Computing socles of finite permutation groups with degree $n \leq 10^7$

Huon Wilson

Supervisors: Prof. John Cannon, Dr. William Unger

An essay submitted in partial fulfillment of
the requirements for the degree of
B.Sc. (Honours)

Pure Mathematics
University of Sydney

October 2014

CONTENTS

Introduction

The field of computational group theory was created early in the history of computational mathematics. This early maturity was driven by the classification of finite simple groups, where construction of certain sporadic simple groups was only feasible with computational methods. The study of algorithms for permutation groups is one of the pillars of computational group theory, and in fact, is the one that has received the most attention. The focus of this essay, the socle of a permutation group, is a key part of many algorithm handling such objects.

There are many difficult problems in these areas, even an innocuous task like computing the intersection of two arbitrary subgroups does not have a known efficient algorithm. However, there are some questions about such groups that can be answered efficiently, such as,

- What are the orbits?
- What is the order?
- Is it solvable? Nilpotent?
- What is a chief series? A composition series?

The very last two are of particular interest in this essay, as efficient algorithms for the composition series and chief series require knowledge of the socle of the group and its components.

The socle of a group is the subgroup generated by the minimal normal subgroups. The name comes from French where it can mean plinth or foundation, and, indeed, the socle of a group can be regarded as a foundation on which the group is built since it forms a useful computational starting point for answering questions. The anatomy of the socle is well-understood due to results like the O'Nan–Scott theorem for primitive groups.

Algorithms for computing the socle have improved progressively. Initially, the only technique for calculating it was enumerating all minimal normal subgroups and using the definition directly. This is unusable for even a moderately sized group and hence was not a useful tool for other algorithms. With time, the mathematical and the algorithmic structure of the socle was further understood leading to algorithmic improvements, culminating in the efficient strategy implemented today in computational algebra packages like MAGMA [BCP97] and GAP [GAP].

Neumann's creation of the EARNS algorithm [Neu87] in the 1980's allowed for efficient handling of primitive groups with an abelian socle, and is still in use today; the core idea is enumerating properties that must be satisfied by such a group, and using this to construct a usually-small set of elements through which to search. Neumann concurrently introduced a routine for computing the socle of a general primitive group, based on enumerating some cases, computing the solvable residual and Sylow p-subgroups, which was known to be possible due

to Kantor [Kan85] but only truly practical for solvable groups (see, for example, Butler's implementation for such groups in [But91]).

The largest missing piece in the socle puzzle was placed by Cannon and Holt in [CH97] which extended the ideas of Kantor for computing composition factors [Kan91] to computing the socle of an arbitrary permutation group. Their core algorithm efficiently computes the socle of all primitive permutation groups of degree up to 10^7. Broadly speaking, the algorithm identifies the O'Nan–Scott type of a group, using the classification of finite simple groups. Cannon and Holt also used a reduction to the primitive case via orbits and block systems to compute the socle of general imprimitive permutation groups satisfying that degree bound. This essay presents these two algorithms, with some adjustments and corrections, but with the same restriction on the degree. Currently, Unger [Ung] is increasing this limit up to 2^{32} for implementation in MAGMA. Advances in algorithms over the last 20 years, along with the increase in speed and memory of modern computers, mean that computation in groups of such large degrees is now feasible.

This essay will detail a standalone algorithm for computing the socle of a group following [Neu87], [CH97] and [Ung]. The background knowledge and the algorithm itself are both broken into three logical parts. Chapter 1 is an introduction to the theory of finite permutation groups, including the important notion of primitivity. Chapter 2 discusses general algorithmic concepts, as well as the concept of a base and strong generating set which is an integral component of many algorithms for computing with permutation groups. The background concludes in Chapter 3 with the theory of the socle and the O'Nan–Scott theorem.

The socle algorithm is first described for primitive groups in Chapters 4 and 5. The former focuses on primitive groups with a nonabelian socle via PRIMITIVESOCLE, while the latter covers the abelian case, via EARNS. The necessary knowledge of groups of affine type for the EARNS algorithm is also introduced in that chapter. Chapter 6 describes SOCLE to complete the algorithm for computing the socle. This computes it in a general permutation group by reducing to the primitive case.

Lastly, Chapter 7 gives some examples and background for the use of the socle in both permutation groups specifically, and in other areas of computational group theory.

Notation

The notation used often in this essay is listed here for clarity. Let G, H, K be groups, and let G act on the set Ω and $\alpha \in \Omega$, $\Delta \subseteq \Omega$. In all cases, if a set is a singleton, that is, $X = \{x\}$, x may be written instead of X, for example, $\langle x^G \rangle = \langle \{x\}^G \rangle = \bigcap_{x \in N \trianglelefteq G} N$.

