MONASH UNIVERSITY

Construction and Identification of C-Groups

HONOURS THESIS

SUBMITTED TO THE SCHOOL OF MATHEMATICS

as part of the B.Sc. (Honours) degree

By

Darren Low

Supervisor: A/Prof Heiko Dietrich

July 2020

Acknowledgements

Special thanks to my supervisor Heiko for his continual support throughout the year. Much has been learnt, much more to be learnt, and this would not have been possible without him. It has been an insightful experience working together.

ABSTRACT

A C-group is a finite group whose Sylow subgroups are all cyclic. Given a positive integer n, we describe how to list all isomorphism types of C-groups of order n in a canonical ordering, such that every C-group can be uniquely identified by its size and position in this ordered list, furnishing it with an ID. This reduces isomorphism testing to a comparison of IDs. We also wish for these processes to be efficient — that construction of the i-th group in the list, and identification of a C-group's position be accomplished without having to compute the full list of groups. In 2007, Slattery [**14**] devised algorithms for the construction and identification of groups of squarefree order (groups whose orders are not divisible by any prime squared), which are a subclass of C-groups. We verify his methods and extend them to cover C-groups of all orders, coding an implementation of this for the computer algebra system GAP [**9**], which has been made publicly available at `https://github.com/heikodietrich/cgroups`. The results of this thesis are currently submitted for publication in the Journal of Group theory, and a preprint may be found at `https://arxiv.org/abs/2005.02569`.

Table of Contents

CHAPTER 1

Introduction

Mathematics is full of patterns, and to classify mathematical objects based on these patterns is often a matter of intrigue. Groups are no exception to this. The question of how many non-isomorphic groups there are of a given order traces its roots to as early as 1854, when Arthur Cayley classified the groups of orders 4 and 6 in [**3**]. However this problem becomes hard when looking at larger orders [**8**, p. 1]. As such, one frequently restricts attention to specific orders or classes of groups. For example, Netto classified groups of orders pq and p^2 in [**12**]. A more comprehensive history is collated in [**1**], which itself describes several methods for classifying and constructing "small" groups.

In this thesis, we focus on the class of C-groups. The structure of these groups is described by the Hölder-Burnside-Zassenhaus Theorem ([**13**, 10.1.10]), which shows that they are precisely those with a presentation

$$G = \langle a, b \mid b^m = a^n = 1,\ b^a = b^r \rangle$$

where m is odd, $0 \leq r < m$, $r^n \equiv 1 \pmod{m}$, and $\gcd(m, n(r-1)) = 1$. This is a generalisation of the classification for the subclass of squarefree groups, proved by Hölder [**7**] in 1895. He also proved an enumeration formula for squarefree groups, which has since been generalised to cover all C-groups by Murty & Murty much more recently in [**11**]. They establish that the number of C-groups (up to isomorphism) of order n, denoted $C(n)$, is given by

$$C(n) = \sum_{\substack{n=de \\ \gcd(d,e)=1}} \prod_{\substack{p^\alpha || d \\ p \text{ prime}}} \left(\sum_{j=1}^{\alpha} \frac{(p^{\nu(p^j,e)} - p^{\nu(p^{j-1},e)})}{p^{j-1}(p-1)} \right),$$

where ν is defined by

$$p^{\nu(p^j,e)} = \prod_{\substack{q|e \\ q \text{ prime}}} \gcd(p^j, q-1),$$

and $p^\alpha \,||\, d$ denotes the largest p-power dividing d.

While these results are certainly remarkable, it is not immediately clear how they might lead to effective methods of computing with the groups. However, for the subclass of squarefree groups, by taking a slightly different view of their structure, Slattery [**14**] devised algorithms to efficiently list, construct, and identify them, crucially describing a canonical ordering of these groups. This was implemented for the computer algebra system Magma [**2**]. The original aim of this project was to do a thorough review of Slattery's work, verifying and deciphering the theory underpinning it to see what facets might generalise to all C-groups. This included coding an implementation of his algorithms in GAP [**9**]. However, we found that a full generalisation was possible, thus we discuss the details of the general case and do not repeat it for squarefree groups. This forms part of our main result in Chapter 4: describing a canonical ordering of the C-groups of a given order n, and for any $i \in \{1, \ldots, C(n)\}$, formulating an algorithm for constructing the i-th group of order n from the canonically ordered list. We also outline the process for identifying the position of a given C-group in this list. All this will be done without constructing the full list of groups. This endows every C-group with a unique ID of the form (n, i), where n is its order, and i is its position in our listing, simplifying isomorphism testing to a comparison of IDs. Another advantage of this is that it allows one to construct an individual group dynamically, without having to store all the groups in an existing database.

Our other major result which supplements the theory is an efficient implementation of the algorithms for GAP. When restricted to squarefree groups, the efficacy of our code often appears to be better than the existing SmallGroups Library in GAP. These comparisons are discussed in Chapter 5. We refrain from including the approximately 900 lines of code here, and instead it can be found at `https://github.com/heikodietrich/cgroups`.

CHAPTER 2

Preliminaries

In this chapter we recall some preliminary group theoretic notions that appear throughout the work. We assume that the reader has taken an undergraduate course in group theory, but will occasionally refresh some concepts.

2.1. Notation

x^y	$y^{-1}xy$
$[x, y]$	$x^{-1}y^{-1}xy$
G'	Derived subgroup of G
$Z(G)$	$\{z \in G \mid \forall\, g \in G : g^z = g\}$, centre of G
$C_G(x)$	$\{c \in G \mid x^c = x\}$, centraliser of an element x in G
$C_G(H)$	$\{c \in G \mid \forall\, h \in H : h^c = h\}$, centraliser of a subgroup H in G
$\mathrm{Aut}(G)$	Automorphism group of G
$\mathrm{Hom}(G, H)$	Set of group homomorphisms from G to H.
$\varphi(n)$	Totient function; number of positive integers less than, and coprime to n.

2.2. General theory

Lemma 2.2.1. [**13**, p. 30] *If $G/Z(G)$ is cyclic, then G is abelian.*

Proof. Suppose $G/Z(G)$ is cyclic, say $G/Z(G) = \langle gZ(G)\rangle$ for some $g \in G$. Then $G = \langle g\rangle Z(G)$, and for any $a, b \in G$, we may write $a = g^i z$ and $b = g^j z'$ where $i, j \in \mathbb{Z}$, and $z, z' \in Z(G)$. Then $ab = g^i z g^j z' = z g^i g^j z' = z g^j g^i z' = g^j z' g^i z = ba$, because g^i commutes with g^j and z, z' commute with all elements of G. Hence G is abelian. □

Lemma 2.2.2. [**13**, (1.4.6)] *Let G be a group with normal subgroup N. The subgroups of G/N are of the form U/N where $N \trianglelefteq U \leq G$. Moreover, $U/N \trianglelefteq G/N$ if and only if $U \trianglelefteq G$.*

Proof. Suppose $N \trianglelefteq U \leq G$, and let $\pi : G \to G/N$ be the natural homomorphism. Then $\pi(U) = U/N$ is a subgroup of G/N. If $U \trianglelefteq G$, then for any $uN \in U/N$ and $gN \in G/N$, we have $(uN)^{gN} = u^g N \in U/N$, therefore U/N is normal. On the other hand, let $M \leq G/N$. Consider the full preimage $\pi^{-1}(M) = \{g \in G \mid gN \in M\}$. It is non-empty because $1N \in M$. For any $u, v \in \pi^{-1}(M)$, we have $uv^{-1} \in \pi^{-1}(M)$, since $uv^{-1}N = (uN)(v^{-1}N) \in M$. Therefore $\pi^{-1}(M) \leq G$. It is clear that $N \leq \pi^{-1}(M)$ and that $M = \pi^{-1}(M)/N$. If $M \trianglelefteq G/N$, then for any $g \in G$, we have $u^g N = (uN)^{gN} \in M$, so $u^g \in \pi^{-1}(M)$, and thus $\pi^{-1}(M) \trianglelefteq G$. □

Lemma 2.2.3. [**10**, p. 222] *The number of elements of order d in a finite group is a multiple of $\varphi(d)$.*

Proof. An element of order d generates a cyclic subgroup of size d, and this cyclic group has $\varphi(d)$ elements of that order. Next we show that if U and V are two such distinct subgroups, then their intersection cannot contain any elements of order d. Suppose for contradiction that $g \in U \cap V$ has order d. Then $\langle g \rangle$ has order d. But $\langle g \rangle \subseteq U \cap V$, and both U and V have order d. Hence $\langle g \rangle = U = V$, a contradiction. This means that each element of order d is in exactly one such subgroup. Hence, the total number of elements of order d is a multiple of $\varphi(d)$. □

Lemma 2.2.4. [**6**, Lemma 3.2.1] *Let G be a group, and $g \in G$ be an element of order mn, where m and n are coprime. Then we can write $g = xy = yx$, where x has order m and y has order n.*

Proof. Because m and n are coprime, there exist integers a and b such that $am + bn = 1$. Note that this implies am and bn are coprime. Then $g = g^{am+bn} = g^{am} g^{bn} = g^{bn} g^{am}$, with $x = g^{bn}$ having order m and $y = g^{am}$ having order n. □

The next theorem is a result proven in 1895 by Frobenius, originally using character theory. Now several other proofs are known, and here we present one by Khurana & Khurana [**10**] which appeals to more elementary methods.

Lemma 2.2.5. *(Frobenius' Theorem) Let G be a finite group. For any divisor d of $|G|$, the number of solutions in G to the equation $x^d = 1$ is a multiple of d.*

Proof. We prove this by induction on $|G|$ and reverse induction on its divisors d. For $|G| = 1$, there is only one divisor $d = 1$, and the claim follows trivially. Now suppose $|G| > 1$, and that the result is true for groups of order strictly less than $|G|$. The base case for the reverse induction starts with $d = |G|$, for which the result is clear.

Now suppose $d < |G|$ and that the result holds for any larger divisor of $|G|$. Let p be a prime divisor of $|G|/d$, and write $d = p^\alpha s$, where $\alpha \in \mathbb{N} \cup \{0\}$ and $\gcd(p, s) = 1$. Let $A_{dp} = \{x \in G \mid x^{dp} = 1\}$ and $A_d = \{x \in G \mid x^d = 1\}$ and consider $A = A_{dp} \setminus A_d$. We wish to show that d divides $|A_d|$. Observe that $|A_d| = |A_{dp}| - |A|$, and that by the reverse induction, $|A_{dp}|$ is a multiple of dp, and hence d, so it suffices to show that d divides $|A|$. Note that A consists precisely of the elements of G which have orders dividing $dp = p^{\alpha+1}s$ but not $d = p^\alpha s$, and these are the elements that have order $p^{\alpha+1}r$, for some $r \mid s$. For each such r, the number of elements of G with order $p^{\alpha+1}r$ is a multiple of $\varphi(p^{\alpha+1}r) = \varphi(p^{\alpha+1})\varphi(r) = p^\alpha(p-1)\varphi(r)$ by Lemma 2.2.3 . Thus p^α divides $|A|$, and it remains to show s divides $|A|$.

