$ such that the G^i are imprimitive for $i \leq l$ and primitive for $i > l$.

Theorem 2.4. *For a primitive permutation group G of degree n exactly one of the following applies:-*

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

The proof of this theorem depends on a result of Williamson [11].

Lemma 2.5 (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*

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

Proof of Theorem 2.4: Let G be a primitive permutation group such that $Cyc(G) \neq S_n, A_n$. By the lemma $Cyc(G)$ cannot contain any single m-cycle elements where $1 \leq m \leq (n-m)!$, therefore all single cycle elements must be cycles of length at least $\lceil \frac{n}{2} \rceil$ (as $\lfloor \frac{n}{2} \rfloor \leq \lceil \frac{n}{2} \rceil !$). This means that every cycle involved in an element of G must be of length at least $\lceil \frac{n}{2} \rceil$. So all elements in G are single cycle elements and $G = Cyc(G)$. We have already seen that any non-symmetric transitive group with $G = Cyc(G)$ is prime cyclic. □

Corollary 2.6. *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.*

Now we will consider the case when G is an imprimitive group. The set Ω contains a nontrivial block Δ_1 for G of size r. Transitivity gives us that the action of G partitions Ω into $\frac{n}{r}$ blocks of size r. Let g be an element of G such that the orbit of Δ_1 under g is $\{\Delta_2, \Delta_3, ..., \Delta_s, \Delta_1\}$ with $\Delta_i \neq \Delta_j$ and $s \geq 2$. Now consider the product of cycles involved in g that move Δ_1, call this $\widehat{g} \in Cyc(G)$. The element g is one of three following types:-

1. $\widehat{g}$ is an element of $Cyc(G)$ involving more than one cycle.

2. $\widehat{g}$ is a single rs-cycle and there exists an integer z that properly divides rs but such that z does not divide s and s does not divide z. Note that as $\widehat{g}$ is a single cycle it is of the form

$$(\alpha_1, \alpha_2, ..., \alpha_{rs}),$$

without loss of generality let $\alpha_1 \in \Delta_1$ then $\alpha_i \in \Delta_1$ for all $i \equiv 1 \bmod s$.

3. $\widehat{g}$ is a single rs-cycle and there is no integer z as above. This means that all factors of rs are either multiples or factors of s therefore rs is a prime power.

We will consider these cases one at a time.

1. There exists cycles of $\widehat{g}$ $\widehat{g_1}, \widehat{g_2} \in Cyc(G)$ such that $\text{Supp}(\widehat{g_1}) \cap \text{Supp}(\widehat{g_2}) = \emptyset$ and $\widehat{g} = \widehat{g_1}\widehat{g_2}$, but now $\widehat{g_1}$ must move some points of Δ_1 and fix others so Δ_1 is not a block under the action of $Cyc(G)$.

2. The element $\widehat{g}^z$ is of the form

$$(\alpha_1, \alpha_{z+1}, ..., \alpha_{(\frac{rs}{z}-1)z+1})(\alpha_2, ...) \cdots (\alpha_z, ..., \alpha_{rs}).$$

We will consider the cycle involved in $\widehat{g}^z$ that moves the point α_1. Note that this cycle moves all points of Δ_1 if and only if z divides s and that all points in this cycle are points of Δ_1 if and only if s divide z. As we have chosen z so that neither of these possibilities can occur this cycle must move some points of Δ_1 away from the set Δ_1 and leave others fixed. Therefore Δ_1 is not a block under the action of $Cyc(G)$.

3. Let $r = p^\rho$ and $s = p^\sigma$,

$$\widehat{g} = (\alpha_1, ..., \alpha_{p^{\rho+\sigma}})$$

and $\alpha_i \in \Delta_1$ for all $i \equiv 1 \bmod p^\sigma$. The element g^p involves the cycle $(\alpha_1, \alpha_{p+1}, ..., \alpha_{p^{\rho+\sigma}-p+1})$. Let this be h then h is an element of the group $Cyc(G)$. The element $\widehat{g}h^{-1}$ involves the cycle $\widehat{h} := (\alpha_1, \alpha_2, ..., \alpha_p)$ which moves exactly one point of Δ_1. This cycle is an element of the group $Cyc^2(G)$ and hence Δ_1 is not a $Cyc^2(G)$-block. Also the cycles h and $\widehat{h}$ move exactly one common point and therefore the commutator $[h, \widehat{h}]$ is a 3-cycle and $Cyc^2(G) \geq A_n$.

So for any G-block one of $1, 2$ or 3 from above applies. If all G blocks are of types 1 and 2, then $Cyc(G)$ is primitive. Otherwise there exists a G-block of type 3 and then $Cyc^2(G)$ is primitive, when this happens note that then $Cyc^3(G) = S_n$.

Theorem 2.7. *If a group G is such that $Cyc(G)$ is imprimitive, then G is a p-group.*

Proof: The group G must be imprimitive and satisfy the conditions of section 3 above, that is that all blocks are of p-power size for some prime p and blocks are only 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 $\Delta_1, \Delta_2, ..., \Delta_p$, 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 (theorem 1.3) 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. □

Theorem 2.8. *If G is a transitive, imprimitive permutation group such that $Cyc(G)$ is primitive, then $Cyc^2(G)$ is the full symmetric group.*

Proof: First we need a lemma.

Lemma 2.9 (Hall [6]). *Let G be a primitive permutation group on n points, and let H be a transitive subgroup of G on m points, fixing the remaining $n-m$ points. Then G is doubly transitive.*

The group $Cyc(G)$ contains elements which are single cycles and generate cyclic subgroups. These cyclic subgroups are transitive on their support and

fix the remaining points of the set. Therefore by the lemma $Cyc(G)$ is doubly transitive. It follows that $Cyc^2(G)$ is a primitive group containing a transposition and so by Lemma 2.5 is the full symmetric group. □

Corollary 2.10. *For all finite groups G, $Cyc^3(G) = Cyc^4(G)$.*

Example. *The cyclic group $C_9 = \langle(1,2,3,4,5,6,7,8,9)\rangle$ has maximal chain length.*

$$\begin{aligned} Cyc(C_9) &\cong C_3 \ Wr \ C_3, \\ Cyc^2(C_9) &\cong A_9, \\ Cyc^3(C_9) &\cong S_9. \end{aligned}$$

Cameron concludes his paper with several ideas for further research, one of which is to classify the groups finite groups that have a maximum chain length.

Chapter 3

Which finite transitive permutation groups G satisfy $Cyc^2(G) \neq Cyc^3(G)$?

We have already seen that such groups are p-groups for p an odd prime, 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.

3.1 Groups of degree p^2

Theorem 3.1. *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. We have already seen that blocks of $Cyc(G)$ are also blocks of G. Let Δ be a nontrivial block of the group G and $\alpha, \beta \in G$ 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 $|\Delta| = p$, 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 $\Delta \cap (\Delta)c \neq 0$ 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. □

We can say more than just that $Cyc(G)$ is primitive. Lemma 2.5 tells us that $Cyc(G)$ is in fact A_{p^2}. So we have the following corollary.

Corollary 3.2. *If G is a transitive p-group of degree p^2 and exponent p, then $Cyc^2(G) = S_{p^2}$.*

Definition. *The Frattini subgroup, $\Phi(G)$, of a finite group $G \neq 1$ is the intersection of all maximal subgroups of G. The Frattini subgroup of the trivial group is defined to be the trivial group.*

We remind the reader of the classical argument that the Frattini subgroup consists of the non-generators of G. Assume that $G \neq 1$. An element $g \in G$ is a non generator if $\langle X, g\rangle = G$ implies that $\langle X\rangle = G$ for every $X \subseteq G$. If g is a non-generator of G and X is a subset of G that generates a maximal subgroup M, then $\langle X, g\rangle$ will also generate M, hence $g \in \Phi(G)$. Conversely if $g \in \Phi(G)$ and $\langle X, g\rangle = G$ but $\langle X\rangle \neq G$, then $\langle X\rangle$ is a subgroup of some maximal subgroup $M < G$. However $g \notin M$ else $M = G$. This contradicts g being an element of the Frattini subgroup and so no such set X exists and g is a non-generator.

The Frattini subgroup of G is clearly a characteristic subgroup, in particular it is normal in G.

Theorem 3.3. *(The Burnside Basis Theorem) Let G be a group of order p^n and $\Phi(G)$ be its Frattini subgroup. Then $\Phi(G) = G'G^p$ (where $G^p = \{g^p : g \in G\}$) so the factor group $G/\Phi(G) = A$ is an elementary abelian group. If the order of A is p^r, then every generating set for G of size s contains a subset of size r that generates G. The natural projection from G onto A will carry any minimal generating set to an $\mathbb{F}_p$-basis of A, and conversely any set of r elements that are mapped to a basis for A will be a minimal generating set for G.*

Proof: See Hall [6].

Theorem 3.4. *The Cyclizer of a cyclic group generated by a p^2-cycle is isomorphic to the group C_p Wr C_p.*

Proof: let g be a p^2-cycle, without loss of generality assume that this cycle is

$$(0, 1, 2, ..., p^2 - 2, p^2 - 1).$$

The only elements of the group generated by this cycle which are not p^2-cycles are powers of g^p. The element g^p is a product of p cycles of length p, call these cycles $g_0, ..., g_d$ where $d = p - 1$ and such that the cycle g_i moves the point i. Note that the cycles $g_1, ..., g_d$ are all conjugates of the cycle g_0 by powers of g. Therefore the group $Cyc(\langle g \rangle)$ is generated by the cycles g and g_0 and is isomorphic to 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 2.5 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 3.5. *If G is a transitive p-group of degree p^2 and exponent p^2, then either $G = Cp$ Wr Cp or $Cyc(G) = Cp$ Wr Cp (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 Cp Wr Cp. 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 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 $(0, 1, 2, ..., p^2 - 2, p^2 - 1)$, g_0 be the p-cycle $(0, p, 2p, ..., (p-1)p)$ 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 $g_0 g_1 \cdots g_d$. The cycles $g_0, ..., g_d$ 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 3.6. *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 $\{0, ..., d\}$.

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 $g_0, ..., g_d$ 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 $g_0, ..., g_d$ 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 $\delta \in \{0, ..., d\}$.

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

and hence $\varepsilon_g = \delta_g$ and $\varepsilon_i = \delta_i$ for all $i \in \{0, ..., d\}$. □

Lemma 3.7. *The Frattini subgroup of W is the set of elements of the form $g_0^{\varepsilon_0} \cdots g_d^{\varepsilon_d}$ such that $\sum_{i=0}^{d} \varepsilon_i = 0 \mod p$.*

*Here the subscripts and powers are taken modulo p

Proof:

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

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

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

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

□

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

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

Lemma 3.8. *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. Each

conjugacy class of p^2-cycles inside $\langle g \rangle \cdot \Phi(W)$ is therefore of size p^{p-2}. 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 $\varepsilon_0, ..., \varepsilon_{d-1}$ 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 $\sum_{i=0}^{d} \zeta_i = 0 \bmod p$.

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

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

Now we have

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

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

equal. □

Proof of Theorem 3.5: Let G be a transitive p-group of degree and exponent p^2 such that $G \neq Cp$ Wr Cp. The group G contains a p^2-cycle, g. As before let $g^p = g_0 \cdots g_d$. We have $Cyc(G) \geq Cyc(\langle g \rangle) \cong C_p$ Wr C_p. Once again we will let $W := \langle g, g_0 \rangle \cong C_p$ 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 $Cyc(G) = W$. □

Corollary 3.9. *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 and $G \neq C_p$ Wr C_p.*

3.2 Extending this result to 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 refering 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

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

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 $g_0, g_1, ...g_d$ 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 $g_{0i}, g_{1i}, ..., g_{di}$ 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-1} p-cycles; each labelled by a string of k digits, for $1 \leqslant k \leqslant n-1$. 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 $P_n = C_p$ Wr $(C_p$ Wr C_p Wr $\cdots$ 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 $P_n = (C_p$ Wr $C_p)$ Wr $(C_p$ Wr $\cdots$ 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 $k \in \{0, 1, ..., d\}$ (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 $j \in \{0, 1, 2, ..., 00, 01, 02, ..., d\cdots d\}$ so for example the level 1 block system consists of the blocks $\Delta_0, \Delta_1, ..., \Delta_d$.