$\mathrm{Sym}(\Omega)$	the symmetric group on Ω
S_n, A_n	symmetric, alternating group of degree n
C_n	cyclic group of order n
$\mathbb{F}_p$	finite field with p elements
$\mathrm{GL}(n,p)$, $\mathrm{AGL}(n,p)$, $\mathrm{SL}(n,p)$, $\mathrm{PSL}(n,p)$	general, affine general, special, projective special linear groups over $\mathbb{F}_p^n$
G^Ω	permutation representation of G on Ω induced by group action
α^g	(right) action of $g \in G$ on a point $\alpha \in \Omega$ (Definition 1.2). If $\Omega \leq G$, α^g is the conjugation action $g^{-1}\alpha g$ unless otherwise stated
α^G	orbit of α under G (Definition 1.8)
G_Δ, $G_{(\Delta)}$, G_α	setwise, pointwise, point stabiliser (Definition 1.9)
$\langle X_1, \ldots, X_n \rangle$	group generated as all finite products of elements (and their inverses) the sets X_i
$\langle x \mid p(x) \rangle$	group generated as all finite products of the elements x (and their inverses) that satisfy the predicate p
$\langle X^G \rangle$	normal closure $\bigcap_{X \subseteq N \trianglelefteq G} N = \left\langle g^{-1} X g \,\middle|\, g \in G \right\rangle$ of the set $X \subseteq G$ inside G
$H \times G$, G^m	direct product of H and G, direct power (direct product of m copies of G)
$H \rtimes_f G$	semidirect product of H and G, with homomorphism $f : G \to \mathrm{Aut}(H)$ (Definition 1.25)
$H \wr_\Gamma G$	wreath product of H with G^Γ (Definition 1.26)
$[a,b]$	commutator $a^{-1}b^{-1}ab$ of elements $a, b \in G$
$[H,K]$	subgroup $\langle [h,k] \mid h \in H, k \in K \rangle$. If $[H,K] = 1$, H centralises K
G'	derived subgroup $[G,G]$
$C_G(H)$, $N_G(H)$	centraliser, normaliser of H in G. The set of elements $g \in G$ such that $gh = hg$ for all $h \in H$ and $gH = Hg$ respectively
$Z(G)$	centre $C_G(G)$ of G

$H \leq G$, $H \trianglelefteq G$, $H \operatorname{char} G$	H is a subgroup, a normal subgroup, a characteristic subgroup (Definition 3.4) of G
$\operatorname{soc} G$	socle of G (Definition 3.9)
$O^\infty(G)$	solvable residual of G (Definition 4.2)
$O_p(G)$	p-core of G (Definition 5.12)
$\Omega_1(G)$	subgroup $\langle g \in G \mid g^p = 1 \rangle$ if G is a p-group (Definition 5.13)
$\operatorname{Fix}_\Delta(G)$	set of fixed points of G in Δ: $\{\delta \in \Delta \mid \delta^G = \delta\}$
$\operatorname{Aut}(G)$	automorphism group of G
$\operatorname{Inn}(G)$	inner automorphism group of G (automorphisms induced by conjugation by an element of G)
$\operatorname{Out}(G)$	outer automorphism group of G, $\operatorname{Aut}(G)/\operatorname{Inn}(G)$

CHAPTER 1

Permutation Groups, Group Actions and Primitivity

Every group can be realised as a set of permutations of some other set. This is a very general idea, but hints that studying permutation groups is a good way to understand some of the theory of groups. This study is naturally attacked from the angle of group actions, since a group action is built into the very definition of a permutation group.

Definition 1.1. *The set of all permutations of a set* Ω *forms the* symmetric group *of* Ω*, written* $\mathrm{Sym}(\Omega)$.

A subgroup of $\mathrm{Sym}(\Omega)$ *is called a* permutation group.

If $|\Omega| < \infty$, an element $\sigma \in \mathrm{Sym}(\Omega)$ can be written in cyclic permutation notation. This consists of a series of juxtaposed cycles, where a cycle $\tau \in \mathrm{Sym}(\Omega)$ is written $(a_1 a_2 \dots a_n)$ where τ maps a_1 to a_2, a_2 to a_3, ..., and a_n to a_1. Fixed points (cycles with a single element) are elided, with an exception for the identity, written $()$.