Because an element $x \in A$ has order $p^{\alpha+1}r$ where $\gcd(p, r) = 1$, by Lemma 2.2.4, we can write $x = yz = zy$, for some $y, z \in G$, where y and z have orders $p^{\alpha+1}$ and r respectively. For each $a \in G$ of order $p^{\alpha+1}$, define the set $S_a = \{ac \in G \mid c \in C_G(a) \text{ and } c^s = 1\}$. Then A is the union of all such S_a. We show that this union is disjoint. If there exists some $ac = bd \in S_a \cap S_b$, then $(ac)^s = (bd)^s$, which implies $a^s = b^s$. Since a and b both have order $p^{\alpha+1}$, and $\gcd(p^{\alpha+1}, s) = 1$, we can find integers i, j such that $ip^{\alpha+1} + js = 1$, which gives $a = a^{ip^{\alpha+1}+js} = b^{ip^{\alpha+1}+js} = b$. So $S_a \cap S_b = \emptyset$ if $a \neq b$, and A is the disjoint union of the various S_a. If L is set of conjugacy classes of elements with order $p^{\alpha+1}$ in G, then

$A = \bigcup_{C \in L} \bigcup_{a \in C} S_a$, and this union is disjoint, so $|A| = \sum_{C \in L} \sum_{a \in C} |S_a|$. Thus it suffices to show s divides $\sum_{a \in C} |S_a|$ for an arbitrary conjugacy class C.

Fix one such C and $a \in C$. Let $m = |C_G(a)/\langle a \rangle|$, and $e = \gcd(s, m)$. Consider the set

$$T_a = \{t \in C_G(a)/\langle a \rangle \mid t^s = 1\} = \{t \in C_G(a)/\langle a \rangle \mid t^e = 1\}.$$

Define the map $S_a \to T_a$ by $ac \mapsto c\langle a \rangle$. Let $ac, a\tilde{c} \in S_a$. If $c\langle a \rangle = \tilde{c}\langle a \rangle$, then $\tilde{c}c^{-1} \in \langle a \rangle$. The left hand side has order dividing s, but s is coprime to $p^{\alpha+1} = |\langle a \rangle|$, thus $\tilde{c}c^{-1} = 1$, and $c = \tilde{c}$. This shows the map is injective. On the other hand, let $c\langle a \rangle \in T_a$, so that $c^s\langle a \rangle = 1$, if and only if $c^s \in \langle a \rangle$. If the order of c is coprime to $p^{\alpha+1}$, then $c^s = 1$ and $ac \in S_a$. Otherwise, by Lemma 2.2.4 we can write $c = yz = yz$ with z having p-power order and y having order coprime to p. Then $y^s = 1$ and $y \in C_G(a)$, so $ay \in S_a$ is mapped to $c\langle a \rangle$. Thus the map is surjective. Having constructed a bijection from $|S_a|$ to $|T_a|$, this means $|S_a| = |T_a|$. Because $|C_G(a)/\langle a \rangle| \leq |G|$, by induction, the size of T_a is a multiple of e, say $|T_a| = ke$ for some $k \in \mathbb{N}$. Note that for any $b = a^g \in C$, the map $ac \mapsto (ac)^g = a^g c^g$ gives a bijection from S_a to S_b, so

$$\sum_{b \in C} |S_b| = |C||S_a| = |G : C_G(a)||T_a| = |G|ke/|C_G(a)| = |G|ke/p^{a+1}m.$$

Since both s and m divide $|G|$, their lowest common multiple $\operatorname{lcm}(s, m) = sm/\gcd(s, a) = sm/k$ divides $|G|$ too. This implies s divides $|G|ke/m$. As $p^{\alpha+1}$ also divides $|G|ke/m$, with $\gcd(p, s) = 1$, this means s does divide $|G|ke/p^{\alpha+1}m = \sum_{b \in C} |S_b|$, thus completing the proof. □

We conclude this section by stating von Dyck's theorem.

Theorem 2.2.6. [**8**, Theorem 2.53] *Let $\langle X \mid R \rangle$ be a presentation of a group G, and let $\Theta : X \to H$ be a map from X to a group H. If for all relators $r = x_1^{e_1} \cdots x_r^{e_r} \in R$, where each $x_i \in X$ and $e_i \in \{\pm 1\}$, we have $\Theta(x_1)^{e_1} \cdots \Theta(x_k)^{e_k} = 1_H$, then Θ can be extended uniquely to a group homomorphism $G \to H$.*

2.3. Sylow theorems

The next few results are about maximal prime order subgroups of a group, named epynomously after Norwegian mathematician Ludwig Sylow. As mentioned in the introduction, Sylow subgroups are key in understanding the structure of C-groups. The Sylow theorems are a collection of theorems regarding these Sylow subgroups, and are among the most famous results in finite group theory. We shall only state them here, and leave the details to be found in [**13**, p. 39 - 41].

Definition 2.3.1. Let G be a finite group and p be a prime divisor of $|G|$. We denote by $p^a \mid\mid |G|$ the largest p-power dividing $|G|$. A subgroup of G of order p^a is called a *Sylow p-subgroup* of G. The number of Sylow p-subgroups of G is denoted by $n_p(G)$.

Theorem 2.3.2. *(Sylow Theorems) Let G be a finite group and p be a prime divisor of $|G|$. Then the following hold.*

(1) *G has a Sylow p-subgroup,*

(2) *All Sylow p-subgroups of G are conjugate,*

(3) *$n_p(G) \equiv 1 \pmod{p}$, and $n_p(G) \mid m$, where $m = |G|/p^a$.*

Corollary 2.3.3. *Let G be a finite group and S be a Sylow p-subgroup of G. Then the following are equivalent:*

(1) *$S \trianglelefteq G$,*

(2) *$n_p(G) = 1$,*

(3) *Every subgroup of G with p-power order is contained in S,*

(4) *S is a characteristic subgroup of G.*

Lemma 2.3.4. *Let G be a finite group and $N \trianglelefteq G$. The Sylow p-subgroups of N are of the form $N \cap S$, and the Sylow p-subgroups of G/N are of the form SN/N, where S is a Sylow p-subgroup of N.*

Lemma 2.3.5. *A finite abelian group is isomorphic to the direct product of its Sylow subgroups.*

2.4. Group actions, semidirect products, and extensions

We now briefly introduce some tools used in forming new groups out of existing ones. This will be vital in the construction of C-groups. The account here again is drawn from Robinson [**13**, pp. 27, 313].

Definition 2.4.1. An *action* of a group G on a group H is a homomorphism $\sigma : G \to \mathrm{Aut}(H)$. We say that G acts on H via σ. The action is *faithful* if it has trivial kernel, and it is *transitive* if for all $x, y \in H$, there exists a $g \in G$ such that $x^{\sigma(g)} = y$.

Note that it is possible for a group to act on a general set, and not just on other groups, but this definition suffices for the purposes of this thesis.

Definition 2.4.2. Let G be a group and $N \trianglelefteq G$ a normal subgroup. A *complement* to N in G is a subgroup $K \leq G$ such that $G = KN$ and $K \cap N = 1$. We say G is the *internal semidirect product* of N and K, which we denote by $G = K \ltimes N$.

Alternatively, given groups N and K, and an action $\sigma\colon K \to \mathrm{Aut}(N)$, we can construct:

Definition 2.4.3. The *outer semidirect product* of N and K is

$$G = K \ltimes_\sigma N = \{(k, n) \mid k \in K, n \in N\}$$

with group operation $(k_1, n_1)(k_2, n_2) = (k_1 k_2, n_1^{\sigma(k_2)} n_2)$.

Remark 2.4.4. The identity of this outer semidirect product is $(1, 1)$ and inverse elements are given by $(k, n)^{-1} = (k^{-1}, (n^{-1})^{\sigma^{-1}(k)})$. Now the mappings $k \mapsto (k, 1)$ and $n \mapsto (1, n)$ are isomorphisms from K and N onto their respective images, and under these identifications we may consider G as the internal semidirect product of N and K. Note that $(1, n)^{(h,1)} = (1, n^{\sigma(h)})$, so conjugation of N by K induces the action σ. With these, the internal and external semidirect products can be seen as equivalent constructions, and we do not distinguish between the two. Furthermore, if the specific group action σ is clear or unspecified in the context, we often omit writing it.

For a semidirect product $G = K \ltimes N$, note that it has $N \trianglelefteq G$, and $G/N \cong K$. More generally, we have the following definition.

Definition 2.4.5. A *group extension* of N by K is a group E that has a normal subgroup M such that $M \cong N$, and $E/M \cong K$. Formally speaking, a group extension of N by K is a short exact sequence of groups and homomorphisms

$$1 \to N \xrightarrow{\mu} E \xrightarrow{\varepsilon} K \to 1,$$

where exactness of the sequence means the image of a homomorphism is equal to the kernel of the following homomorphism in the sequence.

Definition 2.4.6. An extension $1 \to N \xrightarrow{\mu} E \xrightarrow{\varepsilon} K \to 1$ is *split* if there exists a homomorphism $\tau\colon K \to E$ such that $\tau\varepsilon = 1$, where composition here is read from left to right.

Lemma 2.4.7. *An extension* $1 \to N \xrightarrow{\mu} E \xrightarrow{\varepsilon} K \to 1$ *splits if and only if it is a semidirect product extension.*

Proof. We have already shown that the semidirect product is a type of group extension. Moreover, the map $k \mapsto (k, 1)$ gives a homomorphism satisfying the split extension condition. Conversely, suppose $1 \to N \xrightarrow{\mu} E \xrightarrow{\varepsilon} K \to 1$ splits, so we have a homomorphism $\tau\colon K \to E$ such that $\tau\varepsilon = 1$. For any $x \in E$, we have $((x^{\varepsilon\tau})^{-1}x)^{\varepsilon} = (x^{\varepsilon})^{-1}x^{\varepsilon} = 1$, so $(x^{\varepsilon\tau})^{-1}x \in M = \operatorname{Ker}\varepsilon$. Let $X = E^{\varepsilon\tau}$. Then $x = x^{\varepsilon\tau}((x^{\varepsilon\tau})^{-1}x) \in XM$, thus $E = XM$. Moreover, if $x^{\varepsilon\tau} \in K \cap M$, we get $1 = (x^{\varepsilon\tau})^{\varepsilon} = x^{\varepsilon}$, so $x^{\varepsilon\tau} = 1$ as τ is injective. Therefore, $K \cap M = 1$ and $E = X \ltimes M \cong K \ltimes N$. □

Finally, we state a major theorem that gives us a condition for when a complement to a normal subgroup might exist. We refer to [**13**, (9.1.2)] for the proof.

Theorem 2.4.8. *(Schur-Zassenhaus theorem) Let G be a finite group and N a normal subgroup whose order is coprime to its index. Then there exist complements to N in G, and any two of them are conjugate. In other words, we can write G as a semidirect product $G = K \ltimes N$ for some $K \leq G$.*

2.5. Solvable groups

We bring the discourse onto the topic of solvable groups. These groups have a nice structure in that they can be constructed by taking extensions of abelian groups, which gives them useful properties. They were historically studied by Galois in relation to polynomials, but the theory has since expanded. Our interest in them arises because it turns out that all C-groups are solvable.

Definition 2.5.1. [**13**, p. 28] The *derived subgroup* of a group G is the subgroup G' generated by the set of all commutators $\{[x, y] = x^{-1}y^{-1}xy \mid x, y \in G\}$.