Theorem 3.10. *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 $\Gamma = \Delta_i$. □

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

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

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

$$[g_a, g_b] = g_a^{-1}\, g_a^{g_b} = \begin{cases} g_a^d\, g_c & : \text{ when } r = n-1 \\ g_a^d\, g_c\, g_{1a}^d\, g_{2a}^d \cdots g_{da}^d & : \text{ when } r < n-1. \end{cases} \tag{3.1}$$

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

$$g^{\varepsilon_g}\, g_0^{\varepsilon_0}\, g_1^{\varepsilon_1} \cdots g_d^{\varepsilon_d}\, g_{00}^{\varepsilon_{00}} \cdots\cdots g_{dd\cdots d}^{\varepsilon_{dd\cdots d}} \tag{3.2}$$

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

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 (3.2). It therefore suffices to show that two elements of this form written differently really are distinct.

Let

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

with each $\varepsilon \in \{0, 1..., d\}$

$$b := g^{\delta_g}\, g_0^{\delta_0}\, g_1^{\delta_1} \cdots g_d^{\delta_d}\, g_{00}^{\delta_{00}} \cdots\cdots g_{dd\cdots d}^{\delta_{dd\cdots d}}$$

with each $\delta \in \{0, 1..., d\}$

and assume that $ab^{-1} = \mathrm{Id}$. Note that if an element of this form (3.2) is the identity element, then the exponent of every cycle must be zero. Using the commutator data (3.1) from above we can rewrite ab^{-1} so that it starts $g^{\varepsilon_g} g^{-\delta_g}$... 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 $\varepsilon_i = \delta_i \quad \forall i$. □

Let D_n be the subgroup of P_n generated by the commutators of the cycles $g, g_1, \ldots g_{d\cdots d}$. 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:

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

$$\begin{aligned}
\textstyle\sum_{i=0}^{d} \varepsilon_i &= 0 \bmod p \\
\textstyle\sum_{i=00}^{dd} \varepsilon_i &= 0 \bmod p \\
&\vdots \\
\textstyle\sum_{i=0\cdots0}^{d\cdots d} \varepsilon_i &= 0 \bmod p.
\end{aligned}$$

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:

$$\begin{aligned}
&\textstyle\sum_{i=0}^{d} \varepsilon_i = 0 \bmod p \\
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \bmod p \qquad \forall j \in \{0,\ldots,d\} \\
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \bmod p \qquad \forall j \in \{00,\ldots,dd\} \\
&\qquad\qquad\vdots \\
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \bmod p \quad \forall j \in \{0\cdots0,\ldots,d\cdots d\}.
\end{aligned} \tag{3.3}$$

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

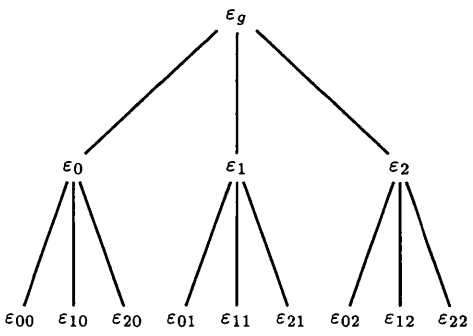
The set M_n is a subgroup of P_n. We can see this by induction on n. Let $m_1 := g^{\varepsilon_g}\ g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}, m_2 := g^{\delta_g}\ g_0^{\delta_0}\cdots g_d^{\delta_d}$ be elements of the set M_2, then $m_1.m_2^{-1} = g^{\varepsilon_g}\ g_0^{\varepsilon_0}\cdots g_d^{\varepsilon_d}\ g_d^{-\delta_d}\cdots g_0^{-\delta_0}\ g^{-\delta_g}$. Using the commutator data (3.1 top line only) and the fact that $\sum_{i=0}^{d}\varepsilon_i = 0 \bmod p$ and $\sum_{i=0}^{d}\delta_i = 0 \bmod p$ 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.

3.2.1 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.*



We will be considering the action of P_n on its set of associated trees. If

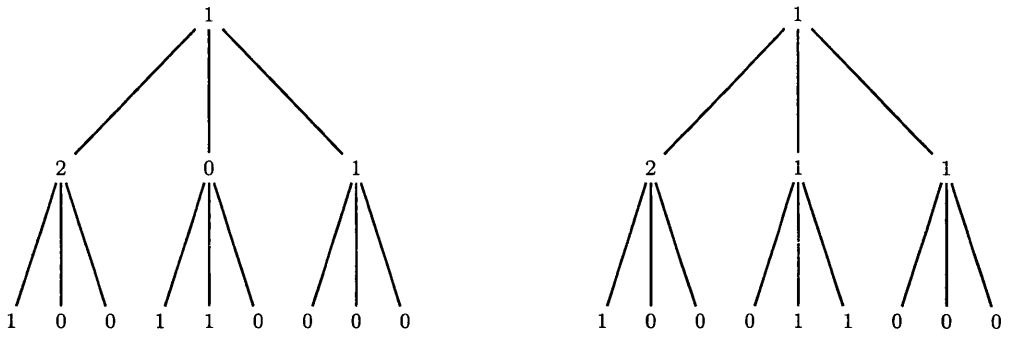


Figure 3.1:

$\alpha, \beta \in P_n$ 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 3.1 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 $r_1 r_2 \cdots r_k$ 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.

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 3.2 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.

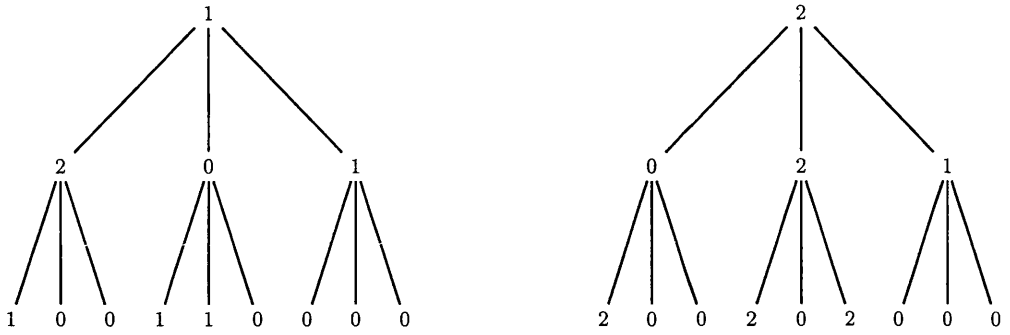


Figure 3.2:

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. 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 3.12. *If $H \leqslant P_n$ such that $Cyc(H) \leqslant P_n$, 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

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

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:

$$\begin{aligned}
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \pmod p && \forall j \in \{0, \ldots, d\} \\
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \pmod p && \forall j \in \{00, \ldots, dd\} \\
&\qquad\qquad\qquad \vdots \\
&\textstyle\sum_{i=0}^{d} \varepsilon_{ij} = 0 \pmod p && \forall j \in \{0\cdots0, \ldots, d\cdots d\}.
\end{aligned}$$

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.

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

□

Theorem 3.13. *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 class 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 3.14. *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 $r \in \{2, 3, ..., p-1\}$. Then

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

Let k be the least integer such that $r^k \equiv 1 (\text{mod } p^n)$ (such a k does exist as the Fermat-Euler Theorem [7] gives $r^{\varphi(p^n)} \equiv 1 (\text{mod } p^n)$ 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 $r^k \equiv 1 (\text{mod } p^n)$, 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

$$\lambda^{-1} g^{\varepsilon_g} \lambda \tag{3.4}$$

$$\text{where } \lambda := g_0^{\varepsilon_0}\, g_{00}^{\varepsilon_{00}}\, g_{01}^{\varepsilon_{00}} \cdots g_{0d}^{\varepsilon_{00}} \cdot \cdots \cdot g_{00\cdots0}^{\varepsilon_{00\cdots0}}\, g_{00\cdots1}^{\varepsilon_{00\cdots0}} \cdots g_{00\cdots d}^{\varepsilon_{00\cdots0}}$$

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

Lemma 3.15. *Elements of the form (3.4) 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 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 $g_{00\cdots0}^{-\varepsilon_{00\cdots0}}\ g_{00\cdots1}^{-\varepsilon_{00\cdots0}}\cdots g_{00\cdots d}^{-\varepsilon_{00\cdots0}} g^{\varepsilon_g}\gamma\ g_{00\cdots0}^{\varepsilon_{00\cdots0}}\ g_{00\cdots1}^{\varepsilon_{00\cdots0}}\cdots g_{00\cdots d}^{\varepsilon_{00\cdots0}}$ with $g^{\varepsilon_g}\gamma \in M_{k-1}$. Rearranging this we get

$$g^{\varepsilon_g} g_{\varepsilon_g 0\cdots0}^{-\varepsilon_{00\cdots0}}\ g_{\varepsilon_g 0\cdots1}^{-\varepsilon_{00\cdots0}}\cdots g_{\varepsilon_g 0\cdots d}^{-\varepsilon_{00\cdots0}}\gamma\ g_{00\cdots0}^{\varepsilon_{00\cdots0}}\ g_{00\cdots1}^{\varepsilon_{00\cdots0}}\cdots g_{00\cdots d}^{\varepsilon_{00\cdots0}}$$

$$= g^{\varepsilon_g}\gamma g_{\varepsilon_g 0\cdots0}^{-\varepsilon_{00\cdots0}}\ g_{\varepsilon_g 0\cdots1}^{-\varepsilon_{00\cdots0}}\cdots g_{\varepsilon_g 0\cdots d}^{-\varepsilon_{00\cdots0}} g_{00\cdots0}^{\varepsilon_{00\cdots0}}\ g_{00\cdots1}^{\varepsilon_{00\cdots0}}\cdots g_{00\cdots d}^{\varepsilon_{00\cdots0}}$$

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 (3.4) are in the same conjugacy class, where

$$\alpha := g_0^{\varepsilon_0}\ g_{00}^{\varepsilon_{00}}\ g_{01}^{\varepsilon_{00}}\cdots g_{0d}^{\varepsilon_{00}}\cdots\cdots g_{00\cdots0}^{\varepsilon_{00\cdots0}}\ g_{00\cdots1}^{\varepsilon_{00\cdots0}}\cdots g_{00\cdots d}^{\varepsilon_{00\cdots0}} \text{ and}$$

$$\beta := g_0^{\delta_0}\ g_{00}^{\delta_{00}}\ g_{01}^{\delta_{00}}\cdots g_{0d}^{\delta_{00}}\cdots\cdots g_{00\cdots0}^{\delta_{00\cdots0}}\ g_{00\cdots1}^{\delta_{00\cdots0}}\cdots g_{00\cdots d}^{\delta_{00\cdots0}}.$$

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 3.14 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

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

and hence $\varepsilon_0 = \delta_0$.

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

$$\begin{aligned} v_{\alpha^{-1}\, g^c}(g_i) &\equiv v_{\alpha^{-1}}(g_r) + v_{g^c}(g_i) \ (\bmod p)^\dagger \qquad \forall i \\ &\equiv -\underbrace{\varepsilon_{0\cdots0}}_{k \text{ zeros}} + 0 \ (\bmod p) \end{aligned}$$

therefore

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

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

We have now shown that all elements of the form (3.4) are in distinct conjugacy classes, hence there are at least $p^{n-1}(p-1)$ conjugacy classes. This gives at least

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

†Here r is as defined on page 44 , however in the tree corresponding to α^{-1} the value of all level $k-1$ vertices is the same.

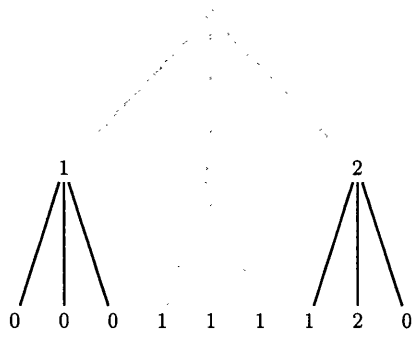
p^n-cycles in M_n and therefore all h with $\varepsilon_g \neq 0$ must be p^n-cycles.

Lemma 3.16. *$Cyc(M_n) = P_n$.*

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. □

Proof of Theorem 3.13: 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. □

Theorem 3.17. *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 $\Delta_1, \Delta_2, ..., \Delta_n$, 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 $Cyc(G_{\{\Gamma\}}) \leqslant Cyc(G)_{\{\Gamma\}}$.

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 $\Omega_1, ..., \Omega_{n-1}$.

Choose r to be the least number such that $\Omega_0, \Omega_1, ..., \Omega_r$ 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 $Cyc(H)^{\Omega_{r+s}|_{\Delta_i}}_{\{\Delta_i\}}$ 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 on 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 $H^{\Omega_{r+s}|_{\Delta_i}}_{\{\Delta_i\}}$ is also a p-group and hence contains an element which involves a p-cycle. This p-cycle is in $Cyc(H^{\Omega_{r+s}|_{\Delta_i}}_{\{\Delta_i\}}) \leqslant Cyc(H)^{\Omega_{r+s}|_{\Delta_i}}_{\{\Delta_i\}}$.