For example, if $\Omega = \{1,2,3,4,5\}$, the permutation σ which interchanges the two pairs 1 with 2 and 3 with 5 but leaves 4 fixed would be written $\sigma = (12)(35)$.

The theory of groups and finite permutation groups in particular is covered in detail elsewhere, such as Dixon and Mortimer's comprehensive textbook [DM96] and the enduring notes of Wielandt [Wie64]. This essay will prove some of the key results required in this chapter, and simply refer without proof to many more.

1.1. Group actions

A lot of interesting properties of groups can only be deduced when regarding them as a set of symmetries of some object. In this framework, one identifies each group elements with a bijective transformation of the object. We focus on groups that transform sets, and occasionally other groups. This section gives a brief overview of some elementary definitions and results with group actions.

Definition 1.2 (Action)**.** *We say* G acts *(from the right) on a set* Ω*, if there exists a group homomorphism* $\varphi : G \to \mathrm{Sym}(\Omega)$*. The action is written* $\omega^g = \varphi(g^{-1})(\omega)$ *for the image of* ω *under the permutation* $\varphi(g)$.

The map φ is sometimes also called a *permutation representation* of G, and the set Ω is called a G-set. The inversion is necessary to ensure that ω^g satisfies

Definition 1.3 (Faithful action)**.** *An action of a group* G *on a set* Ω*, with permutation representation* φ*, is said to be* faithful *if* $\ker \varphi = 1$.

Example 1.4. If $\Omega = \{1,\dots,n\}$, then the symmetric group $S_n = \mathrm{Sym}(\Omega)$ has a natural faithful action on Ω. If $n = 5$, then $\sigma = (12)(35) \in S_5$ acts like $1^\sigma = 2$, $4^\sigma = 4$, $5^\sigma = 3$ and so on.

We use the notation G^Ω to denote the group of permutations of $\mathrm{Sym}(\Omega)$ induced by G. This action is always faithful, that is, G^Ω is isomorphic to some subgroup of $\mathrm{Sym}(\Omega)$. If G acts faithfully on Ω then $G^\Omega \cong G$ otherwise it is some quotient group.

Proposition 1.5. *If a group G acts on a non-empty set Ω via the homomorphism φ, then*

a) $\omega^1 = \omega$ *for all* $\omega \in \Omega$
b) $(\omega^g)^h = \omega^{gh}$ *for all* $\omega \in \Omega$, $g,h \in G$

and, conversely, anything satisfying both properties induces a group homomorphism $\psi : G \to \mathrm{Sym}(\Omega)$ by $\psi(g)(\omega) = \omega^{g^{-1}}$.

Proof. φ is a group homomorphism, so $\varphi(1_G) = 1_{\mathrm{Sym}(\Omega)}$ and hence

$$\omega^1 = \varphi(1)(\omega) = 1(\omega) = \omega.$$

The second property follows similarly,

$$\begin{aligned}(\omega^g)^h &= \varphi(h^{-1})(\omega^g) && (1.6)\\ &= \varphi(h^{-1})(\varphi(g^{-1})\omega) = (\varphi(h^{-1})\varphi(g^{-1}))(\omega)\\ &= \varphi((gh)^{-1})(\omega)\\ &= \omega^{gh}. && (1.7)\end{aligned}$$

On the other hand, given an set action of G on Ω satisfying the two properties, take the function $\psi : G \to \mathrm{Sym}(\Omega)$ defined in the statement of this proposition. It is clear that $\psi(1)(\omega) = \omega$ so $\psi(1_G) = 1_{\mathrm{Sym}(\Omega)}$ as required. Equating the left-hand side of (1.6) with the right hand side of (1.7) directly and using the same working gives $\psi(h^{-1}g^{-1})(\omega) = (\psi(h^{-1})\psi(g^{-1}))(\omega)$ for each $\omega \in \Omega$. Hence ψ is a group homomorphism $G \to \mathrm{Sym}(\Omega)$ as desired. □

For convenience, the following definitions assume that the group G acts on the set Ω.

Definition 1.8 (Orbit)**.** *Let $\alpha \in \Omega$, the* orbit *of α is $\alpha^G := \{\alpha^g \mid g \in G\}$.*

Definition 1.9 (Stabiliser)**.** *Take $\Delta \subset \Omega$, then*

- $G_\Delta := \{g \in G \mid \alpha^g \in \Delta \ \forall \alpha \in \Delta\}$ *is the* set stabiliser *of Δ, and*
- $G_{(\Delta)} := \{g \in G \mid \alpha^g = \alpha \ \forall \alpha \in \Delta\}$ *is the* pointwise stabiliser *of Δ.*

If $\Delta = \{\alpha\}$ is a singleton, then we write the point stabiliser $G_\alpha := G_\Delta = G_{(\Delta)}$.