Remark 2.5.2. Recall that a quotient group G/N is abelian if and only if $G' \leq N$.

Lemma 2.5.3. [**13**, (5.1.5)] *Let x, y, z be elements of a group. Then*

(1) $[xy, z] = [x, z]^y[y, z]$;

(2) $[x, yz] = [x, z][x, y]^z$.

Proof. (1) This is a straightforward calculation:

$$\begin{aligned}
[x, z]^y[y, z] &= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz \\
&= y^{-1}x^{-1}z^{-1}xyz \\
&= (xy)^{-1}z^{-1}xyz \\
&= [xy, z].
\end{aligned}$$

(2) Likewise we have

$$\begin{aligned}[x,z][x,y]^z &= x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz \\ &= x^{-1}z^{-1}y^{-1}xyz \\ &= x^{-1}(yz)^{-1}xyz \\ &= [x,yz],\end{aligned}$$

which completes the proof. □

Definition 2.5.4. [**13**, pp. 121,124] The *derived series* of a group G is the sequence of subgroups

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots$$

where $G^{(i+1)} = (G^{(i)})'$. A group is *solvable* if its derived series reaches the trivial subgroup. An alternative characterisation is that a group G is solvable if it has an abelian series, that is, a chain of subgroups

$$1 = G_0 \leq G_1 \leq \ldots \leq G_k = G$$

where for each i, we have $G_{i+1} \trianglelefteq G_i$, and the consecutive *sections* G_i/G_{i+1} are abelian.

Lemma 2.5.5. [**6**, Corollary 9.2.1] *Let G be a group with normal subgroup $N \trianglelefteq G$. Then G is solvable if and only if N and G/N are solvable.*

Proof. ($\Rightarrow$) Suppose G has abelian series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$. Let $N_i = N \cap G_i$ for each i. Then N_i is normal in N_{i+1}, and $G_i' \leq G_{i+1}$ since G_i/G_{i+1} is abelian, so

$$N_i' = (N \cap G_i)' \leq N \cap G_i' \leq N \cap G_{i+1} = N_{i+1}.$$

Therefore N_i/N_{i+1} is abelian, and $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N$ is an abelian series for N. Consider the quotient groups G_iN/N. For any $g_iN \in G_iN/N$ and $= g_{i+1}N \in G_iN/N$,

$$(g_{i+1}N)^{g_iN} = g_{i+1}^{g_i}N \in G_{i+1}N/N,$$

thus $G_{i+1}N/N$ is normal in G_iN/N. By the Third Noether Isomorphism Theorem [**13**, 1.4.5],

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N.$$

Let $g_iG_{i+1}N$ and $h_iG_{i+1}N$ be arbitrary elements of $G_iN/G_{i+1}N$. As $G_i' \leq G_{i+1}$,

$$\begin{aligned}(g_iG_{i+1}N)(h_iG_{i+1}N) &= g_ih_iG_{i+1}N \\ &= h_ig_i[g_i,h_i]G_{i+1}N \\ &= h_ig_iG_{i+1}N \\ &= (h_iG_{i+1}N)(g_iG_{i+1}N),\end{aligned}$$

so the sections are abelian and

$$1 = G_0N/N \trianglelefteq G_1N/N \trianglelefteq \ldots \trianglelefteq G_nN/N = G/N$$

is an abelian series for G/N.

($\Leftarrow$) Now supppose G/N has abelian series $1 = M_0 \trianglelefteq M_1 \trianglelefteq \ldots \trianglelefteq M_n = G/N$. By Lemma 2.2.2 each $M_i = U_i/N$ for some $U_i \leq G$, where $N \leq U_i$ and $U_i \trianglelefteq U_{i+1}$. Using the third isomorphism theorem, $U_{i+1}/U_i \cong M_{i+1}/M_i$, so the quotient group is abelian. Note that $U_0 = N$. Then if $1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_m = N$ is an abelian series for N, we get that

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{m-1} \trianglelefteq N \trianglelefteq U_1 \trianglelefteq \ldots \trianglelefteq U_n = G$$

is an abelian series for G, hence G is solvable. □

Lemma 2.5.6. [**6**, 146] *Let $G = G^0 \geq G^{(1)} \geq G^{(2)} \geq \ldots$ be the derived series of G. If for some $i \geq 1$ the consecutive sections $G^{(i)}/G^{(i+1)}$ and $G^{(i+1)}/G^{(i+2)}$ are both cyclic, then $G^{(i+1)}/G^{(i+2)} = 1$.*

Proof. First note that the following two series

$$G^{(i)} \geq G^{(i+1)} \geq G^{(i+2)}$$

and

$$G^{(i)}/G^{(i+2)} \geq G^{(i+1)}/G^{(i+2)} \geq G^{(i+2)}/G^{(i+2)} = 1$$

have isomorphic sections, hence we may assume without loss of generality that $G^{(i+2)} = 1$. Then $G^{(i+1)} \cong G^{(i+1)}/G^{(i+2)}$ is cyclic, and it remains to show $G^{(i+1)} = 1$. Note that $G^{(i+1)}$ is normal in G, and so G acts via conjugation on $G^{(i+1)}$, which induces a faithful action of $G/C_G(G^{(i+1)})$ on $G^{(i+1)}$. Thus $G/C_G(G^{(i+1)})$ is embedded into $\mathrm{Aut}(G^{(i+1)})$ which is abelian since $G^{(i+1)}$ is cyclic. This implies $G' = G^{(1)}$ is contained in $G_G(G^{(i+1)})$, and so $G^{(i)} \leq G^{(1)} \leq C_G(G^{(i+1)})$, which means all elements of $G^{(i+1)}$ commute with all elements of G^i. In other words, $G^{(i+1)} \leq Z(G^{(i)})$. Then $G^{(i)}/Z_G(G^{(i)}) \cong (G^{(i)}/G^{(i+1)})/(Z_G(G^{(i)})/G^{(i+1)})$ is cyclic, being isomorphic to a quotient of the cyclic group $G^{(i)}/G^{(i+1)}$, so $G^{(i)}$ is abelian by Lemma 2.2.1, and therefore $G^{(i+1)} = 1$. □

Definition 2.5.7. [**8**, p. 273] A group is *polycyclic* if it has an abelian series in which the sections are cyclic on top of being abelian. This series is called a *polycyclic series*. An equivalent definition of a polycylic group is a solvable group whose subgroups are all finitely generated.

As C-groups are finite and solvable, they are also polycyclic. By [**8**, Theorem 8.8], a polycyclic group admits a special presentation, called a polycyclic presentation.

Definition 2.5.8. [**8**, Definition 8.7] A presentation $\langle x_1, \ldots, x_n \mid R \rangle$ is a *polycyclic presentation* if there exists a sequence $S = (s_1, \ldots, s_n)$ where $s_i \in \mathbb{N} \cup \{\infty\}$, and integers $a_{i,k}, b_{i,j,k}, c_{i,j,k}$ such that the relations in R are:

$$\begin{aligned} x_i^{s_i} &= x_{i+1}^{a_{i,i+1}} \ldots x_n^{a_{i,n}} \text{ for } 1 \leq i \leq n \text{ and } s_i < \infty, \\ x_i^{x_j} &= x_{j+1}^{b_{i,j,j+1}} \ldots x_n^{b_{i,j,n}} \text{ for } 1 \leq j < i \leq n, \\ x_i^{x_j^{-1}} &= x_{j+1}^{c_{i,j,j+1}} \ldots x_n^{c_{i,j,n}} \text{ for } 1 \leq j < i \leq n. \end{aligned}$$

The relations of the first type are called *power relations*, while the latter two are called *conjugate relations*. Lastly, S is called the sequence of *power exponents* of the presentation.

Remark 2.5.9. The relations of the third type are redundant if the power exponents are finite [**8**, Lemma 8.20]. In that case we may omit them. It is also typical to omit *trivial conjugate relations*: those of the form $x_i^{x_j} = x_i$. With this, it is necessary to distinguish these polycyclic presentations from standard group presentations, and we write $\mathrm{Pc}\langle x_1, \ldots, x_n \mid R\rangle$ for a polycyclic presentation.

A group that is defined by a polycyclic presentation is called a PC-group, and this type of presentation is very practical to compute with, which is why we will opt to represent C-groups as PC-groups. Furthermore, we can make this presentation refined — each of the power exponents being prime [**8**, Lemma 8.17]. Several results and algorithms for computing with (refined) PC-groups are known, and we refer to the Handbook of Computational Group Theory [**8**, Chapter 8] for these details.

CHAPTER 3

Structure and enumeration of C-groups

This chapter unpacks some of the underlying structure of C-groups that plays a role in the algorithms described later on. We also relate this to the enumeration of C-groups.

3.1. Structure results

Lemma 3.1.1. *The class of C-groups is closed under the operations of taking subgroups and quotients.*

Proof. The first statement follows from the fact that a Sylow subgroup of any subgroup is contained in some cyclic Sylow subgroup of the original group. The second statement is a consequence of Lemma 2.3.4. □

Lemma 3.1.2. *An abelian C-group is cyclic.*

Proof. Let G be an abelian C-group. By Lemma 2.3.5, it is the direct product of its Sylow subgroups. Since Sylow subgroups of G are all cyclic and their orders are coprime, G is also cyclic, by the Chinese Remainder Theorem. □

Theorem 3.1.3. [**6**, 146-147] *Every C-group is solvable.*

Proof. Let G be a C-group, and write the prime factorisation $|G| = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ with $p_1 < \ldots < p_r$ primes, and each $e_i \in \mathbb{N}$. Let $m = p_i^{f_i} p_{i+1}^{e_{j+1}} \ldots p_r^{e_r}$, where $f_i \leq e_i$, with this inequality strict if $i = 1$. This is so that $m < |G|$. If $f_i = e_i$, set $p = p_{i-1}$, and if $f_i < e_i$, set $p = p_i$, so that pm divides $|G|$. We show that if $x^{pm} = 1$ has exactly pm solutions in G, then $x^m = 1$ has exactly m solutions in G.

Supposing the former, if p^f is the largest p-power dividing pm, since a Sylow p-subgroup of G is cyclic, there exist elements of G with order p^f, so the set of solutions

to $x^m = 1$ is strictly contained in the set of solutions to $x^{pm} = 1$. By Lemma 2.2.5 there are km solutions in G to $x^m = 1$ for some $k \in \mathbb{N}$, so the number of elements satisfying $x^{pm} = 1$ but not $x^m = 1$ is $pm - km = (p-k)m$, where $k < p$. If $p = 2$, then $k = 1$ and we have shown that $x^m = 1$ has $2m - m = m$ solutions in G. Now assume p is odd, and note that an element satisfying $x^{pm} = 1$ but not $x^m = 1$ must have order which divides pm but not m, so we can write its order as $p^f a$, for some $a \mid m$. For each such divisor a, the number of elements of order $p^f a$ is a multiple of $\varphi(p^f a) = \varphi(p^f)\varphi(a) = p^{f-1}(p-1)\varphi(a)$. In particular, it is a multiple of $(p-1)$, say $l_a(p-1)$ for some $l_a \in \mathbb{N}$. Since this holds for each such a, we get that $(p-k)m = \sum_{a|m} l_a(p-1) = (p-1)\sum_{a|m} l_a$, so $(p-1) \mid (p-k)m$. Observe that $(p-1)$ cannot divide m because p is the smallest prime divisor of pm, so $(p-1)$ must divide $(p-k)$. But as $1 \leq k < p$, this forces $k = 1$, and thus $x^m = 1$ has exactly m solutions. This finishes the proof that if $x^{pm} = 1$ has exactly pm solutions in G, then $x^m = 1$ has exactly m solutions in G, which allows us to proceed with proving the claim of the theorem.