By the earlier Lemma 2.5, primitive groups of degree p^s with $s \geqslant 2$ which contain a p-cycle are either alternating or symmetric. The group $Cyc(H)^{\Omega_{r+s}|_{\Delta_i}}_{\{\Delta_i\}}$

is the cyclizer of a p-group, it is primitive and contains a p-cycle, therefore

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

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

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

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 3.18. *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 $n \in \mathbb{N}, n \geqslant 2$.*

Chapter 4

Classification of finite groups according to sequence length

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 which are not prime cyclic

Theorem 2.4 says 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.

Imprimitve groups (other than p-groups)

By Theorem 2.7 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 2.5. If $|G|$ is odd, then $Cyc(G) \leq A_n$ and by Theorem 2.8 $Cyc^2(G) = S_n$.

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)

Chapter 3 gives us that a p-group G has a cycliser 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 cycliser 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 Chapter 3 we can see that $Cyc(G) = C_2$ Wr $C_2 \cdots$ 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

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 Chapter 3 • 2-groups G such that $Cyc(G) \neq S_n$
3	• p-groups ($p \neq 2$) as specified in Chapter 3

Figure 4.1: *A partial classification of groups according to the length of their cyclizer sequence*

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 4.1.

Chapter 5

The infinite cyclic group

It has already been noted that for an infinite group G it is not necessarily the case that $G \leq Cyc(G)$. If a group contains a permutation involving an infinite number of cycles, then it seems natural to look at the group $C\widehat{yc}(G) := \langle G, Cyc(G) \rangle$. For finite groups and groups whose elements involve only a finite number of cycles the two definitions of cyclizer coincide. In his paper Cameron [2] defines four different functions; the two we have already seen, $R(G) := \langle \{\sigma | \sigma\rho \in G, \sigma \text{ and } \rho \text{ are disjoint permutations } \} \rangle$ the group generated by all restrictions of elements of G and $C^+(G) := \langle \{g | \text{ if } c \text{ is involved in } g \; \exists h \in G \text{ such that } c \text{ is involved in } h\} \rangle$. For the purposes of this thesis we will look only at the functions Cyc and $C\widehat{yc}$.

We begin our investigation of infinite groups by considering the infinite cyclic group on the integers, generated by σ where $(x)\sigma = x + 1$ for all $x \in \mathbb{Z}$. All elements of this group involve only a finite number of cycles hence all definitions of cyclizer seen above coincide.

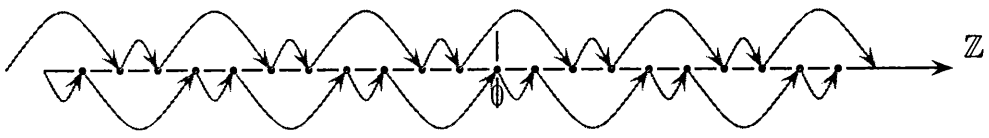


Figure 5.1: *A pictorial representation of the permutation m.*

Definition. *A permutation, p, of the integers is modular if there exists some* $n \in \mathbb{N}$ *such that for every* $k \in \{0, 1, ..., n-1\}$ $\exists\ i_k \in \mathbb{Z}$ *and* $(x)p = x + i_k$ *whenever* $x \equiv k \pmod{n}$. *The least possible n in this context is the period of the modular permutation.*

Example. *The following permutation, m, is modular with* $n = 2$ *(see figure 5.1).*

$$(x)m = \begin{cases} x+1 & : \quad x = 0(mod 2) \\ x+3 & : \quad x = 1(mod 2) \end{cases}$$

Note that if m_1 and m_2 are modular permutations with period t_1 and t_2 respectively, then the permutation $m_1 m_2$ is also modular and has period dividing $\text{lcm}(t_1, t_2)$. The set of modular permutations form a group which we shall call M. The cycles involved in elements from M are either finitary (they fix all but a finite number of points) or they are infinite cycles which are themselves modular. Hence $Cyc(M) =< M, FS(\mathbb{Z}) >$ where $FS(\mathbb{Z})$ is the group of finitary permutations on $\mathbb{Z}$.

Theorem 5.1. *Let* $C_\infty := \langle \sigma \rangle$, *the infinite cyclic group, then :-*

(i) $Cyc(C_\infty) = M$

(ii) $Cyc^2(C_\infty) =< M, FS(\mathbb{Z}) >$.

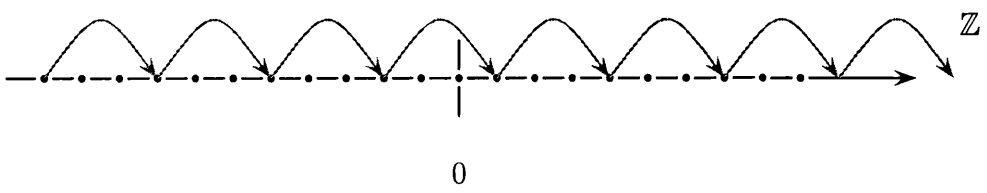


Figure 5.2: *The elementary permutation* $\pi_{3,1}$.

Proof: (i)The group $Cyc(C_\infty)$ is generated by the cycles involved in powers of σ. These cycles are $\pi_{i,j}$ for $i \in \mathbb{N}, j \in \mathbb{Z}, 0 \leq j < i$ where

$$(x)\pi_{i,j} = \begin{cases} x+i & \text{if } x \equiv j \pmod{i} \\ x & \text{otherwise} \end{cases}$$

We will call these π elementary permutations. For example $\pi_{3,1}$ is the following elementary permutation (see figure 5.2).

$$(x)\pi_{3,1} = \begin{cases} x+3 & \text{if } x \equiv 1 \pmod{3} \\ x & \text{otherwise} \end{cases}$$

For $n \in \mathbb{N}$ let M_n be the subgroup consisting of those $p \in M$ with period dividing n and note that $M_n \leq M_m$ whenever n divides m. For each of these subgroups there exists a natural homomorphism $\Phi_n : M_n \longrightarrow S_n$ into the symmetric group of degree n by looking at M_n acting on residue classes modulo n on $\mathbb{Z}$, so that

$$(k)(\Phi_n(p)) = k + i_k \pmod{n} \qquad \forall k \in \{0, 1, ..., n-1\}$$

where $(x)p = x + i_k$ for $x \equiv k \pmod{n}$. The kernel of this homomorphism is

the group of permutations that respect the residue classes, denote this by R_n.

Notice that all the elementary permutations π are modular therefore $Cyc(C_\infty) \leq M$, hence it suffices to show that $M \leq Cyc(C_\infty)$. This will be done by firstly showing that $R_n \leq Cyc(C_\infty)$ for all $n \in \mathbb{N}$, and then that for any $n \in \mathbb{N}$ $\Phi_n(Cyc(C_\infty) \cap M_n) = S_n$.

Consider $r \in R_n$ and the action this element has on the residue class containing 0. If 0 is fixed, then r acts as the identity on this residue class, otherwise due to the modularity of r the action on the residue class containing 0 will be completely defined by where it sends 0. Let $(0)r = kn$ then the cycles involved in r which affect this residue class will be $(..., 0, kn, 2kn, ...), (..., n, (k+1)n, ...), ..., (..., -n, (k-1)n, ..)$ all of which are elementary permutations. Similarly for other residue classes, so r is a finite product of elementary permutations and hence is in $Cyc(C_\infty)$.

Now we are required to show $\Phi_n(Cyc(C_\infty) \cap M_n) = S_n$. Note that it is sufficient to show that $\Phi_m(Cyc(C_\infty) \cap M_m) = S_m$ for any m a multiple of n. We will show it holds for np where p is the smallest prime that is not a factor of n. Let $H_{np} := \Phi_{np}(Cyc(C_\infty) \cap M_{np})$, the cycle σ is in $Cyc(C_\infty) \cap M_{np}$ and $\Phi_{np}(\sigma) = (0, 1, 2, .., np-1)$ $\forall n$ so $(0, 1, 2, .., np-1) \in H_{np}$.
The following lemma will be used.

Lemma 5.2. *(Jordan) A primitive subgroup of S_n is equal to S_n or A_n whenever it contains a q-cycle for some $q \leq n-3$.*
In particular a primitive subgroup of S_n containing an odd permutation and a 3-cycle will be the whole of S_n for $n \geq 6$.

The odd permutation $(0, 1, ..., np-1)$ is in the group H_{np}, to satisfy the

conditions of the lemma we need H_{np} to be primitive and contain a 3-cycle. The image of the following commutator is a 3-cycle from H_{np}.

$$\begin{aligned}[\pi_{p,0}, \pi_{n,0}] = & \quad (..., 3p, 2p, p, 0, -p, ...)(...3n, 2n, n, 0, -n, ...) \\ & \quad (... - p, 0, p, 2p, ...)(..., -n, 0, n, 2n, ...) \\ = & \quad ...(0, n, p)(np, np + n, np + p)(2np, 2np + n, 2np + p)...\end{aligned}$$

$$\Phi_{np}([\pi_{p,0}, \pi_{n,0}]) = (0, n, p) \in H_{np}$$

As $(0, 1, ..., np - 1) \in H_{np}$ any non trivial block in H_{np} must be of the form $\Delta = \{0, k, 2k, ..\}$ for some k dividing np. If such a block exists, it cannot contain both n and p as they are co-prime, but it does contain 0. If we let $g = (0, n, p)$, then $(\Delta)g$ and Δ are neither equal or disjoint and thus no non trivial blocks exist and H_{np} is primitive. The conditions of the lemma are satisfied giving us that $H_{np} = S_{np}$ and hence $Cyc(C_\infty) = M$. (ii) follows immediately from (i). □

The cyclizer of the infinite cyclic group was looked at by Cameron [2]. The following is taken from that paper and completes the investigation into the infinite cyclic group as started above (everything that has come before was done independently of Cameron).

Theorem 5.3. (i) *$Cyc^3(C_\infty)$ is the set of all permutations g of $\mathbb{Z}$ for which there exist $r > 0$ and h_+,$h_- \in M$ such that $(x)g = (x)h_+$ for $x > r$ and $(x)g = (x)h_-$ for $x < -r$.*

(ii) *$Cyc^3(C_\infty) = Cyc^4(C_\infty)$, that is, $Cyc^3(C_\infty)$ is cycle-closed.*

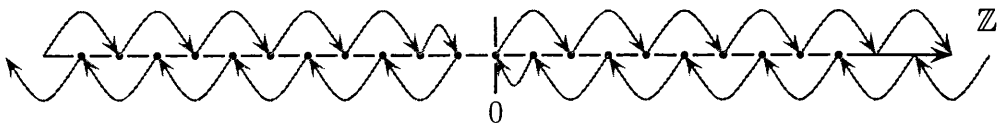


Figure 5.3: *The permutation* $\pi_{2,0}(0,1)\pi_{2,1}^{-1}$

Proof: (i) These elements occur as there are some cycles involved in elements of $Cyc^2(C_\infty)$ that are not modular, for example consider the cycles involved in the permutation $\pi_{2,0}(0,1)\pi_{2,1}^{-1}$, illustrated in figure 5.3.

We show first that any cycle of an element of $Cyc^2(C_\infty)$ satisfies the specifications of (i). This is clear for a finite cycle, so let g be an infinite cycle. The two 'ends' of g agree with those of two cycles (possibly equal) of an element of M. Since M contains all infinite cycles of all its elements, the result is true. It follows that any element of $Cyc^3(C_\infty)$ has the form (i).

To conclude, we must show that every permutation of the form (i) belongs to $Cyc^3(C_\infty)$. So let g be such a permutation. By multiplying g by h_-^{-1}, we may assume that $h_- = 1$. Now any cycle of h_+ is either ascending, descending, or finite. (We call an infinite cycle ascending if some power of it translates points in its support by a positive number; see the argument later on the flow of a permutation. Descending cycles are defined analogously.) Our permutation g must have equal numbers of descending and ascending cycles as it is only one ended. Thus we may pair the ascending and descending cycles of h_+. We can find an element of $Cyc^2(C_\infty)$ with a cycle which agrees with the product of a paired pair of cycles of h_+ on the positive end of $\mathbb{Z}$, and fixes the negative end pointwise. (This element is the product of the two paired cycles and a

transposition interchanging points in the two cycles.)