Similarly, the taking of repeated elementwise stabilisers is collapsed into a single subscript, that is, $G_{\alpha_1,\alpha_2,\ldots} := (G_{\alpha_1})_{\alpha_2} \ldots = G_{(\{\alpha_1,\alpha_2,\ldots\})}$.

Definition 1.10 (Transitivity)**.** *The group G acts* transitively *on Ω if all points lie in the same orbit; equivalently, if, for each $\alpha, \beta \in \Omega$, there exists $g \in G$ such that $\alpha^g = \beta$.*

Definition 1.11 (Regularity)**.** *The group G acts* regularly *on Ω if G^Ω is transitive and $G_\alpha = 1$ for some $\alpha \in \Omega$, that is, for each pair $\alpha, \beta \in \Omega$ there is exactly one $g \in G$ such that $\alpha^g = \beta$.*

The orbits and stabilizers of a group are intimately connected, via the well-known Orbit-Stabilizer theorem (e.g. [DM96, Theorem 1.4A]).

Theorem 1.12 (The Orbit-Stabilizer theorem)**.** *For $\alpha \in \Omega$, $\left|\alpha^G\right| = |G : G_\alpha|$; and, hence, if G is finite, $|G| = \left|\alpha^G\right| |G_\alpha|$.*

This theorem directly provides us with some precise information about regular groups.

Proposition 1.13. *Let G^Ω be regular, then*

(a) $|G| = |\Omega|$,
(b) if $H < G$, H^Ω is intransitive.

Proof. Let $\alpha \in \Omega$, by the Orbit-Stabilizer theorem, $|G| = \left|\alpha^G\right| |G_\alpha| = |\Omega| \cdot 1$, proving (a).

If we want $\alpha^H = \left\{\alpha^h \,\middle|\, h \in H\right\} = \Omega$, there is no possibility of the left-hand side being large enough unless $|H| \geq |\Omega|$. The first part implies that $|G| = |\Omega|$ so $|H| < |\Omega|$ and hence H cannot be transitive, proving (b). □

1.2. Primitivity

Primitivity is a notion that appears throughout computational group theory, since, in some sense, primitive group actions form building blocks of group actions.

Given a group G acting on a set Ω, we extend the group action G^Ω to $G^{\mathscr{P}(\Omega)}$ by writing $\Delta^g = \{\delta^g \mid \delta \in \Delta\}$ for any $\Delta \subset \Omega$.

Definition 1.14 (Block)**.** *A set $\Delta \subset \Omega$ is a* block *for G if either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for each $g \in G$.*

Every group action has two classes of *trivial* blocks: the singleton set $\{\omega\}$ for $\omega \in \Omega$, and the set Ω itself. Any blocks other than these is *nontrivial*.

Definition 1.15 (System of blocks)**.** *Let G act transitively on Ω, take a block $\Delta \subset \Omega$ for G, then $\Sigma := \{\Delta^g \mid g \in G\}$ partition Ω and form a* system of blocks.

Definition 1.16 (Primitivity)**.** *Let G act transitively on Ω, if there are no nontrivial blocks G is said to be* primitive*, otherwise it is* imprimitive.

Example 1.17. The natural action of S_n on $\Omega = \{1, \ldots, n\}$ is primitive. Take $\Delta \subset \Omega$ with $2 \leq |\Delta| < |\Omega|$, and choose $\delta_1 \in \Delta$, $\delta_2 \notin \Delta$. The transposition $g = (\delta_1 \delta_2) \in S_n$ has $\Delta \neq \Delta^g$ and $\Delta \cap \Delta^g = \Delta \setminus \{\delta_1\} \neq \emptyset$. Hence, there can be no nontrivial block system for S_n.

The key property required for that proof is just the 2-transitivity of S_n: a group G^Ω is 2-transitive if for any $\alpha \neq \beta, \gamma \neq \delta \in \Omega$, there is $g \in G$ such that $\alpha^g = \gamma$ and $\beta^g = \delta$. This generalises the notion of transitivity on the individual elements of Ω to transitivity on tuples (α, β). As one might expect, this can be generalised further, to k-transitivity for any k, but merely 2-transitivity is sufficient for primitivity, and, furthermore, there are diminishingly few examples of highly transitive groups: if $k \geq 6$, the only k-transitive groups are A_{n+2} and S_n for $n \geq k$.