Clearly $x^{|G|} = 1$ has $|G|$ solutions in G. Applying the above result repeatedly, we find that $x^{(p_r^{e_r})} = 1$ has exactly $p_r^{e_r}$ solutions, which implies there is a unique Sylow p_r-subgroup $S \trianglelefteq G$. Then S and G/S are both C-groups, and by induction on the size of the group, they are solvable, hence G is solvable by Lemma 2.5.5. □

Through the proof of the previous theorem, we have also shown the following corollary.

Corollary 3.1.4. *If G is a C-group of size $|G| = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ with $p_1 < \ldots < p_r$ primes, then G has a normal Sylow p_r-subgroup. By induction on the group order, we see that G can be constructed by iteratively making split extensions with cyclic groups of prime power order $p_i^{e_i}$, with $i \in \{1, \ldots, r\}$ increasing. In particular, this shows that G has a polycyclic presentation where the generators have prime-power orders. This can be further refined to make G a refined PC-group.*

We are now ready to prove Hölder's famous classification theorem for C-groups.

Theorem 3.1.5. [**6**, 146-148] *(Hölder, Burnside, Zassenhaus). Every C-group G has a presentation of the form*

$$G \cong G_{m,n,r} = \langle a, b \mid b^m = a^n = 1,\ b^a = b^r \rangle$$

where m is odd, $0 \leq r < m$, $r^n \equiv 1 \pmod{m}$, and $\gcd(m, n(r-1)) = 1$.

Proof. If G is abelian, it is cyclic by Lemma 3.1 and we simply choose $n = |G|$, $m = 1$, and $r = 0$. Now suppose G is not abelian and consider its derived series

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(d)} = 1.$$

The sections G_i/G_{i+1} are abelian, and they are also C-groups by Lemma 3.1.1. Hence each G_i/G_{i+1} is cyclic by Lemma 3.1. Then $G^{(2)}/G^{(3)} = 1$ by Lemma 2.5.6. Since G is solvable, the derived series has to reach 1, so two consecutive derived subgroups are identical if and only if they are both trivial, otherwise the series would repeat indefinitely. Thus $G^{(2)} = 1$ and $G' = G^{(1)}$ is cyclic.

We then write $G' = \langle b \rangle$ and $G/G' = \langle aG' \rangle$ for some $a, b \in G$, and $G = \langle a, b \rangle$. Let $m = |G'|$ and $n = |G/G'|$, such that $|G| = mn$. As G' is normal, conjugation of b by a defines an automorphism of $\langle b \rangle$, where $b^a = b^r$ for some $1 \leq r < m$. Note that this also tells us $\gcd(m, r) = 1$. Furthermore, $b^{(r^n)} = b^{(a^n)} = b$, so $b^{r^n - 1} = 1$, which implies $m \mid (r^n - 1)$, or equivalently $r^n \equiv 1 \pmod{m}$.

Next recall that $\langle b \rangle = G'$ is generated by all commutators of G, each of which have the form $[a^i b^j, a^k b^l]$ for some positive integers i, j, k, l. By expanding using the commutator

identities described in Lemma 2.5.3, we find

$$\begin{aligned}
[a^ib^j, a^kb^l] = [a^i, a^kb^l]^{b^j}[b^j, a^kb^l] &= ([a^i, b^l][a^i, a^k]^{b^l})^{b^j}[b^j, b^l][b^j, a^k]^{b^l} \\
&= [a^i, b^l][b^j, a^k] \\
&= (b^{-l})^{a^i}b^lb^{-j}(b^j)^{a^k} \\
&= b^{lr^i}b^lb^{-j}b^{jr^k} \\
&= b^{-l(r^i-1)}b^{j(r^k-1)} \\
&= b^{-l(r^0+\ldots+r^{i-1})(r-1)}b^{j(r^0+\ldots+r^{k-1})(r-1)} \in \langle\, b^{r-1} \,\rangle,
\end{aligned}$$

so $\langle b\rangle \leq \langle b^{r-1}\rangle$. Moreover, $[b, a] = b^{-1}a^{-1}ba = b^{r-1} \in G'$, so $\langle b^{r-1}\rangle \leq \langle b\rangle$. Therefore $\langle b^{r-1}\rangle = \langle b\rangle$, so $\gcd(m, r-1) = 1$. We showed before that $\gcd(m, r) = 1$. As either r or $r-1$ is even, this means m is odd.

Lastly, suppose on the contrary that there is a prime p dividing both m and n. Then $a^{n/p}$ and $b^{m/p}$ both have order p. Now note that $\langle b^m/p\rangle$ is a normal subgroup of G, so $L = \langle a^{n/p}\rangle\langle b^{m/p}\rangle$ is a subgroup of G with order p^2. Being a p-group, L is contained in some Sylow p-subgroup of G, which is cyclic by assumption. This cyclic group has a unique subgroup of size p, but L has two subgroups of size p, a contradiction. Hence there is no such prime dividing both m and n, and $\gcd(m, n)$=1. Combining this with the previous result, we get $\gcd(m, n(r-1)) = 1$, as desired. □

Remark 3.1.6. The proof of this classification here shows that one can decompose any C-group G into $U \ltimes D$, where $U \cong G/G'$ and $D \cong G'$.

Lemma 3.1.7. *Two C-groups $G_{m,n,r}$ and $G_{m',n',r'}$ are isomorphic if and only if $m = n'$, $n = n'$, and r and r' have the same order modulo d.*

Proof. Because m is the size of the derived subgroup $G'_{m,n,r}$ and n is its index, they are uniquely determined by the isomorphism type of the group. The last claim follows from [**11**, Lemma 3.6] and [**4**, Lemma 4.14b]. □

3.2. Enumeration of C-groups

Although impressive, at present, this classification result does not lead to an apparent way of counting the groups, as noted by Murty & Murty in [**11**, p. 4]. They present a variant of the decomposition that is more conducive to enumeration and show in [**11**, Theorem 1.1] that up to isomorphism, the number of C-groups of order n is

$$C(n) = \sum_{\substack{n=de \\ \gcd(d,e)=1}} \prod_{\substack{p^\alpha || d \\ p \text{ prime}}} \left(\sum_{j=1}^{\alpha} \frac{(p^{\nu(p^j,e)} - p^{\nu(p^{j-1},e)})}{p^{j-1}(p-1)} \right). \tag{3.2.1}$$

Recall that ν is defined by

$$p^{\nu(p^j,e)} = \prod_{\substack{q|e \\ q \text{ prime}}} \gcd(p^j, q-1)$$

and $p^\alpha \,||\, d$ denotes the largest p-power dividing d. To build up to this, first we need the following definition, which generalises [**14**, Definition 4].

Definition 3.2.1. Let G be a C-group and let $p < q$ be two prime divisors of $|G|$. We say p *acts on* q *(with exponent* e*, in* G*)* if a Sylow p-subgroup $P = \langle x \rangle \leq G$ acts via conjugation on a Sylow q-subgroup $Q \leq G$, and the action is described by $\sigma : P \to \mathrm{Aut}(Q)$ which maps x to an automorphism of order p^e, where $e > 0$.

The following decomposition inspired by [**11**, Lemma 3.4] is the one we will more frequently make use of.

Lemma 3.2.2. *Every C-group* G *decomposes as* $G = (A \ltimes D) \times C$ *where* $A \times C \cong G/G'$ *and* $D \cong G'$*; the groups* A, C, D *are cyclic of coprime orders, and* p *divides* $|A|$ *if and only if* p *acts on some* q *in* G *with exponent* e*; in this case,* p^e *divides* $q-1$*, and* q *divides* $|D|$*.*

Proof. By Remark 3.1.6 we know that $G = U \ltimes D$ where $U \cong G/G'$ and $D \cong G'$ are cyclic of coprime orders. Let P be a Sylow p-subgroup acting on a Sylow q-subgroup Q of G. If Q has order q^m, then $\mathrm{Aut}(Q)$ is cyclic of order $q^{m-1}(q-1)$; since P acts on Q as an automorphism of order p^e, we have $p^e \mid q-1$. If p divides $|D|$, then $P \leq D$, because

$D \trianglelefteq G$ is a normal subgroup and the orders of U and D are coprime. In particular, P is the unique Sylow p-subgroup of $D \trianglelefteq G$, and hence P and Q normalise each other. This implies that $x^{-1}y^{-1}xy \in P \cap Q = \{1\}$ for all $x \in P$ and $y \in Q$, so P centralises Q, a contradiction. Hence p must divide $|U|$ instead. Now let $x \in P$ and $y \in Q$ be two non-identity elements. Observe that $[x, y^{-1}] = x^{-1}yxy^{-1} = y^x y^{-1} \in Q \cap D$. Since P acts on Q non-trivially, we have $y^x \neq y$, so $Q \cap D$ is a non-trivial Sylow p-subgroup of D, and thus q divides $|D|$.

We can write $U = A \times C$ where A is the direct product of those Sylow p-subgroups of U that have p acting on some q in G, and C is the direct product of the remaining Sylow subgroups of U. By construction, $C \leq Z(G)$ and $A \ltimes D$ is a complement to C in G. □

Definition 3.2.3. Let $G = (A \ltimes D) \times C$ be a C-group as in Lemma 3.2.2. The *acting divisor* of G is $|A|$.

3.2.1. Murty & Murty's enumeration formula

From the preceding definition, we see that an acting divisor d for a C-group of order n must satisfy $\gcd(d, n/d) = 1$. Let $\mathcal{D}(n)$ be the set of divisors of n satisfying this condition; more specifically, $\mathcal{D}(n)$ consists of the 2^k numbers $p_{i_1}^{a_{i_1}} \dots p_{i_m}^{a_{i_m}}$ where $\{i_1, \dots, i_m\}$ runs over all subsets of $\{1, \dots, k\}$. We sort them as $d_1 < \dots < d_{2^k}$. For $d \in \mathcal{D}(n)$ denote by $C_d(n)$ the number of isomorphism types of C-groups of order n with acting divisor d; by [**11**, pp. 303–304], we have

$$C_d(n) = \prod_{\substack{p^\alpha || d \\ p \text{ prime}}} \left(\sum_{j=1}^{\alpha} \frac{(p^{\nu(p^j, n/d)} - p^{\nu(p^{j-1}, n/d)})}{p^{j-1}(p-1)} \right).$$

Summing over all such d gives the total number of isomorphism classes of C-groups of order n, which proves the equation stated at the start of this section:

$$C(n) = \sum_{\substack{n=de \\ \gcd(d,e)=1}} \prod_{p^\alpha || d} \left(\sum_{j=1}^{\alpha} \frac{(p^{\nu(p^j, e)} - p^{\nu(p^{j-1}, e)})}{p^{j-1}(p-1)} \right).$$

Remark 3.2.4. An acting divisor d not only satisfies $\gcd(n, n/d) = 1$, but also $p_k \nmid d$, and that there exists some $q \mid n/d$ with $\gcd(p, q-1) \neq 1$, and. To aid efficiency in our implementation of the formula, we narrow down the possible values of d using these extra criteria.