It remains to deal with finite cycles. Now the finite cycles of h_+ fall into congruence classes modulo n, for some n. We express the product of the positive cycles as an element of $Cyc^3(C_\infty)$. Take one congruence class of cycles, defining a permutation g. Suppose first that some congruence class (say x mod n) is fixed. Let y mod n be a congruence class moved by g. There is a permutation $\tilde{g_1}$ satisfying $(kn+x)\tilde{g} = k(n-1)+x$ and $(kn+y)\tilde{g} = k(n+1)+y$ for sufficiently large k, all negative points being fixed. (Take $\tilde{g_1}$ to be the product of two infinite cycles and a transposition interchanging points in the two cycles.) Then $g\tilde{g}$ has a single infinite cycle $\dot{g}$ on the positive end of $\mathbb{Z}$, fixing the negative end pointwise. On the other hand, if g has no fixed points, we can write it as a product of two permutations in $Cyc^3(C_\infty)$ with finite cycles, each of which has fixed points; then the positive end of each factor belongs to $Cyc^3(C_\infty)$, and hence so does the positive end of g.

(*ii*) Finally we show the $Cyc^3(C_\infty)$ is cycle-closed. Clearly it contains all the finite cycles. Any infinite cycle of a permutation satisfying (*i*) itself satisfies (*i*), and so also belongs to $Cyc^3(C_\infty)$. □

Chapter 6

The infinite dihedral group

We now find the cyclizer sequence for the infinite dihedral group $D =< \sigma, \tau > \leq \mathrm{Sym}(\mathbb{Z})$ where $(x)\sigma = x+1$ and $(x)\tau = 1-x$ for all $x \in \mathbb{Z}$. The group $Cyc(D)$ is generated by the elementary permutations, $\pi_{i,j}$, and a transposition from τ, say $(1,-1)$. Hence $Cyc(D)$ contains $Cyc(C_\infty)$ as a subgroup.

Lemma 6.1. *The group of modular permutations, $Cyc(C_\infty)$ is highly transitive.*

Proof: Suppose that $(a_1, ..., a_n)$ and $(b_1, ..., b_n)$ are sets of n distinct points of $\mathbb{Z}$. Let $s := \max\{a_1, ..., a_n, b_1, ..., b_n\}$ and $r := \min\{a_1, ..., a_n, b_1, ..., b_n\}$ and let m be the difference $m := s-r$. We can construct a finite permutation π on the interval $[r, s]$ such that $(a_i)\pi = b_i$ for all i. By repeating the pattern of this permutation throughout the integers at intervals of $m+1$ we can construct a modular permutation σ with period $m+1$ that also satisfies $(a_i)\sigma = b_i$ for all i. □

As $Cyc(D)$ is highly transitive and contains a transposition, it also has the finitary symmetric group $FS(\mathbb{Z})$ as a subgroup. We therefore have that $Cyc(D) = Cyc^2(C_\infty)$. It follows that $Cyc^2(D) = Cyc^3(C_\infty)$ which has already been shown to be self-cyclising. It is natural to consider next the group $C\widehat{yc}(D) :=< Cyc(D), D >$, which is generated by the elementary permutations $\pi_{i,j}$, a transposition $(1, -1)$ and the reflection τ.

Theorem 6.2. *The group* $C\widehat{yc}(D) = Cyc^2(C_\infty) \cup Cyc^2(C_\infty)\tau$, *where* $Cyc^2(C_\infty)\tau = \{g\tau | g \in Cyc^2(C_\infty)\}$.

Proof: Let $g \in C\widehat{yc}(D)$, then $g = \alpha_1\tau\alpha_2\tau...\alpha_{n-1}\tau\alpha_n$ for some $\alpha_i \in Cyc^2(C_\infty)$ and $n \in \mathbb{Z}$. However $\tau\alpha_i\tau = \alpha_i^\tau \in Cyc^2(C_\infty)$ so for odd n we have

$$g = \alpha_1 \underbrace{\tau\alpha_2\tau}_{\in Cyc^2(C_\infty)} \alpha_3 \underbrace{\tau\alpha_4\tau}_{\in Cyc^2(C_\infty)} \dots \underbrace{\tau\alpha_{n-1}\tau}_{\in Cyc^2(C_\infty)} \alpha_n \in Cyc^2(C_\infty)$$

and for even n we have

$$g = \alpha_1 \underbrace{\tau\alpha_2\tau}_{\in Cyc^2(C_\infty)} \alpha_3 \underbrace{\tau\alpha_4\tau}_{\in Cyc^2(C_\infty)} \dots \underbrace{\tau\alpha_n\tau}_{\in Cyc^2(C_\infty)} \tau \in Cyc^2(C_\infty)\tau.$$

□

We can see from Theorem 6.2 that $C\widehat{yc}(D)$ contains $Cyc^2(C_\infty)$ as a subgroup of index two. We have already looked at this subgroup so it remains to understand elements of the type $g\tau$ where $g \in Cyc^2(C_\infty)$. These elements will still exhibit repetitive patterns (i.e with the exception of some finite region they can be defined on an interval of the integers). However the presence of the

reflection τ means that there is no longer any bound on the distance an integer is moved by the permutation. The reflection also causes all integers outside some central finite region to be mapped to an integer the other side of zero (negatives are mapped to positives and positives are mapped to negatives).

To overcome these difficulties we can reorder the integers so that our group acts on $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$, via the bijection $f : \mathbb{Z} \mapsto \mathbb{N}_0$.

$$f(x) = \begin{cases} 0 & : \quad x = 0 \\ 2x - 1 & : \quad x > 0 \\ -2x & : \quad x < 0 \end{cases}$$

Pictorially this bijection is a folding of the integers, see figure 6.1.

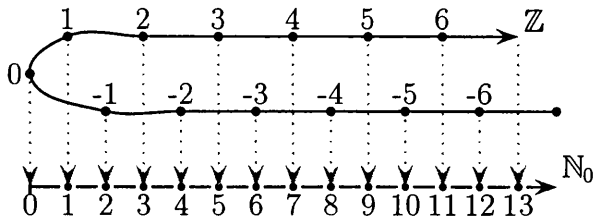


Figure 6.1: *The bijection* $f : \mathbb{Z} \mapsto \mathbb{N}_0$.

Let $F : \mathrm{Sym}(\mathbb{Z}) \mapsto \mathrm{Sym}(\mathbb{N}_0)$ map permutations on $\mathbb{Z}$ to permutations on $\mathbb{N}_0$ via this folding of the integers. The generators of D become $\tilde{\tau} = F(\tau)$ and $\tilde{\sigma} = F(\sigma)$ where

$$(x)\tilde{\tau} = \begin{cases} x - 1 & : \quad x = 1 \ (\mathrm{mod}\ 2) \\ x + 1 & : \quad x = 0 \ (\mathrm{mod}\ 2) \end{cases}$$

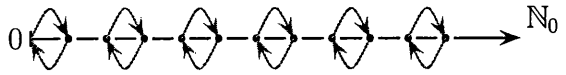


Figure 6.2: $\tilde{\tau}$

and

$$(x)\tilde{\sigma} = \begin{cases} 1 & : \quad x = 0 \\ x+2 & : \quad x = 1 \pmod 2 \\ x-2 & : \quad x = 0 \pmod 2, x \neq 0 \end{cases}$$

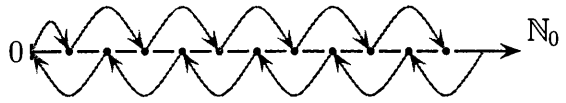


Figure 6.3: $\tilde{\sigma}$

We can now define *m*odular permutations on $\mathbb{N}_0$ analogous to those on $\mathbb{Z}$.

Definition. *A permutation, $p \in Sym\ \mathbb{N}_0$ is modular if there exists some $r, n \in \mathbb{N}$ such that for every $k \in \{0, 1, ..., n-1\}$ $\exists\ i_k \in \mathbb{Z}$ such that $(x)p = x + i_k$ whenever $x > r$ and $x \equiv k \pmod n$. The period of a modular permutation is the smallest n that can be used in this context.*

The modular permutations on $\mathbb{N}_0$ form a group ($M(\mathbb{N}_0)$) which contains both $\tilde{\sigma}$,$\tilde{\tau}$ and all finitary permutations of $\mathbb{N}_0$. Moreover this group is cycle-closed as any infinite cycle involved in an element from the group must itself be modular.

Theorem 6.3. *If ξ is a modular permutation on $\mathbb{Z}$, then $\tilde{\xi} = F(\xi)$ is a modular permutation on $\mathbb{N}_0$.*

Proof: For clarity, relabel the group of modular permutations in $\mathbb{Z}$ as $M(\mathbb{Z})$. Let $\xi \in M(\mathbb{Z})$ be a modular permutation with period n, then for all $k \in$

$\{0, 1, ..., n-1\}$ there exists $i_k \in \mathbb{Z}$ such that $(z)\xi = z + i_k$ whenever $z \equiv k(\mod n)$. Let $m \in \mathbb{Z}$ such that $|z - (z)\xi| \leqslant m$ for all $z \in \mathbb{Z}$. Then notice that under the isomorphism f positive integers are mapped to odd numbers and negative integers are mapped to even numbers moreover if $z \equiv k(\mod n)$, then

$$f(z) \equiv \begin{cases} 2k-1 \ (\mod 2n) & : \quad z > 0 \\ -2k \ (\mod 2n) & : \quad z \leqslant 0 \end{cases}$$

for all $z \in \mathbb{Z}$. Hence if $\tilde{\xi} = F(\xi)$, then for all $x \in \mathbb{N}_0$ greater than $2m$

$$(x)\tilde{\xi} = \begin{cases} x + 2i_k & : \quad x \equiv 2k-1 \ (\mod 2n) \\ x - 2i_k & : \quad x \equiv -2k \ (\mod 2n) \end{cases}$$

and therefore $\tilde{\xi} \in M(\mathbb{N}_0)$ and is a permutation with period n or $2n$. □

Let $M_{2n}(\mathbb{N}_0)$ be the set of elements of $M(\mathbb{N}_0)$ which have period dividing $2n$ and consider an element p of this set. Partition $\mathbb{N}_0$ into disjoint intervals $\{k2n, ..., (k+1)2n-1\}$ for $k \in \mathbb{N}_0$. On each of these intervals the permutation induces a map $\mathbb{Z}_{2n} \to \mathbb{Z}_{2n}$. Because of the modularity of p there will be a unique map that occurs an infinity of times $\hat{p} : \mathbb{Z}_{2n} \to \mathbb{Z}_{2n}$. Let N be the smallest integer such that $|(x)\hat{p} - x| < N \ \forall x$. Then there exists a sequence of $2N+1$ consecutive intervals which all give rise to the map $\hat{p}$. Assume for contradiction that $\hat{p}$ is not a bijection. Then there is some point $i \in \mathbb{Z}_{2n}$ that is not in the image of $\hat{p}$. If the equivalence class $[i]$ is not in the image, then consider the representative of this class from the set in the centre of the $2N+1$ consecutive sets $((N+1)2n + i)$. There must be a point $a \in \mathbb{N}_0$ such that

$(a)p = (N+1)2n + i$. However as the equivalence class $[i]$ is not in the image of $\hat{p}$, a cannot be a member of the chosen $2N+1$ sets. It also cannot be in the complement of these sets as no point is moved more than N places. Therefore the map $\hat{p}$ is a bijection. We are now in a position to define a homomorphism

$$\Theta_{2n} : M_{2n}(\mathbb{N}_0) \to S_{2n}$$

that takes each modular permutation to the particular $\hat{p}$ that it induces on $\mathbb{Z}_{2n}$.

Example. *The following modular permutation p has period 4 (Figure 6.4).*

$$(x)p = \begin{cases} 1 & : \quad x = 0 \\ x-1 & : \quad x = 0 \ (\ mod\ 4), x \geq 4 \\ x+4 & : \quad x = 1 \ (\ mod\ 4) \\ x & : \quad x = 2 \ (\ mod\ 4) \\ x-3 & : \quad x = 3 \ (\ mod\ 4) \end{cases}$$

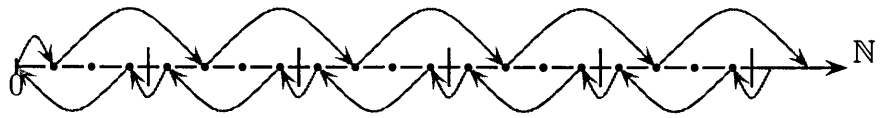


Figure 6.4: *A permutation with period* 4.

Under the homomorphism p is sent to an element from S_4.

$$\Theta_4(p) = (0,3)(1)(2)$$

We return now to the group $C\widehat{yc}(D)$ in order to determine the image of this group under the above homomorphism. We know that $C\widehat{yc}(D) = Cyc^2(C_\infty) \cup Cyc^2(C_\infty)\tau$ and we have already seen that elements of $Cyc^2(C_\infty)$ are modular on the integers except possibly on a finite region. Now we will consider the action of $C\widehat{yc}(D)$ on $\mathbb{N}$ that comes from the folding bijection and we will be looking at what happens to these permutations under the homomorphism defined above. We want to know which permutations of $\{[0],[1],...,[2n-1]\}$ are images of permutations from $C\widehat{yc}(D)$ under the homomorphism Θ (where the $[i]$ are equivalence classes mod $2n$) .

Figure 6.5 shows how the residue classes modulo n on $\mathbb{Z}$ map to residue classes modulo $2n$ on $\mathbb{N}_0$. Consider first the elements of $Cyc^2(C_\infty)$. Except on a finite central region these act as modular permutations (on $\mathbb{Z}$) and hence we can find elements of $Cyc^2(C_\infty)$ that will induce arbitrary permutations on $\{\bar{1},\bar{2},\ldots,\bar{n}\}$ and hence also on the set $\{[1],[3],\ldots,[2n-1]\}$, whence the same permutation will be induced on the sets $\{\tilde{1},\tilde{2},\ldots,\tilde{n}\}$ and $\{[2n-2],[2n-4],\ldots,[2],[0]\}$. Elements of $Cyc^2(C_\infty)\tau$ exchange the two sets $\{\bar{1},\bar{2},\ldots,\bar{n}\}$ and $\{[1],[3],\ldots,[2n-1]\}$ and hence their images under F will exchange the two sets $\{[1],[3],\ldots,[2n-1]\}$ and $\{[2n-2],[2n-4],\ldots,[2],[0]\}$. So the group $C\widehat{yc}(D)$ acts on the residue classes $\{[1],[2],\ldots,[2n-1]\}$ of $\mathbb{N}_0$ like $S_n \times C_2$ acting on $2n$ points.

The following lemma will be required for the exploration of $C\widehat{yc}^2(D)$.

Lemma 6.4. *The group S_n Wr C_2 is a maximal subgroup of S_{2n}.*

Proof: The group S_nWr C_2 is a transitive imprimitive group with a unique nontrivial block system consisting of two blocks of size n. Any element of S_{2n}

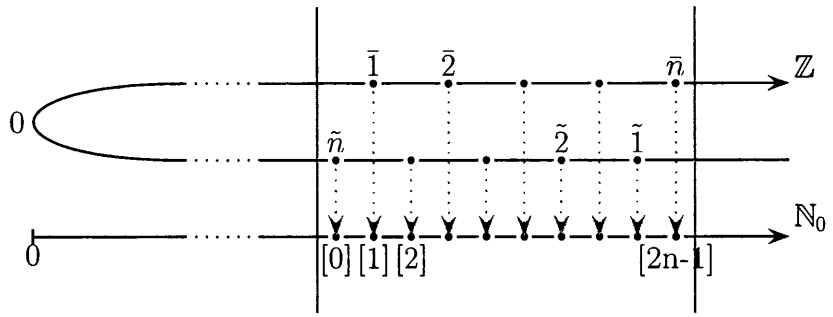


Figure 6.5: *Residue classes modulo n under the map f.*

that preserves this block system either fixes both blocks and is therefore an element of $S_n \times S_n \leq S_n$ Wr C_2, or it exchanges the blocks and is therefore also an element of S_n Wr C_2. Consider a group G such that S_n Wr $C_2 < G \leq S_{2n}$ then any system of blocks in the group G must contain the two blocks from S_n Wr C_2 as a sub-system, hence G either preserves the two blocks or is primitive. G is strictly greater than S_n Wr C_2 and so contains elements that do not preserve the blocks and therefore is primitive. G contains a three cycle and odd elements and so by Lemma [11] is the whole of S_{2n} for $n \geq 3$. When $n = 2$ inspection shows that S_n Wr C_2 is also maximal in S_{2n}. When $n = 1$ S_{2n} and S_nWr C_2 coincide. □

Theorem 6.5. *$C\widehat{yc}^2(D)$ is the group of modular permutations on $\mathbb{N}_0$ and is therefore cycle-closed.*

Proof: As before we will analyze the action on the residue classes of $\mathbb{Z}$ and $\mathbb{N}_0$. The group $Cyc^3(C_\infty)$ is contained in $C\widehat{yc}^2(D)$. Elements of this group act as modular permutations on each end of the integers so we can now induce any

permutation on the set $\{\bar{1}, \bar{2}, \ldots, \bar{n}\}$ and at the same time any permutation on the set $\{\tilde{1}, \tilde{2}, \ldots, \tilde{n}\}$. We can still exchange these sets via the reflection τ and hence S_n Wr $C_2 \leq \Theta_{2n}(C\widehat{yc}(D) \cap M_{2n}(\mathbb{N}_0))$. However this is a strict inequality as the following is an example of an element that is not in S_nWr C_2. We will consider a permutation $m \in Cyc^2(C_\infty)$ pictured in Figure 6.6 acting on $\mathbb{Z}$.

$$(x)m = \begin{cases} x+3 & : \quad x = 0 \ (\mod 2) \\ x-1 & : \quad x = 1 \ (\mod 2) \end{cases}$$

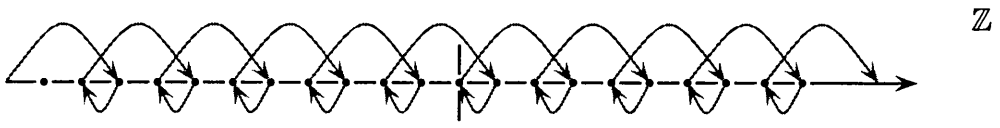


Figure 6.6:

The permutation $m\tau \in C\widehat{yc}(D)$ involves two cycles, which are pictured in figure 6.7.

$$(x)m\tau = \begin{cases} -(x+3) & : \quad x = 0 \ (\mod 2) \\ -(x-1) & : \quad x = 1 \ (\mod 2) \end{cases}$$

Each of which is itself a permutation of $C\widehat{yc}^2(D)$, and both take some positive integers to negative integers, but not all. Hence under the map F their action on the residue classes will break the block structure of S_nWrC_2. Lemma 6.4 gives us that the group $\Theta_{2n}(C\widehat{yc}^2(D) \cap M_{2n}(\mathbb{N}))$ is therefore the whole symmetric group.

The kernel of $\Theta_{2n} \leq M(\mathbb{N}_0)$ is the group of modular permutations that

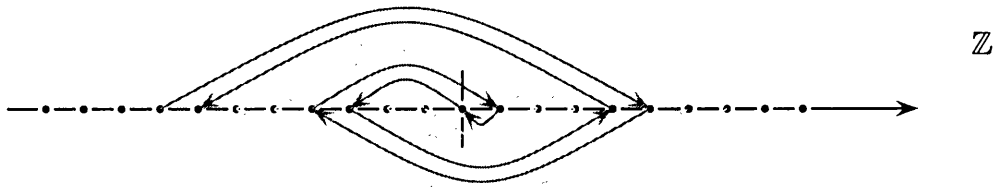


Figure 6.7:

preserve the residue classes modulo $2n$ on $\mathbb{N}_0$. For any such permutation the pre-image under F preserves the residue classes modulo n on $\mathbb{Z}$ and is modular on both ends of the integers. We know all such permutations are contained in the group $Cyc^3(C_\infty)$ and hence are in $C\widehat{yc}^2(D)$, so in the action on $\mathbb{N}_0$, $C\widehat{yc}^2(D) = M(\mathbb{N})$. □

Chapter 7

Other infinite groups

7.1 Finitary groups

Obviously the group $FS(\mathbb{Z})$ of finitary permutations on $\mathbb{Z}$ is cycle closed. The following lemma and theorem from Cameron's paper [2] will be necessary later.

Lemma 7.1. *Let g and h be permutations on Ω both of which are prime cycles, such that their supports are neither equal nor disjoint. Then the group generated by the cycles g and h has even order.*

Proof: Let $G := \langle g, h \rangle$ and $\omega \in \mathrm{Supp}(h)$. The conjugates of g by powers of h generate a group,in which the stabilizer of ω is transitive on $\Omega \backslash \{\omega\}$. Hence G is two transitive and therefore has even order. □

Theorem 7.2. *If G is an infinite transitive permutation group on Ω, then $Cyc^3(G)$ contains $FS(\Omega)$.*

Proof: The proof is similar to the finite case. If G is imprimitive and contains

some element that acts as a finite cycle on blocks, then the finite argument can be used. If G is imprimitive and moves blocks only in infinite cycles, then the elements that move the blocks must do so with more than one cycle and therefore these are not blocks of $Cyc(G)$.

Suppose that G is primitive. If G involves a cycle of finite length, then $Cyc(G)$ contains a prime cycle g. The support of g is not a block of $Cyc(G)$ and therefore there is some conjugate of g whose support is neither equal to nor disjoint from the support of g. By Lemma 7.1 $Cyc(G)$ contains a subgroup of even order giving that $Cyc^2(G)$ contains a transposition and $Cyc^3(G)$ contains $FS(\Omega)$. We have already seen that $Cyc^3(C_\infty)$ contains all finitary permutations and therefore if G involves only infinite cycles, the theorem still holds.□

The above theorem shows in particular that all finitary groups G are such that $Cyc^3(G) = Cyc^4(G)$.

7.2 Finite flow permutations

We now give another example of a cycle closed subgroup of $\mathrm{Sym}(\mathbb{Z})$.

Definition. *For a permutation p and each $n \in \mathbb{Z} + \frac{1}{2} := \{x + \frac{1}{2} | x \in \mathbb{Z}\}$ define two maps from $Sym(\mathbb{Z})$ to $\mathbb{N}$ by*

$$\Phi_n^+(p) := |\{i \in \mathbb{Z} | i < n, (i)p > n\}| \text{ and}$$

$$\Phi_n^-(p) := |\{i \in \mathbb{Z} | i > n, (i)p < n\}|.$$

A permutation $p \in Sym(\mathbb{Z})$ is said to have finite flow if $\Phi_n^+(p)$ and $\Phi_n^-(p)$ are finite for all $n \in \mathbb{Z} + \frac{1}{2}$.

For a permutation p with finite flow let $\Phi_n(p) = \Phi_n^+(p) - \Phi_n^-(p)$.

Theorem 7.3. *For a given p with finite flow, the value of $\Phi_n(p)$ is constant for all $n \in \mathbb{Z} + \frac{1}{2}$.*

Proof: Let $n, m \in \mathbb{Z} + \frac{1}{2}$ with $n < m$ and note that as there are only finitely many integer points between n and m

$$\begin{aligned} &|\{i \in \mathbb{Z} | i < n, n < (i)p < m\}| \quad + \quad |\{i \in \mathbb{Z} | m < i, n < (i)p < m\}| \\ = &|\{i \in \mathbb{Z} | n < i < m, (i)p < n\}| \quad + \quad |\{i \in \mathbb{Z} | n < i < m, m < (i)p\}|. \end{aligned}$$

So that

$$\begin{aligned} \Phi_n(p) &= \Phi_n^+(p) - \Phi_n^-(p) \\ &= |\{i \in \mathbb{Z} | i < n, n < (i)p < m\}| + |\{i \in \mathbb{Z} | i < n, m < (i)p\}| \\ &\qquad -|\{i \in \mathbb{Z} | n < i < m, (i)p < n\}| - |\{i \in \mathbb{Z} | i > m, (i)p < n\}| \\ &= |\{i \in \mathbb{Z} | n < i < m, m < (i)p\}| + |\{i \in \mathbb{Z} | i < n, m < (i)p\}| \\ &\qquad -|\{i \in \mathbb{Z} | m < i, n < (i)p < m\}| - |\{i \in \mathbb{Z} | i > m, (i)p < n\}| \\ &= \Phi_m^+(p) - \Phi_m^-(p) = \Phi_m(p). \end{aligned}$$

□

As the **flow** of a finite flow permutation is constant for all $n \in \mathbb{Z} + \frac{1}{2}$ we can talk unambiguously of the flow of a permutation, and write $\Phi_n(p)$ as $\Phi(p)$.