CHAPTER 4

Generation of C-groups

Our focus is this chapter is describing the methods used to extend Slattery's [**14**] algorithms for squarefree groups to C-groups. His organisation of squarefree groups relies on the notion of *clusters*, which, roughly speaking describe how the Sylow subgroups of a squarefree group interact with each other. A key part of our work is generalising this definition to cover C-groups. While in theory, changing that and a few other minor things would suffice, we found the performance of our implementation in GAP unsatisfactory; computation of clusters was time and memory inefficient for certain large group orders. Thus we sought out the work of Murty & Murty [**11**] to minimise these computations. The complexity of other operations is not within the scope of this project, and we assume, as Slattery does, that the tools for performing basic computations with groups are readily available. This includes computing orders, generators of groups, Sylow subgroups, quotient groups, etc. Much of this background theory is explored in [**8**].

4.1. Construction of C-groups by ID

Given an ID (n, i), we wish to be able to build the i-th group in a canonically ordered list of C-groups of order n. As we are only interested in groups up to isomorphism, we need to be able to determine when two C-groups are isomorphic. Recall from Remark 3.1.4 that every C-group of order $n = p_1^{a_1} \dots p_k^{a_k}$ can be constructed by iteratively making split extensions by a cyclic group of size $p_u^{a_u}$, where u runs over integers from 1 to k in increasing order. Two C-groups are isomorphic if and only if at each stage of this process, the extensions are isomorphic, so we need to know when two such extensions give rise to isomorphic groups.

Let H be a C-group, and let Q be a cyclic group of prime power order q^m, where q is strictly greater than every prime divisor of $|H|$. Denote by $V = \mathrm{Hom}(H, \mathrm{Aut}(Q))$ the set

of all group actions $\sigma : H \to \mathrm{Aut}(Q)$. We can define an action of $\mathrm{Aut}(H)$ on V by

$$\sigma^{\alpha}(h) = \sigma(h^{\alpha^{-1}}),$$

where $\sigma \in V$, and $\alpha \in \mathrm{Aut}(H)$. This indeed defines a group action because

$$\sigma^{\alpha\beta}(h) = \sigma(h^{\beta^{-1}\alpha^{-1}}) = \sigma^{\alpha}(h^{\beta^{-1}}) = (\sigma^{\alpha})^{\beta}(h)$$

for all $h \in H$ and $\alpha, \beta \in \mathrm{Aut}(H)$.

Theorem 4.1.1. *Two actions $\sigma, \omega \in V$ give rise to isomorphic split extensions if and only if they are in the same* $\mathrm{Aut}(H)$*-orbit.*

Proof. Let $E_1 = H \ltimes_{\sigma} Q$ and $E_2 = H \ltimes_{\omega} Q$ be two split extensions with the same underlying set $H \times Q$, and suppose $\omega = \sigma^{\alpha}$ for some $\alpha \in \mathrm{Aut}(H)$, so that for all $h \in H$ we have $\omega(h) = \sigma(h) = \sigma(h^{\alpha^{-1}})$ and hence $\omega(h^{\alpha}) = \sigma(h)$. Define the map $\alpha_* : E_1 \to E_2$ by $(h, a)^{\alpha_*} = (h^{\alpha}, a)$. Let $(h, a), (g, b) \in E_1$. Firstly,

$$\begin{aligned}((h, a)(g, b))^{\alpha_*} &= (hg, a^{\sigma(g)}b)^{\alpha_*} \\ &= ((hg)^{\alpha}, a^{\sigma(g)}b) \\ &= (h^{\alpha}g^{\alpha}, a^{\omega(g^{\alpha})}b) \\ &= (h^{\alpha}, a)(g^{\alpha}, b) \\ &= (h, a)^{\alpha_*}(g, b)^{\alpha_*},\end{aligned}$$

thus α_* is a homomorphism. That the map is bijective follows from α being an automorphism of H. Therefore α_* is an isomorphism from E_1 to E_2.

Conversely, suppose E_1 and E_2 are isomorphic via $\beta : E_1 \to E_2$. Since Q is a characteristic Sylow q-subgroup of both E_1 and E_2, any isomorphism maps Q in E_1 to Q in E_2, so we can consider the restriction of β to Q as an automorphism of Q, and write $(1, a)^{\beta} = (1, a^{\beta}) \in Q \leq E_2$. For $(h, 1) \in H \leq E_1$, we have $(h, 1)^{\beta} = (h^{\alpha}, h^{\tau}) \in E_2$ for

some maps $\alpha : H \to H$ and $\tau : H \to Q$. Let $(h, 1), (g, 1) \in H \leq E_1$. Then

$$\begin{aligned}((hg)^\alpha, (hg)^\tau) &= (hg, 1)^\beta \\ &= ((h, 1)(g, 1))^\beta \\ &= (h, 1)^\beta (g, 1)^\beta \\ &= (h^\alpha, h^\tau)(g^\alpha, g^\tau) \\ &= (h^\alpha g^\alpha, (h^\tau)^{\omega(g^\alpha)} g^\tau)\end{aligned}$$

and equating the first component shows that $(hg)^\alpha = h^\alpha g^\alpha$, so α is a homomorphism. Moreover it is bijective, with its inverse being the map $H \to H$ induced by β^{-1}. Thus $\alpha \in \mathrm{Aut}(H)$. Now for any $(1, a), (h, 1) \in E_1$, we have

$$\begin{aligned}((1, a)(h, 1))^\beta &= (h, a^{\sigma(h)})^\beta \\ &= (h^\alpha, h^\tau n^{\sigma(h)\beta})\end{aligned}$$

but also

$$\begin{aligned}((1, a)(h, 1))^\beta &= (1, a)^\beta (h, 1)^\beta \\ &= (1, a^\beta)(h^\alpha, h^\tau) \\ &= (h\alpha, n^{\beta\omega(h^\alpha)} h^\tau).\end{aligned}$$

Equating the second components and applying the cancellation laws, we get

$$a^{\sigma(h)\beta} = a^{\beta\omega(h^\alpha)}.$$

As Q is cyclic, $\mathrm{Aut}(Q)$ is abelian [**13**, 1.5.5], so β commutes with $\sigma(h)$ and $\omega(h^\alpha)$, which gives us

$$a^{\sigma(h)} = a^{\omega(h^\alpha)}.$$

This holds for all $h \in H$ and $a \in N$, hence $\omega = \sigma^\alpha$ as desired. □

4.1.1. Further streamlining

With this result, we now need only consider one representative of each orbit to construct the split extensions up to isomorphism. This process can be broken down further. Recall that $V = \mathrm{Hom}(H, \mathrm{Aut}(Q))$, where H is a C-group, and Q is a cyclic group of prime power order q^m, with q strictly greater than every prime divisor of $|H|$. Since $\mathrm{Aut}(Q)$ is abelian, any action $\sigma \in V$ has H' in its kernel, thus inducing an action $\tilde{\sigma} \in W = \mathrm{Hom}(H/H', \mathrm{Aut}(Q))$ defined by

$$\tilde{\sigma}(hH') = \sigma(h).$$

Moreover, any such $\tilde{\omega} \in W$ can be lifted back to some $\omega \in V$ by setting $\omega(h) = \tilde{\omega}(hH')$, because H' has to be in the kernel of ω. As H' is characteristic in H, the action of $\mathrm{Aut}(H)$ on V induces an action of $\mathrm{Aut}(H)$ on W, namely

$$\tilde{\sigma}^{\alpha}(hH') = \tilde{\sigma}((hH')^{\alpha^{-1}}) = \tilde{\sigma}(h^{\alpha^{-1}}H') = \sigma(h^{\alpha^{-1}}) = \sigma^{\alpha}(h).$$

We verify that this is well defined. Suppose $hH' = gH'$. Then $g = hk$ for some $k \in H'$, and for any $\alpha \in \mathrm{Aut}(H)$,

$$\begin{aligned}
\tilde{\sigma}^{\alpha}(gH') = \sigma^{\alpha}(g) = \sigma(g^{\alpha^{-1}}) &= \sigma((hk)^{\alpha^{-1}}) \\
&= \sigma(h^{\alpha^{-1}}k^{\alpha^{-1}}) \\
&= \sigma(h^{\alpha^{-1}})\sigma(k^{\alpha^{-1}}) \\
&= \sigma(h^{\alpha^{-1}}) \\
&= \tilde{\sigma}^{\alpha}(hH').
\end{aligned}$$

From this definition, two actions $\tilde{\sigma}, \tilde{\omega} \in W$ are in the same $\mathrm{Aut}(H)$-orbit if and only if their lifts $\sigma, \omega \in V$ are in the same orbit. To further simplify this, since H/H' is abelian and factors into the direct product of its cyclic Sylow subgroups $S_1, \ldots, S_\ell$, we have that

$$\mathrm{Hom}(H/H', \mathrm{Aut}(Q)) \cong \bigoplus_{j=1}^{\ell} \mathrm{Hom}(S_j, \mathrm{Aut}(Q)).$$

That is, if $\sigma \in W$, then we can consider σ as the following product

$$\sigma = (\sigma_1 \times \ldots \times \sigma_l) \colon S_1 \times \ldots \times S_l \to \mathrm{Aut}(Q).$$

As each of these Sylow subgroups is characteristic, the action of $\mathrm{Aut}(H)$ on W can be factored once more into the actions of $\mathrm{Aut}(H)$ on $\mathrm{Hom}(S_i, \mathrm{Aut}(Q))$ by setting $\sigma^\alpha = \sigma_1^{\alpha_1} \times \ldots \times \sigma_k^{\alpha_k}$ where $\alpha_i = \alpha|_{S_i}$ for each i. Then if two actions $\sigma, \omega \in \mathrm{Hom}(H, \mathrm{Aut}(Q))$ are in the same $\mathrm{Aut}(H)$-orbit, the induced maps $\sigma_j, \omega_j \in \mathrm{Hom}(S_j, \mathrm{Aut}(Q))$ are also in the same $\mathrm{Aut}(H)$-orbit for each j. Thus we would like to examine how $\mathrm{Aut}(H)$ acts on each of the summands. Note that each of the S_j is cyclic because C-groups are closed under taking quotients, so we look at the actions of cyclic p-groups on Q.

Remark 4.1.2. Let $P = \langle x \rangle$ be a cyclic p-group of order p^m and $Q = \langle y \rangle$ be a cyclic q-group of order q^m, where p and q are primes and $q > p$. Note that $\mathrm{Aut}(Q)$ is a cyclic group of order $\varphi(q^m) = q^{n-1}(q-1)$. For every divisor a of $|\mathrm{Aut}(Q)|$, the automorphisms of order a are described by $y \mapsto y^r$, where r is an a-th root of unity mod q^n. For each $k \in \{1, \ldots, a-1\}$ coprime to a, we can define an a-th root of unity by $r_k = s^{kq^{n-1}(q-1)/a} \bmod q^n$, where s is a primitive root modulo q^n. Then the automorphisms of Q of order a are $\alpha_k \colon Q \to Q$, $y \mapsto y^{r_k}$, where $t_k = r^{kq^{m-1}(q-1)/a} \bmod q^m$.