Theorem 7.4. *If two permutations $p, q \in Sym(\mathbb{Z})$ have finite flow, then the product pq also has finite flow. In fact $\Phi(pq) = \Phi(p) + \Phi(q)$.*

Proof: Let $p, q \in Sym(\mathbb{Z})$ be permutations with finite flow and $n \in \mathbb{Z} + \frac{1}{2}$, then $\Phi_n^+(pq) - \Phi_n^-(pq) =$

$$\begin{aligned}
&\Big(\big|\{i \in \mathbb{Z} | i < n, (i)p > n\}\big| + \big|\{i \in \mathbb{Z} | i < n, (i)p < n, (i)pq > n\}\big| \\
&-\big|\{i \in \mathbb{Z} | i < n, (i)p > n, (i)pq < n\}\big|\Big) \\
&-\Big(\big|\{i \in \mathbb{Z} | i > n, (i)p < n\}\big| + \big|\{i \in \mathbb{Z} | i > n, (i)p > n, (i)pq < n\}\big| \\
&-\big|\{i \in \mathbb{Z} | i > n, (i)p < n, (i)pq > n\}\big|\Big)
\end{aligned}$$

$$\begin{aligned}
= \ &\big|\{i \in \mathbb{Z} | i < n, (i)p > n\}\big| - \big|\{i \in \mathbb{Z} | i > n, (i)p < n\}\big| \\
&+\Big(\big|\{i \in \mathbb{Z} | i < n, (i)p < n, (i)pq > n\}\big| + \big|\{i \in \mathbb{Z} | i > n, (i)p < n, (i)pq > n\}\big|\Big) \\
&-\Big(\big|\{i \in \mathbb{Z} | i < n, (i)p > n, (i)pq < n\}\big| + \big|\{i \in \mathbb{Z} | i > n, (i)p > n, (i)pq < n\}\big|\Big)
\end{aligned}$$

$$\begin{aligned}
= \ &\big|\{i \in \mathbb{Z} | i < n, (i)p > n\}\big| - \big|\{i \in \mathbb{Z} | i > n, (i)p < n\}\big| \\
&+\big|\{i \in \mathbb{Z} | i < n, (i)q > n\}\big| - \big|\{i \in \mathbb{Z} | i > n, (i)q < n\}\big|
\end{aligned}$$

$$= \Phi_n^+(p) - \Phi_n^-(p) + \Phi_n^+(q) - \Phi_n^-(q)$$

Hence $\Phi(pq) = \Phi(p) + \Phi(q)$ as required. □

Also we have $\Phi(p^{-1}) = -\Phi(p)$, so the elements of $Sym(\mathbb{Z})$ that have finite flow form a group. Moreover this group is cycle closed as if c is a cycle involved

in a permutation p, then $\Phi_n^+(c) \leq \Phi_n^+(p)$.

Another example of an infinite cycle closed group is the group of elements of Sym($\mathbb{Z}$) which have bounded movement. By bounded movement we mean that for a permutation g there exist a constant k_g such that for all $x \in \mathbb{Z}$ $|x - (x)g| \leq k_g$.

7.3 Permutations with "modular ends"

Recall that if C_∞ is the infinite cyclic group, then $C\widehat{yc}^3(C_\infty)$ (where $C\widehat{yc}(G) := \langle Cyc(G), G\rangle$) is the set of all permutations g of $\mathbb{Z}$ for which there exist $r > 0$ and h_+,h_- modular permutations of $\mathbb{Z}$, such that $(x)g = (x)h_+$ for $x > r$ and $(x)g = (x)h_-$ for $x < -r$. This group $C\widehat{yc}^3(C_\infty)$ will be denoted by $ME(\mathbb{Z})$ as it contains permutations with "modular ends". We will now consider finitely generated transitive subgroups of $ME(\mathbb{Z})$ and show that they have a cyclizer sequence of length at most six.

Consider an infinite cycle $p \in ME(\mathbb{Z})$ such that Supp(p) = $\mathbb{Z}$. We can reorder the integers via a bijection ρ so that $((x)\rho)p = (x)\rho + 1$. Now on the reordered integers $\mathbb{Z}_\rho$, the permutation p is the infinite cycle that we have studied before and therefore $C\widehat{yc}^3(\langle p\rangle) = ME(\mathbb{Z}_\rho)$. As p has modular ends so must the bijection ρ, so the group $ME(\mathbb{Z}_\rho)$ is the same as the group $ME(\mathbb{Z})$.

Recall that when looking at modular permutations we defined the *period* of repetition as the size of the smallest set of consecutive integers on which the permutation can be defined. We then looked at the natural subgroups $M_n(\mathbb{Z})$ of $M(\mathbb{Z})$ consisting of permutations with period a factor of n. A homomorphism, $\Phi_n : M_n(\mathbb{Z}) \mapsto S_n$ was defined by looking at how residue classes modulo

n are permuted. We can define a similar homomorphism on the group $ME(\mathbb{Z})$. There are two periods associated with a permutation from the group $ME(\mathbb{Z})$, that of the modular permutation on the negative end of the integers *(the negative period)* and that of the permutation on the positive end of the integers *(the positive period)*. The group $ME(\mathbb{Z})$ therefore has subgroups $ME_{m,n}(\mathbb{Z})$ of elements whose negative period is a factor of m and positive period is a factor of n. We can now define a homomorphism $\chi_{m,n} : ME(\mathbb{Z}) \mapsto S_m \times S_n$. If $g \in ME_{m,n}(\mathbb{Z})$, then there exists $r \in \mathbb{Z}$ and $g_- \in M_m(\mathbb{Z}), g_+ \in M_n(\mathbb{Z})$ such that for all $x \geq r$ $(x)g = (x)g_+$ and for all $x \leq -r$ $(x)g = (x)g_-$. We then define $\chi_{m,n}(g) = \Phi_m(g_-) \times \Phi_n(g_+)$. Where $\Phi_n : M_n(\mathbb{Z}) \mapsto S_n$ as above. Let $R_{m,n}(\mathbb{Z})$ be the kernel of $\chi_{m,n}$ and note that this is the group of elements g as above such that $g_- \in R_m(\mathbb{Z}) := Ker(\Phi_m)$ and $g_+ \in R_n(\mathbb{Z}) := Ker(\Phi_n)$.

For the remainder of this section G is a transitive subgroup of $ME(\mathbb{Z})$ with finite generating set $\{g_1, \ldots, g_n\}$. If all elements of G involve only finite cycles, then we have already seen that $C\widehat{yc}^3(G) = FS(\mathbb{Z})$, so assume that there is an element in G involving the infinite cycle c.

Let M (respectively N) be the lowest common multiple of the negative periods (positive periods) of the permutations $g_1, \ldots, g_n$ and the cycle c, hence $G \leq ME_{N,M}(\mathbb{Z})$.

Theorem 7.5. *The group $R_{M,N}$ is a subgroup of $C\widehat{yc}(G)$*

Proof: We consider just the positive end of the integers as similar results will hold for the negative end. It is sufficient to show that there exists an element

of G which involves a cycle

$$(\underbrace{\ldots\ldots\ldots\ldots\ldots}_{\text{any permutation permitted}},\ x_0,\ x_0+N,\ x_0+2N,\ x_0+3N,\ \underbrace{\ldots\ldots\ldots\ldots\ldots}_{\text{pattern repeats}})$$

for some $x_0 \in \mathbb{Z}$. Such a cycle does occur in a power of the cycle c as we know that the positive period of c is some factor of N. This cycle is involved in an element of G and will therefore be an element of the group $C\widehat{yc}(G)$. As the group G is transitive we can conjugate this cycle to take x_0 to any integer. These cycles together will generate the group $R_{M,N}$. □

Lemma 7.6. *If H is a primitive permutation group on a finite set Ω such that there exists $\Delta \subset \Omega$, $|\Delta| > 1$, with $Sym(\Delta) \leq H$, then $H = Sym(\Omega)$.*

Proof: Let Δ be the largest subset of Ω such that $Sym(\Delta) \leq H$. As H is primitive there exists $h \in H$ such that $(\Delta)h \cap \Delta$ is non empty and not equal to Δ. Hence $\langle K, h^{-1}Kh\rangle \cong Sym(\Delta \cup (\Delta)h)$. Thus contradicts the hypothesis so H is the full symmetric group on Ω. □

Theorem 7.7. *The group $\chi_{M,N}(C\widehat{yc}^3(G) \cap ME_{M,N}(\mathbb{Z})) = S_M \times S_N$.*

Proof: Let $\chi_{M,N}(C\widehat{yc}^3(G) \cap ME_{M,N}(\mathbb{Z})) = H_1 \times H_2$ and $\chi_{M,N}(G) = K_1 \times K_2$. The groups K_i are finite and transitive, hence $C\widehat{yc}^3(K_i)$ are primitive. This gives us that

$$\begin{aligned} C\widehat{yc}^3(\chi_{M,N}(G)) &= C\widehat{yc}^3(K_1) \times C\widehat{yc}^3(K_2) \\ &\leq \chi_{M,N}(C\widehat{yc}^3(G) \cap ME_{M,N}(\mathbb{Z})) = H_1 \times H_2 \end{aligned}$$

so the groups H_i are primitive. We also know that $C\widehat{yc}^3(\langle c\rangle) = ME(\mathrm{Supp}(c))$ so the groups H_i satisfy the conditions of the above lemma and are therefore S_M and S_N respectively. □

Corollary 7.8. *The group $ME_{M,N}$ is a subgroup of $C\widehat{yc}^3(G)$.*

Proof: We saw above that $R_{N,M} \leq C\widehat{yc}^2(G) \leq C\widehat{yc}^3(G)$ and also

$$\chi_{m,n}(C\widehat{yc}^3(G) \cap ME_{m,n}(\mathbb{Z})) = S_m \times S_n$$

from which the result follows. □

In particular the group $C\widehat{yc}^3(G)$ contains the infinite cycle σ where

$$(x)\sigma = x + 1 \ \ \forall x \in \mathbb{Z}.$$

Therefore

$$\langle\sigma\rangle \leq C\widehat{yc}^3(G)$$
$$ME(\mathbb{Z}) = C\widehat{yc}^3(\langle\sigma\rangle) \leq C\widehat{yc}^6(G) \leq ME(\mathbb{Z})$$

and G has reached a cycle closed group after taking cyclizers at most six times.

Chapter 8

Conclusions and open problems

This thesis replicates and then extends the work of Peter Cameron's paper [2]. (Replication occurred as the author was unaware of the existence of the paper until after completing the work on finite groups and the second cyclizer of the infinite cyclic group.) In the study of cyclizers of finite groups we determine the maximum length of a cyclizer sequence and those groups which have cyclizer sequences of maximal length, in doing so we answer the question "which finite transitive permutation groups G satisfy $Cyc^2(G) \neq Cyc^3(G)$?" posed in the paper [2]. The investigation of cyclizers of finite groups is almost exhausted, however there remains the question of distinguishing 2-groups with cyclizer length 1 from 2-groups with cyclizer length 2. This problem would be solved by finding which groups have imprimitive cyclizers, which we leave as an open problem. Another avenue that could be explored is to look at whether the length of the cyclizer sequence of a particular group is dependent on how that group is presented as a permutation group. The section on finite groups is concluded with a summary of results in Chapter 4.

Investigation into cyclizers of infinite groups is far from exhausted. We have only looked at particular examples of infinite groups and made no new statements about cyclizers of infinite groups in general. However in investigating particular infinite groups we have highlighted the existence of some interesting infinite groups, such as the group of modular permutations and the group of permutations of finite flow. This thesis makes no contribution to answering another question from Cameron's paper, that is to determine if $Cyc^3(G) = Cyc^4(G)$ for all permutation groups G. Given the vast range of possibilities for infinite groups it seems hard to believe that this is the case. A further research project could be to try to construct a counter example to this claim.

References

[1] M.Bhattacharjee, D.Macpherson, R.G.Möller and P.M.Neumann, Notes on infinite permutation groups, Springer (1998).

[2] P.J.Cameron, Cycle-closed permutation groups, Journal of Algebraic Combinatorics (1996), 315–322.

[3] J.D.Dixon and B.Mortimer, Permutation groups, Springer (1996).

[4] The GAP Group, GAP — Groups, algorithms and programming, Version 4.3, 2002 (http://www.gap-system.org).

[5] D.A.Gewurz, Reconstruction of permutation groups from their Parker vectors, Journal of Group Theory 3 (2000), no. 3, 271–276.

[6] M.Hall, The theory of groups, The Macmillan Company (1959).

[7] G.H.Hardy and E.M.Wright, An introduction to the theory of numbers, Oxford University Press (1979).

[8] C.Lenart and N.Ray, Hopf algebras of set systems, Discrete Mathematics 180 (1998), 255–280.

[9] D.J.S.Robinson, A course in the theory of groups, Springer (1996).

[10] H.Wielandt, Finite permutation groups, Academic Press (1964).

[11] A.G.Williamson, On primitive permutation groups containing a cycle, Math. Z.,130 (1973), 159–162.

[12] R.J.Wilson, Introduction to graph theory, Oliver and Boyd (1972).

Appendix A

GAP code

Whilst none of the results in this thesis depends on computational calculations, extensive use was made of GAP [4] to investigate the cyclizer function. The following three short functions take a permutation g in cycle notation and turn it into a list of the cycles it involves, which is then used in the function `Cyc` to generate the cyclizer of a group G.

```
ListToCycle:=l->Product(List([2..Length(l)],
i->(l[1],l[i])));

ListListToCycle:=l->List([1..Length(l[1])],
i->ListToCycle(l[1][i]));


PermToCycles:=function(g) local c,d,e;
c:=LargestMovedPointPerm(g);
d:=[List([1..c],k->OrbitPerms([g],k))];
e:=ListListToCycle(d); return e; end;
```

This function is then used to write a procedure which calculates $Cyc(G)$ given G.

```
Cyc:=function(G) local n,j,x,b,c,d,U,H,J;
n:=LargestMovedPoint(G);
U:=ShallowCopy(G);
H:=ConjugacyClasses(G);
J:=List([1..Length(H)],c->Representative(H[c]));
for x in J do j:=1;
b:=PermToCycles(x);
c:=SSortedList(b);
RemoveSet(c,1);
while j<=Length(c) do d:=c[j];
U:=ClosureGroup(U,d); j:=j+1; od;
if Size(U)=Factorial(n) then break; fi;
od; return U; end;
```

GAP was particularly useful in getting a feel for which finite groups had a cyclizer sequence length of three. The following function calculates the length of the cyclizer sequence for a given group, this was used inside procedures that worked through the library of transitive groups in GAP and stored those which had a sequence of length three.

```
SeqLength:=function(G) local n,i;
i:=0; n:=LargestMovedPoint(G);
while not G=SymmetricGroup(IsPermGroup,n) do;
if i<=10 then G:=Cyc(G);
i:=i+1;
else i:=ShallowCopy(G);
G:=SymmetricGroup(IsPermGroup,n);
fi; od; return i; end;
```

It is not a very efficient program and many minor changes were made to decrease the computation time. For instance it is obviously quicker to return those groups G such that $Cyc^2(G) \neq S_n$ than to explicitly calculate $Cyc^3(G)$.

Appendix B

Swap connected groups

The work in this appendix is completely unrelated to the main body of the thesis; it is a project I worked on during my first year as a postgraduate. There is scope for further investigation of this topic, however I did not pursue this as other interests took hold.

B.1 Introduction and definitions

For a given group G we will study the relationships within $\Gamma_n(G)$ the set of generating sets for G of cardinality n.

Definition. *Let* $(\alpha_1, ...\alpha_n)$ *be an ordered generating set for our group* G. *For any permutation* π *of* $1, 2, ..., n$ *and* $\varepsilon_i = \pm 1$ *for* $i \in \{1, ..., n\}$, *let* $\phi : (\alpha_1, ..., \alpha_n) \mapsto (\alpha_{(1)\pi}^{\varepsilon_1}, ..., \alpha_{(n)\pi}^{\varepsilon_n})$, *this is a* **permutation automorphism**. *The automorphism given by* $\rho : (\alpha_1, \alpha_2, ..., \alpha_n) \mapsto (\alpha_1\alpha_j, \alpha_2, ..., \alpha_n)$ *and its inverse* $\rho' : (\alpha_1, \alpha_2, ..., \alpha_n) \mapsto (\alpha_1\alpha_j^{-1}, \alpha_2, ..., \alpha_n)$ *are* **Nielsen automorphisms**.

Definition. *Two generating sets* $\mu, \lambda \in \Gamma_n(G)$ *are* **Nielsen equivalent**, *writ-*

ten $\mu \sim_N \lambda$, if there exists a sequence of Nielsen automorphisms from one to the other.

Definition. *A* **swap** *takes one generating set to another of the same cardinality if they differ in only one element. Two generating sets $\mu, \lambda \in \Gamma_n(G)$ are* **swap equivalent**, *written $\mu \sim_S \lambda$, if there exists a sequence of swaps taking one to the other.*

It is easily seen that both $\sim_N$ and $\sim_S$ are equivalence relations. A group G will be called swap connected (Nielsen connected) if $\Gamma_n(G)$ has only one swap equivalence class (Nielsen equivalence class) for $n = rank(G)$. The term connected coming from the graph that can be constructed with $\Gamma_n(G)$ as vertex set and edges representing elementary swaps (elementary Nielsen automorphisms). Note that Nielsen equivalence implies swap equivalence but the converse does not hold. In 1992 overwhelming evidence led Raymond Tennant and Edward Turner [4] to conjecture that all groups were swap connected, but [3] showed that this is not the case. However, as we shall illustrate, there are many examples of classes of groups that are swap connected. It will also be shown that if a group of rank 2 is known to be swap connected, then the swap graph associated with that group will contain a Hamiltonian path. Lastly we shall see an example of a group that is not swap connected.

B.2 Free groups

The automorphism group of a free group of finite rank is generated by permutation and Nielsen automorphisms [2] so the free group is both Nielsen and

swap connected.

In the free abelian group

$$\frac{F_n}{[F_n, F_n]} \cong \mathbb{Z}^n$$

any generating set $\{a_1 = (\alpha_{1,1}, ..., \alpha_{1,n}), ..., a_n = (\alpha_{n,1}, ..., \alpha_{n,n})\}$ is a basis of the vector space $\mathbb{Z}^n$ and can be written as a matrix $M = (\alpha_{i,j}) \in GL_n(\mathbb{Z})$. An application of a Nielsen automorphism taking this generating set to another is equivalent to pre-multiplying by one or a combination of the following matrices:-

swap automorphisms:
$$\begin{pmatrix} 1 & 0 & . & . & . & . & 0 \\ 0 & . & & & & & \\ . & & 0 & 1 & & & \\ . & & 1 & 0 & & & \\ . & & & & . & & \\ 0 & & & & & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & . & . & . & . & 0 \\ 0 & . & & & & & \\ . & & -1 & & & & \\ . & & & & . & & \\ . & & & & & . & \\ 0 & & & & & & 1 \end{pmatrix}$$

Nielsen automorphisms:
$$\begin{pmatrix} 1 & 0 & . & . & . & . & 0 \\ 0 & . & & & & & \\ . & & 1 & . & . & 1 & \\ . & & & 1 & & & \\ . & & & & . & & \\ 0 & & & & & & 1 \end{pmatrix}$$

Theorem B.1. *For any $M_\lambda \in GL_n(\mathbb{Z})$ representing the generating set λ of $\mathbb{Z}^n$ there exists $N_\lambda = N_1 N_2 ... N_k$ such that $N_\lambda M_\lambda = I_n$ and each N_i is a Nielsen transformation.*

Proof Proof follows by induction on n. When $n = 2$ $M = (\alpha_{i,j})$ where $\{(\alpha_{1,1}, \alpha_{1,2}), (\alpha_{2,1}, \alpha_{2,2})\}$ generate $\mathbb{Z}^2$. As $\gcd(\alpha_{1,1}, \alpha_{2,1}) = 1$ Euclid's algorithm gives a method for reducing M via Nielsen transformations to $M\prime = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$.

Now pre-multiply by $\begin{pmatrix} 1 & -\frac{a}{b} \\ 0 & \frac{1}{b} \end{pmatrix}$ to get $M\prime\prime = I_2$.

Suppose now that this holds for $\mathbb{Z}^k$ and consider M representing the generating set $\{a_1, ..., a_{k+1}\}$ of $\mathbb{Z}^{k+1}$. Again $\gcd(\alpha_{1,1}, ..., \alpha_{k+1,1}) = 1$, so Euclid's algorithm gives a method of reducing M to

$$M\prime = \begin{pmatrix} 1 & a_1 & . & . & a_{k+1} \\ 0 & & & & \\ . & & & & \\ . & & & & \\ 0 & & & & \end{pmatrix}.$$

This is still a generating set so there exist a linear combination of rows 2 to

$k+1$ equal to $(0, a_1, ..., a_{k+1})$ hence $M\prime$ can be reduced to

$$M\prime\prime = \begin{pmatrix} 1 & 0 & . & . & 0 \\ 0 & & & & \\ . & & & & \\ . & & & & \\ 0 & & & & \end{pmatrix}$$

and thus by induction to I_{k+1}. □

Corollary B.2. *$\mathbb{Z}^n$ has only one Nielsen equivalence class (and therefore only one swap class).*

Proof If M_λ and M_μ represent generating sets λ and μ for $\mathbb{Z}^n$, then there exists N_λ, N_μ such that $N_\lambda M_\lambda = I_n = N_\mu M_\mu$. Thus $N_\mu^{-1} N_\lambda M_\lambda = M_\mu$ and so M_λ and M_μ are Nielsen equivalent. □

If G is a group of rank n such that for any epimorphism $\phi : F_n \to G$ $\phi(\Gamma(F_n)) = \Gamma(G)$ holds, then it follows from swap connectedness of F_n that G is swap connected.

B.3 The primitive property

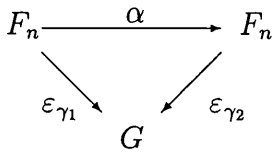
Definition. *For $\gamma \in \Gamma_n(G)$ let ε_γ be the natural epimorphism from F_n to G. An element $g \in G$ is said to be primitive if it is contained in some minimal generating set for G, a set is said to be primitive if it is a subset of some*

minimal generating set for G (here minimal generating set is taken to mean that the set contains no redundant elements). Let $Prim(G), Prim_k(G)$ be the set of primitive elements and the set of primitive sets of cardinality k respectively. Say that a group G has **primitive property** *(k-**primitive property**) if $\varepsilon_\gamma(Prim(F_n)) = Prim(G)$ ($\varepsilon_\gamma(Prim_k(F_n)) = Prim_k(G)$) for all γ.*

The following proposition and theorem are from [4].

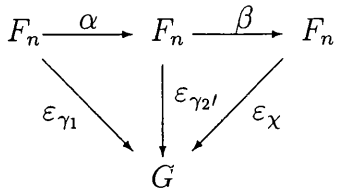
Proposition B.3. *The k-primitive property of G does not depend on the choice of generating set γ. Furthermore, G has the k-primitive property if and only if for any ordered $\gamma, \gamma' \in \Gamma_n(G)$, there is a $\gamma'' \sim_N \gamma'$ such that γ'' agrees with γ in the first k entries.*

Proof We use the fact that $\gamma_1 \sim_N \gamma_2$ if and only if there is an automorphism α of F_n such that the following diagram commutes.



It then follows that the k-primitive property of G relative to γ depends only on the Nielsen class of γ. Now let γ_1, γ_2 be elements of $\Gamma_n(G)$, $\gamma_1 = (g_1, ..., g_n)$ and suppose that G has k-primitive property relative to γ_2. Let $\{w_1, ..., w_n\} \in \Gamma(F_n)$ ($F_n = F[x_1, ..., x_k]$) be a primitive set such that $\varepsilon_{\gamma_2}(w_i) = g_i \forall 1 \leq i \leq k$, define $\alpha \in \mathrm{Aut}(F_n)$ by $\alpha(x_i) = w_i$ and let $\gamma_2\prime = \{\varepsilon_{\gamma_2}(\alpha(x_i)) | 1 \leq i \leq n\}$. Then $\gamma_2\prime$ agrees with γ_1 in the first k entries of n and since $\gamma_2\prime \sim_N \gamma_2, G$ has the k-primitive property relative to $\gamma_2\prime$. For any $\{h_1, ..h_k\} \subset \{h_1, ..h_n\} = \chi \in \Gamma_n(G)$, we can similarly get an automorphism β so that in the following diagram, the

right hand triangle commutes on the subgroup $F[x_1, ..., x_k]$.



But since α is the identity on $F[x_1, ..., x_k]$, the large triangle commutes as well; thus $\{h_1, ..h_k\} = \epsilon_{\gamma_1}\{x_1, ..., x_k\}$ and G has the k-primitive property relative to γ_1.

Theorem B.4. *If $r(G) = n$ and G has the $(n-1)$-primitive property, then any two minimal generating sets are swap equivalent.*

Suppose γ_1 and γ_2 are two minimal generating sets. The preceding proposition says that γ_2 is Nielsen equivalent (and so swap equivalent) to $\gamma_2\prime$ so that $\gamma_2\prime$ agrees with γ_1 in all but the last entry. Then $\gamma_2\prime$ is swap equivalent to γ_1.