Next, we require a canonical ordering on C-groups. To describe this, we expand on a few earlier definitions.

Definition 4.1.3. Let $G = (A \ltimes D) \times C$ be a C-group as in Lemma 3.2.2. Its acting group is the cyclic subgroup of $\mathrm{Aut}(D)$ that is the image of the action of A on D.

Remark 4.1.4. If a C-group has acting divisor d and acting group of size m, then $m \mid d$, and for every prime divisor $p \mid d$, we also have $p \mid m$. We denote by $\mathcal{M}(d)$ the set of all possible acting group sizes for a C-group with acting divisor d, and these are precisely the numbers satisfying the aforementioned conditions.

Lemma 4.1.5. [**11**, p. 303] *Let $C_{d,m}(n)$ be the number of isomorphism types of C-groups of order n with acting divisor d and acting group order m. Then*

$$C_{d,m}(n) = \prod_{\substack{p^j || m \\ p \text{ prime}}} \left(\frac{(p^{\nu(p^j, n/d)} - p^{\nu(p^{j-1}, n/d)})}{p^{j-1}(p-1)} \right).$$

Next we present a modification of [**14**, Definition 7].

Definition 4.1.6. The *cluster* of a C-group G is the set $\mathcal{C}(G)$ of all triples (p, q, e) such that p acts on q in G with exponent e.

Definition 4.1.7. A *permissible set* for a group order $n > 1$ is a set $\mathcal{P}$ of triples (p, q, e) such that $q > p$ are primes dividing n, $p^e \neq 1$ divides $q - 1$, and if $(p, q, e) \in \mathcal{P}$, then $(q, *, *), (*, p, *), (p, q, c) \notin \mathcal{P}$ for all $c \neq e$.

Remark 4.1.8. If G is a C-group, then $\mathcal{C}(G)$ is a permissible set for $|G|$ by Lemma 3.2.2. The acting divisor of G is the product of all $p^\alpha \,||\, |G|$ where p runs over $\{p : (p, *, *) \in \mathcal{C}(G)\}$; every such p divides the size of the acting group of G. Conversely, if $\mathcal{P}$ is a permissible set for a group order $n > 1$, then there exists a C-group G with $\mathcal{C}(G) = \mathcal{P}$: let $n = p_1^{a_1} \dots p_k^{a_k} q_1^{b_1} \dots q_\ell^{b_\ell} r_1^{c_1} \dots r_m^{c_m}$ be the prime power factorisation of n and assume, without loss of generality, that $(p, *, *), (*, q, *) \in \mathcal{P}$ if and only if $p \in \{p_1, \dots, p_k\}$ and $q \in \{q_1, \dots, q_\ell\}$. We do this because a prime that acts cannot be acted on by Lemma 3.2.2. A group of order n with cluster $\mathcal{P}$ is

$$G = (C_{{p_1}^{a_1}} \times \dots \times C_{{p_k}^{a_k}}) \ltimes (C_{{q_1}^{b_1}} \times \dots \times C_{{q_\ell}^{b_\ell}}) \times C_{{r_1}^{c_1} \dots {r_m}^{c_m}}$$

where $C_{{p_i}^{a_i}}$ acts on $C_{{q_j}^{b_j}}$ via an automorphism of order $p_i^{e_{i,j}}$ if and only if $(p_i, q_j, e_{i,j}) \in \mathcal{P}$. With this correspondence, we may now speak of clusters and permissible sets interchangeably.

4.1.2. Ordering of C-groups

We sort the C-groups of order $n > 1$ first by their acting divisors (in increasing order), then by the size of their acting groups (in increasing order). For each $d \in \mathcal{D}(n)$ and

$m \in \mathcal{M}(d)$, we may construct all permissible sets that can be a cluster for a C-group of order n with acting divisor d and acting group order m. These are precisely the permissible sets $\mathcal{P}$ where there is at least one triplet of the form $(p, *, j)$ in $\mathcal{P}$ for every $p^j \mid\mid m$, but $(p, *, l) \notin \mathcal{P}$ when $l > j$. We then sort these permissible sets lexicographically, with four tiers of ordering:

(1) compare the acting primes;
(2) for a fixed acting prime p, compare the first prime $q_{\max}$ it acts on with maximal exponent;
(3) for a fixed acting prime p and $q_{\max}$, compare the other primes p acts on;
(4) for a fixed acting prime p acting on $q \neq q_{\max}$, compare the exponents of that action.

Each of these are in increasing order. In practice, this process is done by looking at each distinct prime factor of m. For each such prime p, we consider the permissible sets containing only triplets with p as their first entry. These subsets can be sorted according to $(2) - (4)$, (which we will elaborate on with an example), so that there is an ordered collection of sets for each p. Each permissible set can then be constructed by choosing exactly one set from each such collection and concatenating them together. We arrange these collections by the prime they correspond to, in increasing order, and run over all combinations lexicographically to obtain the ordering on all permissible sets.

Within each permissible set itself, the triplets are sorted first by their first entry (acting prime) then their second entry (prime being acted on), both in increasing order. Now fixing a permissible set, for each triplet (p, q, e) in the set, a C-group that has this set as its cluster will have a Sylow p-subgroup $P = \langle x \rangle$ acting on a Sylow q-subgroup Q, where the action is defined by x being mapped to an automorphism of Q of order p^e. An ordered list of all such automorphisms is defined in Remark 4.1.2, and we make explicit in the next subsection how to refine this list so that there is a canonical choice for construction of each isomorphism type. With this, the groups may be sorted lexicographically with respect to the choice of automorphism corresponding to each triplet.

Example 4.1.9. We sort the permissible sets for $n = 2040 = 2^3 \cdot 3 \cdot 5 \cdot 17$ with $d = 8$ and $m = 4$. The only prime that acts is 2, and because $m = 4$, it has to act with exponent 2 at least once. By (2) we mean that clusters containing $(2, 5, 2)$ (i.e. "$q_{\max} = 5$") come before those containing $(2, 17, 2)$ but not $(2, 5, 2)$ ("$q_{\max} = 17$"). We obtain the following sorted list: $\{(2, 5, 2)\}$, $\{(2, 5, 2), (2, 17, 1)\}$, $\{(2, 5, 2), (2, 17, 2)\}$, $\{(2, 3, 1), (2, 5, 2)\}$, $\{(2, 3, 1), (2, 5, 2), (2, 17, 1)\}$, $\{(2, 3, 1), (2, 5, 2), (2, 17, 2)\}$, $\{(2, 17, 2)\}$, $\{(2, 3, 1), (2, 17, 2)\}$, $\{(2, 5, 1), (2, 17, 2)\}$, $\{(2, 3, 1), (2, 5, 1), (2, 17, 2)\}$.

4.1.3. Construction of clusters

Given a permissible set $\mathcal{P}$ for a group order $n > 1$, we detail how to construct the j-th group that has $\mathcal{P}$ as its cluster. By the extension procedure described in Remark 3.1.4, if a triplet (p_u, p_v, e) is in $\mathcal{C}(G)$, then at some stage in the process of constructing G, we extend a C-group H, of size $|H| = p_1^{a_1} \dots p_{v-1}^{a_{v-1}}$, by Q, a cyclic group of size $p_v^{a_v}$, where the cluster of H is $\mathcal{C}(H) = \{(p, q, c) \in \mathcal{C}(G) \mid q < p_v\}$. As discussed in Section 4.1.1, if $P = \langle x \rangle$ is the Sylow p_u-subgroup of H/H', it suffices to consider the actions of P on Q, and how $\mathrm{Aut}(H)$ acts on that set of actions. Since $H \cong H/H' \ltimes H'$, we may also consider P as a Sylow p_u-subgroup of H. Because $(p_u, p_v, e) \in \mathcal{C}(G)$, the action $\sigma : H \to \mathrm{Aut}(Q)$ that defines this extension maps x to an automorphism of Q of order p_u^e, as detailed in Remark 4.1.2.

If p_v is the smallest prime that p_u acts on in G, then P is central in H. Then $\mathrm{Aut}(H) \cong \mathrm{Aut}(H/P) \times \mathrm{Aut}(P)$ because $|P|$ and $|H : P|$ are coprime, and the action of $\mathrm{Aut}(H)$ on P is determined by the action of $\mathrm{Aut}(P)$ on P. Since $\mathrm{Aut}(P)$ acts transitively on the generators of P, the actions of P on Q with exponent e all lie in the same $\mathrm{Aut}(H)$-orbit. Thus, we simply choose the action that maps x to the first automorphism in the list defined in Remark 4.1.2.

Otherwise, P is not central, and p_u acts on some other primes in H. Let p_w be such a prime, and let $S = \langle y \rangle$ be the Sylow p_w-subgroup of H. Suppose p_u acts on p_w with exponent c_w, that is, the conjugation action of P on S is described by $\kappa : P \to \mathrm{Aut}(S)$, where $\kappa(x)$ has order $p_u^{c_w}$. For any $\beta \in \mathrm{Aut}(H)$, we have $x^\beta = x^t$ for some t coprime to

p_u. Furthermore, as S is a characteristic subgroup, β restricts to an automorphism of S, which commutes with $\kappa(x)$ because $\mathrm{Aut}(S)$ is abelian, so

$$(y^\beta)^{\kappa(x)} = (y^{\kappa(x)})^\beta = (y^x)^\beta = (y^\beta)^{x^\beta} = (y^\beta)^{x^t} = (y^\beta)^{\kappa(x^t)} = (y^\beta)^{\kappa(x)^t},$$

which implies $t \equiv 1 \mod p_u^{c_w}$. This holds for any prime p_w that p_u acts on in H, if and only if $t \equiv 1 \mod p_u^c$, where $c = \max\{c_w \mid p_u \text{ acts on } p_w \text{ with exponent } c_w\}$. Hence if $e \leq c$, then

$$\sigma^{\beta^{-1}}(x) = \sigma(x^\beta) = \sigma(x^t) = \sigma(x)^t = \sigma(x),$$

and the action of $\mathrm{Aut}(H)$ on $\mathrm{Hom}(P, \mathrm{Aut}(Q))$ is trivial, meaning there are $\varphi(p_u^e) = p_u^{e-1}(p_u - 1)$ distinct orbits of actions with exponent e.

On the other hand, suppose $e > c$. Since

$$\sigma^{\beta^{-1}}(x) = \sigma(x^\beta) = \sigma(x^t) = \sigma(x)^t = \sigma(x)^{t \bmod p^e},$$

the actions in the same $\mathrm{Aut}(H)$-orbit as $\sigma(x)$ must be of the form $\sigma(x)^s$ where $s \equiv 1 \mod p^c$, and $1 \leq s < p_u^e$. Conversely, for each such s, we claim that there is an automorphism of H that takes x to x^s.

For each prime divisor $p_w \neq p_u$ of $|H|$, choose a Sylow p_w-subgroup of H. Suppose $P_1, \ldots, P_r$ are the subgroups we have chosen. Then H can be generated by $P, P_1, \ldots, P_r$, so to define an automorphism of H, it suffices to describe how it acts on a generator of each of these subgroups, which we denote by $x, z_1, \ldots, z_r$ respectively. Define the map γ by $\gamma(x) = x^s$, and $\gamma(z_f) = z_f$ for every other generator. We use von Dyck's Theorem (Theorem 2.2.6) to check that this extends to a well-defined automorphism of H. To do this, we check that the conjugation relations in H are preserved by γ. This is true for any $z_f, z_g \neq x$ because γ is the identity on them. Likewise, if z_f commutes with x then no action occurs and

$$\gamma(z_f)\gamma(x) = z_f x^s = x^s z_f = \gamma(x)\gamma(z_f).$$

It remains to check that $\gamma(z_f)\gamma(x) = \gamma(x)\gamma(z_f)$ where x acts non-trivially on z_f. Because p_u acts with at most exponent c in H, and $s \equiv 1 \mod p^c$, we have $z_f^{x^s} = z_f^x$, so

$$\gamma(z_j)\gamma(x) = z_j x^s = x^s z_j^{x^s} = x^s z_j^x = \gamma(x)\gamma(z_j)^x.$$

Therefore, γ extends to an automorphism of H that maps x to x^s. As there are p_u^{e-c} such numbers s, the size of the $\mathrm{Aut}(H)$-orbit of $\sigma(x)$ is p_u^{e-c}. This holds for any generator x of P, thus the number of distinct $\mathrm{Aut}(H)$-orbits of actions of P on Q is

$$\varphi(p_u^e)/p_u^{e-c} = p_u^{e-1}(p_u - 1)/p^{e-c} = p_u^{c-1}(p_u - 1) = \varphi(p_u^c).$$

Thereupon, if the number of orbits of actions corresponding to a triplet is o, because P is cyclic, mapping x to each of the first o automorphisms in the list defined in Remark 4.1.2 gives rise to actions in different orbits, hence we let these be the canonical choices. Thus we have established the lexicographical ordering of groups with cluster $\mathcal{P}$, and are able to construct the j-th group canonically.

Remark 4.1.10. Note that this method of looking at each individual acting prime describes a partial converse to the discussion at the end of Section 4.1.1. We may extend this to a full converse: let $S_1, \ldots, S_\ell$ be the Sylow subgroups of H/H', and suppose for each i we have actions $\sigma_i, \omega_i : S_i \to Q$ such that $\sigma_i = \omega_i^{\alpha_i}$ for some $\alpha_i \in \mathrm{Aut}(H)$. Let z_i be a generator of S_i. Then α_i maps z_i to some power $z_i^{s_i}$. Then as in Section 4.1.3, by considering the S_i as subgroups of $H = H/H' \ltimes H'$, we can define the map γ to be $\gamma(z_i) = z_i^{s_i}$ for each i, and for γ to be the identity on H'. Applying von Dyck's Theorem yields that γ extends to an automorphism $\alpha \in \mathrm{Aut}(H)$, and by construction, it satisfies $(\sigma_1 \times \ldots \times \sigma_\ell) = (\omega_1 \times \ldots \times \omega_\ell)^\alpha$.

As a corollary of the procedure described in the previous section, we have also proved the following algorithm which counts how many non-isomorphic groups of order n have a given cluster.

Algorithm 1: `ClusterCount`

Input: A sorted cluster $\mathcal{P}$ of a group of order n

Output: Number of non-isomorphic groups of order n with $\mathcal{P}$ as their cluster

```
begin
    current := 0
    total := 1
    for (p, q, e) in P do
        if p ≠ current then
            current := p
            max := e
        else if e > max then
            total := total * φ(p^max)
            max := e
        else
            total := total * φ(p^e)
        end
    end
    return total
end
```

4.1.4. C-groups by ID

To construct the C-group G with ID (n, i), we proceed as follows. First, recall from Section 3.2.1 that we have the function $C_d(n)$ that counts the number of C-groups (up to isomorphism of) order n and with acting divisor d. We determine $j \geq 0$ such that

$$C_{d_1}(n) + \ldots + C_{d_{j-1}}(n) < i \leq C_{d_1}(n) + \ldots + C_{d_j}(n),$$

which tells us G must have acting divisor $d = d_j$. Letting $t = i - C_{d_1}(n) - \ldots - C_{d_{j-1}}(n)$, it now remains to construct the t-th group with acting divisor d. Similarly, we have from Lemma 4.1.5 the formula $C_{d,m}(n)$ counting the number of non-isomorphic C-groups of order n, with acting divisor d, and with acting group order m, and determine $j \geq 1$ such that

$$C_{d,m_1}(n) + \ldots + C_{d,m_{j-1}}(n) < t \leq C_{d,m_1}(n) + \ldots + C_{d,m_j}(n),$$

so that G must have an acting group of order $m = m_j$. Again, letting $\ell = t - C_{d,m_1}(n) - \ldots - C_{d,m_{j-1}}(n)$, it remains to construct the ℓ-th group with acting divisor d and acting group of order m. Let $\mathcal{P}_1, \ldots, \mathcal{P}_w$ be all the possible clusters for a C-group of size n, with acting divisor d and acting group of order m, sorted as described in Section 4.1.2, and let $C_{\mathcal{P}_c}(n)$ denote the number of C-groups of order n with cluster $\mathcal{P}_c$, which can be calculated using Algorithm 1. We determine $j \geq 1$ such that

$$C_{\mathcal{P}_1}(n) + \ldots + C_{\mathcal{P}_{j-1}}(n) < \ell \leq C_{\mathcal{P}_1}(n) + \ldots + C_{\mathcal{P}_j}(n),$$

so G must have cluster $\mathcal{P} = \mathcal{P}_j$. Now it remains to construct the s-th group of order n with this cluster, where $s = \ell - C_{\mathcal{P}_1}(n) - \ldots - C_{\mathcal{P}_{j-1}}(n-1)$. For each triple in $\mathcal{P}$, the description in Section 4.1.3 tells us how many non-isomorphic choices of actions there are for p acting on q with exponent e. With $\mathcal{P}$ sorted first by the acting primes then by the primes which are acted on, by running over the triplets lexicographically, we can determine the corresponding canonical action for each triple, as described in Remark 4.1.2. Hence, the group with ID (n, i) is obtained.

Example 4.1.11. To demonstrate, we will construct the canonical polycyclic presentation for the group with ID $(10200, 12)$. It is straightforward to compute that the acting divisor is 8 and the acting group is of size 4. The clusters corresponding to this data are $\{(2,5,2)\}$, $\{(2,5,2),(2,17,1)\}$, $\{(2,5,2),(2,17,2)\}$, $\{(2,3,1),(2,5,2)\}$, $\{(2,3,1),(2,5,2),(2,17,1)\}$, $\{(2,3,1),(2,5,2),(2,17,2)\}$, $\{(2,17,2)\}$, $\{(2,3,1),(2,17,2)\}$, $\{(2,5,1),(2,17,2)\}$, and $\{(2,3,1),(2,5,1),(2,17,2)\}$, sorted as described in Example 4.1.9. Applying the `ClusterCount` algorithm tells us that the group's cluster is $\{(2,5,2),(2,17,2)\}$. We then compute that the ID corresponds to the second group with

this cluster, and that means taking the first action for the triplet $(2, 5, 2)$, and the second action for $(2, 17, 2)$, with respect to the ordering in Remark 4.1.2.

The presentation will be on 7 generators $g_1, \ldots, g_7$, one for each prime divisor of $10200 = 2^3 \cdot 3 \cdot 5^2 \cdot 17$, and they are arranged first by the decomposition in Lemma 3.2.2, then in increasing order. This gives the power relations $g_1^2 = g_2$, $g_2^2 = g_3$, $g_3^2 = 1$, $g_4^5 = g_5$, $g_5^5 = 1$, $g_6^{17} = 1$, $g_7^3 = 1$. We see that 2 first acts on 5 with exponent 2. The smallest primitive root modulo 25 is 2, and so by Lemma 4.1.2 we have g_1 raising g_4 to the power $(2^{5(5-1)/4} \bmod 25) = 7$, and we can simplify $g_4^7 = g_4^2 g_5$, so we add $g_4^{g_1} = g_4^2 g_5$ to the set of relations. This induces more conjugate relations, in particular those which relate generators that are powers of g_1 or g_4, and we have to update them to maintain consistency. This is done easily by computing the powers. In this case, we have to add $g_4^{g_2} = g_4^4 g_5^4$, $g_5^{g_1} = g_5^2$, and $g_5^{g_2} = g_5^4$ to the set of relations.

Finally, we consider 2 acting on 17 with exponent 2. Since 2 has already acted on 5, there are multiple actions of g_1 on g_6 to consider. We have determined that this group will contain the second such action. The smallest primitive root modulo 17 is 3, and so we have g_1 raising g_6 to the power $(3^{(3(17-1)/4)} \bmod 17) = 4$. Recall that the coefficient of 3 in the numerator arises because 3 is the second smallest positive integer coprime to 2, the acting prime, and this is how the second action is determined. Thus we add $g_6^{g_1} = g_6^4$ to the relations. The only other induced relation is $g_6^{g_2} = g_6^{16}$. Therefore, the complete presentation is:

$$\begin{aligned}\mathrm{Pc}\langle\, g_1,\ g_2,\ g_3,\ g_4,\ g_5,\ g_6,\ g_7 \ \mid\ & g_1^2 = g_2,\ g_2^2 = g_3,\ g_3^2 = 1,\ g_4^5 = g_5,\ g_5^5 = 1,\ g_6^{17} = 1,\ g_6^3 = 1,\\ & g_4^{g_1} = g_4^2 g_5,\ g_4^{g_2} = g_4^4 g_5^4,\ g_5^{g_1} = g_5^2,\ g_5^{g_2} = g_5^4\\ & g_6^{g_1} = g_6^4,\ g_6^{g_2} = g_6^{16}\,\rangle.\end{aligned}$$

4.2. Identification of C-groups with ID

Given a C-group G of order $n = p_1^{a_1} \ldots p_k^{a_k}$, we first compute a generator for each of its Sylow subgroups. The cluster of G is determined by examining the conjugation actions of these generators. If x is a generator of a Sylow p_u-subgroup of G, and y a

generator of a Sylow p_v-subgroup of G, then p_u acts on p_v in G if and only if $v > u$ and $y^x \neq y$. Furthermore, the exponent of the action is the smallest integer $e \geq 1$ such that $y^{\left(x^{(p^e)}\right)} = y$. Checking all possible pairs of generators, we are able to construct $\mathcal{C}(G)$. From the cluster, the acting divisor is computed as the product of all $p_u^{a_u} || n$ where there is at least one triplet of the form $(p_u, *, *)$ in $\mathcal{C}(G)$. Similarly, the order of the acting group is the product of the prime powers $p_u^{e_u}$, where again there is at least one triplet $(p_u, *, *) \in \mathcal{C}(G)$, and $e_u = \max\{c \mid (p_u, *, c) \in \mathcal{C}(G)\}$.

Now to determine the position of G within the cluster, recall that for each triplet $(p_u, p_v, e) \in \mathcal{C}(G)$, there is a canonically ordered set of exponents for which a generator of a Sylow p_u-subgroup can raise a generator of a Sylow p_v-subgroup to in the power-conjugate presentation. Moreover, the positions of groups within the cluster are determined lexicographically with respect to these sets, running over all triplets in the sorted cluster. However, the exponent depends on the choice of generator corresponding to the acting prime. Hence this necessitates a normalisation process on the generators.