B.4 Some swap connected groups

Theorem B.5. *Finitely generated abelian groups are swap connected [4].*

Proof: A finitely generated abelian group G has canonical representation as

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{m_1} \oplus ... \oplus \mathbb{Z}_{m_k}, m_{i+1}|m_i$$

As we have already shown that free abelian groups are swap connected we may assume that $r = 0$. Let M_γ be the matrix whose rows form the generating set

γ. M_γ reduces to

$$M_{\gamma\prime} = \begin{pmatrix} a & p_2 & . & . & p_k \\ 0 & & & & \\ . & & & & \\ . & & & & \\ 0 & & & & \end{pmatrix}$$

where a generates $\mathbb{Z}_{m_1}$. Since the rows of $M_{\gamma\prime}$ generate G,

$$(0, p_2, ..., p_k) = l_1 g_1\prime + ... + l_k g_k\prime, \gamma\prime = (g_1\prime, ..., g_k\prime).$$

Considering the first coordinate, $0 \equiv l_1 a(\mathrm{mod} m_1)$. But then $l_1 \equiv 0(\mathrm{mod} m_1)$ and so $l_1 \equiv 0(\mathrm{mod} m_i)$, $1 \leq i \leq k$. Thus we can assume that $l_1 = 0$ and further reduce $M_{\gamma\prime}$ to

$$M_{\gamma\prime\prime} = \begin{pmatrix} a & 0 & . & . & 0 \\ 0 & & & & \\ . & & & & \\ . & & & & \\ 0 & & & & \end{pmatrix}.$$

At this point we can swap the first row to $(1, 0..., 0)$ and proceed as before, completing the proof by induction. This swap may be necessary as if $m \neq 2, 3, 4$ or 6, then $\mathbb{Z}_m$ has a generator $a \neq \pm 1$ and $\{1\}$ and $\{a\}$ are not Nielsen equivalent. □

Theorem B.6. *Finite p-groups are swap connected.*

Proof: By Burnside's basis theorem a finite p-group (for p prime) G is such that $\Phi(G) = G'G^p$, where $\Phi(G)$ is the Frattini subgroup of G. Thus X will generate G if and only if the image of X generates $G/G'G^p$. The group $G/G'G^p$ is abelian of exponent p and as p is prime is a vector space, thus $G/G'G^p$ is swap connected. The group $G/G'G^p$ is swap connected if and only if G is. So now we have that G is connected. □

Theorem B.7. *Finitely generated nilpotent groups are swap connected.*

Proof: A finite nilpotent group is the direct product of its unique Sylow p-groups, so we can move from one generating set to another by concentrating on each p-group one at a time and the connectedness of the p-groups will ensure that the whole group is swap connected. Similarly for a finitely generated nilpotent group$G$, X generates G if and only if X and G' generate G. The group G/G' is the cartesian product of a finite abelian group and a free abelian group of finite rank, which have already been shown to be swap connected and cartesian products of connected groups are also connected. □

B.5 Swap connected groups of rank 2

In this section all groups discussed have minimal generating sets of cardinality two. We will take a closer look at the swap graphs of rank two groups.

Definition. *For a group G the* **complement** *of any $g \in G$ is the set of elements $h \in G$ such that $\langle g, h \rangle = G$.*

Theorem B.8. *The complement, $\bar{g}$ of an element g is*

$$G \setminus \bigcup_{m \in M} m,$$

where M is the set of all maximal subgroups of G that contain g.

Proof For $h \in G \setminus \bigcup_{m \in M} m$, $\langle h, g \rangle$ is either contained in some maximal subgroup of G or it is equal to G. But due to our choice of h $\langle h, g \rangle$ cannot be contained in a maximal subgroup, therefore $\langle h, g \rangle = G$ and so $h \in \bar{g}$.

Conversely if $h \in \bigcup_{m \in M}$, then $\langle h, g \rangle$ is contained in some maximal subgroup of G and hence $\langle h, g \rangle \neq G$. □

For a group G construct a complement graph with vertex set $G \setminus \{1\}$ and edges joining elements g and h if $g \in \bar{h}$ (this is not a digraph as $g \in \bar{h}$ implies $h \in \bar{g}$). We can now construct the dual of this graph by making a dual vertex for every edge in the complement graph and joining vertices whose corresponding edges are adjacent. Notice that the dual of the complement graph is the swap graph for our group G. Swap connectedness is therefore equivalent to complement connectedness. This can be used to give another example of a swap connected group.

Theorem B.9. *Any group of order pq where $p \leq q$ are prime has a connected complement graph and hence be a swap connected group. Moreover the complement graph will have diameter 2.*

Proof: By Cauchy's theorem the group has an element, and thus a cyclic subgroup, of order q, say a. As $p \leq q$ this cyclic subgroup is maximal hence any

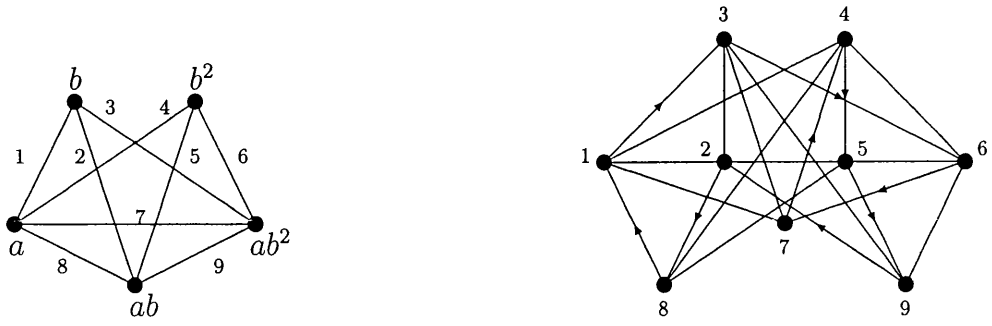


Figure B.1: *The complement and swap graph for* $D_{2.3}$. *The swap graph is shown with highlighted Hamiltonian path.*

non-identity element of $\langle a \rangle$ will be connected to all other elements of $G \backslash \langle a \rangle$. Now there exists a path of length 2 connecting any two non-identity elements of $\langle a \rangle$ via any $g_0 \in G \backslash \langle a \rangle$. Any $g, h \in G \backslash \langle a \rangle$ are connected via a. And all a^n, $1 \leq n \leq q$ are connected to all $g \in G \backslash \langle a \rangle$. The diameter is not less than two as $\langle a^n, a^m \rangle = \langle a \rangle$. □

Example. *The dihedral group of order* 6, $D_{2.3}$.

Figure B.1 shows the complement graph for $D_{2.3}$, by drawing a vertex for every edge we get its dual, the swap graph of $D_{2.3}$ also shown in this Figure.

It is clear that both are connected but also as illustrated the swap graph is Hamiltonian (there exists a closed path that passes through every vertex once and once only). This Hamiltonian path is not unique.

When is the swap graph Hamiltonian?

As taking the dual of a graph sends edges to vertices, any map that has a Eulerian path will have a Hamiltonian dual. However the converse is not true

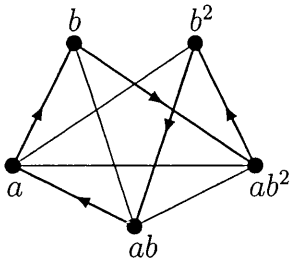


Figure B.2: *Lifting the Hamiltonian path back to the complement graph.*

as can be seen in Figure B.2. If we lift the Hamiltonian path of the swap graph to the complement graph, then we do not even get a path. What we do get contained in the lift is a closed path such that any edge not in the path is adjacent to one that is.

Theorem B.10. *A graph Γ has a Hamiltonian dual if and only if it contains a closed path such that any edge not in the path is adjacent to one that is.*

Proof

$\Leftarrow$ Given a Hamiltonian path in the dual graph it can be lifted to give either a Eulerian path in the original graph or it will contain a closed path that is adjacent to every edge.

$\Rightarrow$ If γ contains a closed path such that any edge not in the path is adjacent to one that is, then taking the dual of Γ ($D(\Gamma)$) will map this path to a closed path in $D(\Gamma)$ that either goes through every vertex or that can be adapted to go through every vertex. Consider a section of the path in Γ as in Figure B.3.

This maps to the path in $D(\Gamma)$ shown in Figure B.4.

Which can be adapted to go through all three vertices, as shown in Figure B.5.

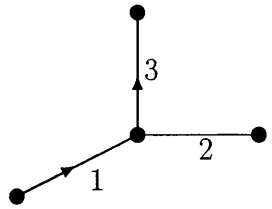


Figure B.3: *A section of a path from* Γ.

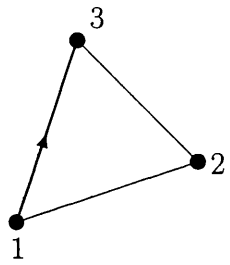


Figure B.4: *The image of this section of path in* $D(\Gamma)$.

Hence $D(\Gamma)$ is Hamiltonian.

Lemma B.11. *Any two vertices in the complement graph of* G *form one side of a triangle. (A* **triangle** *being defined as a complete graph on three vertices.)*

Proof If vertices a and b are connected by a single edge in the complement graph, then $\langle a, b\rangle = G$ therefore $\langle a, ab\rangle = \langle ab, b\rangle = G$. $ab \neq a$ and $ab \neq b$ as G is noncyclic. Hence the vertices a,b and ab form a triangle. □

Theorem B.12. *All connected complement graphs contain a closed path such that any edge not in the path is adjacent to one that is.*

Proof Let C be a circuit in the complement graph of G that does not fit the above specification, we will show that it can be added to to make a path as

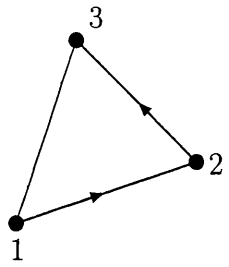


Figure B.5: *Adapting the path to go through all three vertices.*

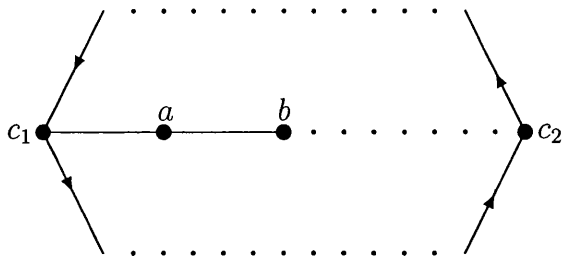


Figure B.6:

required. In G there exists vertices a and b as illustrated in Figure B.6, where the C passes through c_1 and c_2 but not a and b. □

By Lemma 1, there exists t_1 and t_2 (possibly not distinct) that form triangles with the edges c_1, a and a, b respectively. Now a path C' can be drawn that is all of C with the illustrated extra triangles included, see Figure B.7.

Note this method of creating C' will still work even if either t_1 or t_2 are already in C. In this way C can be adapted until it does fit the requirements of the theorem.

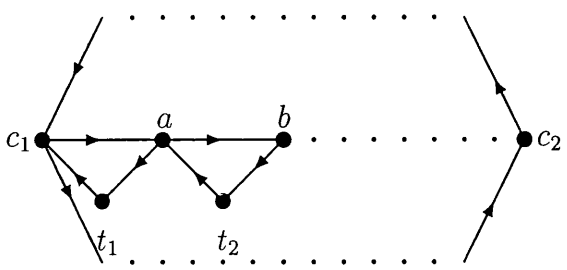


Figure B.7:

Corollary B.13. *Any group G whose complement graph is connected has a Hamiltonian swap graph.*

B.6 A group that is not swap connected

Roman'kov [3] gives an example of a group which is not swap connected and thus refutes the conjecture made by Tennant and Turner, that all groups were swap connected. What follows is a brief outline of the proof given in [3] that a free meta-abelian group of rank 3 is not swap connected.

For a group, G of rank n with presentation $< x_1, ...x_n|R >$, $(x_1, .., x_n)$ is the image of $(f_1, ..., f_n)$ the basis of the free group rank n, F_n, under the natural epimorphism from F_n to G. A basis $(g_1, ..., g_n)$ for G is called *tame* if the automorphism of G, ϕ given by $\phi : x_i \rightarrow g_i$ is the lift of an automorphism of the free group. Using previous notation $\{g_1, ..., g_n\} \in Prim_k(G)$ and so by the above section on the primitive property, groups where all bases are tame are swap connected. An automorphism of G is called *tame* if it is induced by an automorphism of the free group, hence if all automorphisms of G are tame,

then G is swap connected. For a free meta-abelian group $M_n = \frac{F_n}{F_n''}$ Bachmuth [1] and Roman'kov have shown that all automorphisms are tame when $n = 2$ or $n \geq 4$. In the exceptional case M_3 Roman'kov has shown that there exist bases that are not tame (references can be found in [3]) and it is this that leads to showing M_3 is not swap connected.

References

[1] Bachmuth, S. (1965). Automorphisms of free metabelian groups. Trans. Am. Math. Soc. no. 118, 93–104.

[2] Collins, D.J., Grigorchuk, R.I, Kurchanov, P.F. and Zieschang, H. (1998). Combinatorial group theory and applications to geometry. Springer-Verlag.

[3] Roman'kov, V.A. (1995). The swap conjecture of tennant and turner. Algebra and Logic. vol 34, no. 4.

[4] Tennant, R.F. and Turner, E.C. (1992). The swap conjecture. Rocky Mountain J. of Math. vol 22, no. 3.