The first time a prime p_u acts, there is only one choice for the canonical exponent: the one corresponding to the first action in the ordered list described in Remark 4.1.2. Thus we cycle through generators of a Sylow p_u-subgroup of G until one is found which acts accordingly, that raises a generator of the Sylow subgroup it is acting on to the correct power. Note that there may be more than one such generator, which happens in the case if the triplet (p_u, p_v, e) corresponding to this action has $e < a_u$. If x is the chosen generator, then the other such generators are precisely those of the form x^{bp^e+1}, where $1 \leq b < p_u^{a_u - e}$. On subsequent occasions that p_u acts, we first cycle through the set of possible exponents, and if the chosen generator does not give rise to an exponent in the list, we cycle through to the next candidate generator, repeating this process until a valid exponent is obtained. Doing this for all triplets, we thereby deduce the group's position in the cluster.

Having the acting divisor d, the size of the acting group m, cluster $\mathcal{C}(G)$, and group position within the cluster ℓ, if $d_1 < \ldots < d_j = d$ are the possible acting divisors less-equal d, with $m_1 < \ldots < m_r = m$ the possible acting group orders (of a C-group of order n

with acting divisor d) less-equal m, and $\mathcal{P}_1, \ldots, \mathcal{P}_t$ the clusters corresponding to n and m that come before $\mathcal{C}(G)$, then the position of the isomorphism type of G in our canonically ordered list is

$$i = C_{d_1}(n) + \ldots + C_{d_j-1}(n) + C_{d,m_1}(n) + \ldots + C_{d,m_{r-1}}(n) + C_{\mathcal{P}_1}(n) + \ldots + C_{\mathcal{P}_t}(n) + \ell.$$

Example 4.2.1. We will identify the C-group given by the metacyclic presentation

$$G = \langle\, a, b \;\mid\; a^9 = b^{133} = 1,\; b^a = b^{25} \,\rangle.$$

This group has order $n = 1197 = 3^2 \cdot 7 \cdot 19$. GAP computes the generators of the Sylow subgroups of G to be $g_1 = a, g_2 = b^{19}$, and $g_3 = b^7$, corresponding to primes $\{3, 7, 19\}$ respectively. By checking the conjugation action of different pairs of generators, we find the cluster of G to be $\{(3, 7, 1), (3, 19, 2)\}$, from which we can compute the acting divisor to be 9, and acting group to have size 9. The first occasion 3 acts in G is on 7 with exponent 1. We cycle through powers of g_1, until we find j such that $g_2^{(g_1^j)} = g_2^2$, which is the only choice of exponent according to our canonical description. Here we find that $j = 2$ satisfies the condition, so we proceed with calculations from here replacing g_1 with g_1^2 as the fixed generator of order 8. Since 1 is not the maximal exponent that 3 acts with in G, we note that $j = 5$ and $j = 8$ are also valid candidates. Next we consider 3 acting on 19 with exponent 2. We find that there should be 2 choices of possible canonical actions, and that $g_3^{g_1^2} = g_3^{17}$ is not either of those, hence we have to check through the other candidates as previously noted, of which only g_1^8 fits the criteria, giving $g_3^{(g_1^8)} = g_3^{16}$, which is the second choice action in our list. Having gone over all triplets, we can calculate that G is the second group within the cluster $\mathcal{C}(G)$. Overall, we sum the number of groups that having acting divisor and acting group order smaller than G, then those with the same acting divisor and acting group order but cluster which comes before $\mathcal{C}(G)$, and add 2 to get that G is the 8-th group of size 1197 in our list, and its ID is $(1197, 8)$.

CHAPTER 5

Tests and Performance

An implementation of our algorithms for GAP can be found at `https://github.com/heikodietrich/cgroups`. The main functions are:

(1) `NumberOfCGroups`: takes in a positive integer n and outputs the number of C-groups of order n, up to isomorphism.

(2) `AllCGroups`: takes in a positive integer n and outputs a list of all C-groups of order n up to isomorphism, ordered as described in Section 4.2.

(3) `CGroupById`: takes in two positive integers (n, i), with $i \leq$ `NumberOfCGroups`(n), and constructs the i-th C-group of order n in our list.

(4) `IdCGroup`: takes in a C-group G and returns the pair (n, i) where n is the order of G, and i is the position of the C-group in our list that is isomorphic to G.

To verify the correctness of our algorithms, we performed various tests.

5.1. Tests

5.1.1. Testing against the SmallGroups library

The SmallGroups library that comes inbuilt with GAP [**9**] contains the functions `AllSmallGroups` and `IdSmallGroup`, which, like the functions we have coded, allow one to list all groups up to isomorphism of a given order, and assign them a unique ID. Note that due to differences in the implementation, the library ID differs from ours. Likewise, it is also independent of Slattery's algorithms for Magma [**2**]. For all orders up to 2,000, cubefree orders up to 50,000, and squarefree orders up to 100,000, we used `AllCGroups` to generate our list of C-groups, and then applied `IdSmallGroup` to verify that each group was non-isomorphic, and had a unique ID between 1 and NumberOfCGroups. For the groups of squarefree orders, as every such group is also a C-group, we were able to test the

reverse: applying our identification function `IdCGroup` to the output of `AllSmallGroups`, we checked that every ID appeared exactly once.

5.1.2. Internal testing

We compared the results of the four aforementioned functions to check consistency with each other. Up to orders of 100,000, we have verified that the output of NumberOfC-Groups agrees with the size of the output of `AllCGroups`. We have also verified that IDCGroup returns the correct ID when given a C-group constructed via `AllCGroups` or CGroupByID.

5.1.3. Comparison with a brute force construction

By Lemma 3.2.2, one can construct all isomorphism types of C-groups (possibly with repetition) by considering all coprime metacyclic decompositions. We checked up to orders of 50,000 that `IdCGroup` correctly identifies C-groups constructed in this fashion.

Remark 5.1.1. Beyond the orders that have been mentioned, we also performed the tests on several random larger orders (containing at least 5 distinct prime factors).

5.2. Performance

It is also of practical interest that our algorithms run efficiently. In addition to verifying correctness against the SmallGroups Library, we conducted runtime tests and found our implementation no worse than the library when restricted to squarefree orders, often running several times faster. All computations here have been carried out with GAP 4.10.0 on an Intel(R) Core(TM) i5-7500 CPU@3.40GHz with 16GB RAM.

For the 566801 squarefree groups of to order 250000, it took `AllCGroups` 201 seconds to construct these. In comparison, `AllSmallGroups` required 2844 seconds. For the 208014 squarefree groups of to order 100000, `IdCGroup` needed 161 seconds to identify the list constructed by `AllSmallGroups`, whereas `IdGroup` took 267 seconds to identify the list constructed by `AllCGroups`.

For more general orders, `AllCGroups` took 247 seconds to construct the 576093 C-groups of orders up to 100000. Identification using `IdCGroup` on (isomorphic copies of) these groups took 846 seconds.

In Table 5.1 we list some squarefree orders and the times `AllCGroups` and `AllSmallGroups` take to construct all the groups of that order. We also have the times that `IdCGroup` and `IdSmallGroup` take to identify all the groups in the list from the opposite implementation. Note that `IdCGroup` relies on being able to compute the Sylow subgroups of a given group efficiently. One major bottleneck we found was the inbuilt capability of GAP to compute Sylow subgroups — in some cases with large orders (such as 24898143467617960290), runtimes blew up while doing so, and we indicate this in the table by 'syl'. The same issue was encountered with `IdSmallGroup`, so the two functions remain comparable. Construction of these groups was still functional. In Table 5.2 we showcase more general orders, particularly those which give rise to many possible pairs of prime actions, as we believe that is a potential computational bottleneck.

Order	#Groups	`AllCGroups`	`AllSmallGroups`	`IdCGroup`	`IdSmallGroup`
414080602190760145047404609 5	126	0.1	1.4	51.8	61.3
1054578325689038795758113	299	0.1	1.6	121	156
18246294181628283634185	1678	0.6	2.7	80.3	95.2
2885806013236681535396389205274 45	110	0.06	6.5	syl	syl
24898143467617960290	384	0.2	175.7	syl	syl
4100698523844820373769891971054	1024	0.55	15.6	syl	syl
2533036924228662499419966	3840	1.9	49.8	syl	syl

Table 5.1. Comparison of times (in seconds) to construct and identify all groups of some squarefree orders.

factorised group order	#Groups	`AllCGroups`	`IdCGroup`
$5^5.7^5.11^5.13^5.197^7.251^4.677^8.727^4$	225	0.9	9.9
$2^2.31^2.113^3.227^4.293^4.373$	276	0.3	1.9
$2^5.3^5.101^3.103.313^2.367^5$	840	1.3	8.5
$2^3.173^2.233^4.241^2.307^2.337^2$	1168	1.1	10.0
$3^3.5^3.7^2.11^3.23^2.43^2.101^2.127^2$	1305	0.9	6.3
$2^4.5^4.73.101^2.113^3.349^3$	2720	2.1	17.5
$2^2.3^5.5.61^2.73^5.349^4$	4128	5.1	38.2
$3^3.5^2.7^3.29^3.59^2.233^3.43^3.173^3.431^2$	6006	4.6	73.9

Table 5.2. Times (in seconds) to construct and identify all C-groups of some non-squarefree orders.

References

[1] Besche, H. U., Eick, B., & O'Brien, E. A. (2002). *A Millennium Project: Constructing Small Groups.* International Journal of Algebra and Computation, 12(05), 623-644.

[2] Bosma, W., Cannon, J., Playoust, C. (1997). The Magma algebra system I: The user language. *Journal of Symbolic Computation 24*, 235–265.

[3] Cayley, A. (1854). *On the theory of Groups as depending on the Symbolical Equation* $\theta^n = 1$. (40–47). Philosophical Magazine, *7*, 40–47.

[4] Dietrich, H. & Wilson, J. B. (2020). Polynomial time isomorphism tests of groups of most orders, *submitted*.

[5] Dietrich, H., & Low, D. (2020). Generation of finite groups with cyclic Sylow subgroups, *submitted*.

[6] Hall, M. (2018). *The Theory of Groups*. Mineola, NY: Dover Publications Inc.

[7] Hölder, O., (1895). Die Gruppen mit quadratfreier Ordnungszahl, *Nachrichten Von Der Gesellschaft Der Wissenschaften Zu Göttingen, Mathematisch-Physikalische Klasse*, 211–229.

[8] Holt, D. F., Eick, B., & O'Brien, E. A. (2005). *Handbook of computational group theory*. Boca Raton, FL Chapman & Hall.

[9] GAP – Groups, Algorithms and Programming. Available at `gap-system.org`.

[10] Khurana, B., & Khurana, A. (2005). A Theorem of Frobenius and Its Applications. *Mathematics Magazine*, 78(3), 220–225.

[11] Murty, M. R., & Murty, V. K. (1984). On groups of squarefree order. *Mathematische Annalen*, 267(3), 299–309.

[12] Netto, E., & Cole, F. N. (1892). The theory of substitutions and its application to algebra (pp. 146-149). Ann Arbor, MI.

[13] Robinson, D. J. S. (1996). *A course in the theory of groups (2nd ed.)*. New York: Springer.

[14] Slattery, M. C. (2007). Generation of groups of square-free order. *Journal of Symbolic Computation*, 42(6), 668–677.