Example 1.18. The cyclic group $C_{12} < S_{12}$ is imprimitive, with nontrivial block systems:

- $\{\{1,3,\ldots,11\},\{2,4,\ldots,12\}\}$
- $\{\{1,4,7,10\},\{2,5,8,11\},\{3,6,9,12\}\}$
- $\{\{1,5,9\},\{2,6,10\},\{3,7,11\},\{4,8,12\}\}$
- $\{\{1,7\},\{2,8\},\ldots,\{6,12\}\}$

As one would expect, there are connections between the subgroup structure of a group G^Ω and any blocks it has.

Proposition 1.19. *Let G^Ω is transitive and $\alpha \in \Omega$. There is a one-to-one correspondence between blocks Δ for G that contain α and subgroups H such that $G_\alpha \leq H \leq G$ given by $\Delta \mapsto G_\Delta$ with inverse $H \mapsto \alpha^H$.*

We note that we do include the singleton and whole-set trivial blocks, corresponding to $H = G_\alpha$ and $H = G$ respectively.

Proof. For a block Δ of G with $\alpha \in \Delta$, we can induce the subgroup that is the set stabiliser of Δ, that is, $H = G_\Delta = \{g \in G \,|\, \Delta^g = \Delta\}$. If $g \in G_\alpha$, then $\alpha^g = \alpha \in \Delta$, so we must have $\Delta^g = \Delta$ and hence $G_\alpha \leq H$. G is transitive on Ω, so Δ will be exactly an orbit of H: for every $\beta \in \Delta$ there is an element $g \in G$ such that $\alpha^g = \beta$, and so $g \in H$. Therefore, the map $\Delta \mapsto G_\Delta$ is injective: if blocks Δ_1 and Δ_2 containing α both have stabiliser H, then $\Delta_1 = \alpha^H = \Delta_2$.

We claim that for a general H as in the statement of the proposition the orbit α^H forms a block for G^Ω. Take $g \in G$, suppose there is $\beta \in (\alpha^H)^g \cap \alpha^H$, we can write $\beta = \alpha^{h_1 g} = \alpha^{h_2}$ and so $h_1 g h_2^{-1} \in G_\alpha \leq H$ hence $g \in H$. Thus, if the intersection is nonempty, it must be the full orbit α^H and hence it forms a block, which clearly contains α. Therefore, the map $\Delta \mapsto G_\Delta$ is surjective: every subgroup H with $G_\alpha \leq H \leq G$ can be realised as the set stabiliser of its orbit α^H.

Hence $\Delta \mapsto G_\Delta$ is a bijection, and the discussion above makes it clear that $H \mapsto \alpha^H$ is its inverse. □

This proposition leads us to the following, now easy, fact, which provides one technique by which one could test whether an arbitrary group is primitive.

Corollary 1.20. *G^Ω is primitive if and only if G_α is a maximal subgroup of G.*

In a similar vein to the previous proposition, normal subgroups form class of subgroups that induce blocks. However, it is definitely not true that these normal subgroups satisfy $G_\alpha \leq N \trianglelefteq G$ in general.

Proposition 1.21. *Let G^Ω be transitive and $N \trianglelefteq G$, then, for any $\omega \in \Omega$, the orbit ω^N forms a block.*

Proof. Take $g \in G$ arbitrary, the image of the orbit under the action of g is

$$(\omega^N)^g = \omega^{Ng} = \omega^{gN} = (\omega^g)^N,$$

which is also orbit of N, so it is either exactly ω^N, if $\omega^g \in \omega^N$, or, otherwise, it is disjoint. This is exactly saying that ω^N is a block. □

Corollary 1.22. *If G^Ω is primitive and $1 < N \trianglelefteq G$ then N^Ω is transitive.*

Proof. There are no nontrivial blocks of G^Ω, hence, the previous proposition shows that an orbit ω^N of N must either be $\{\omega\}$ or Ω. The action is faithful and N is nontrivial so it cannot be the former, thus $\omega^N = \Omega$. □

Corollary 1.23. *Let G^Ω be primitive, if $N \trianglelefteq G$ is regular, then N contains no other normal subgroups of G. That is, N is a minimal normal subgroup.*

Proof. Proposition 1.13 implies that any subgroup of N is intransitive, and so cannot be a normal subgroup of the primitive group G. □

As is common in mathematics, it is productive to consider the extremes of block systems for a group, since that restricts the properties they can have, form the most useful reduction tools and opens the field for certain easy-to-manipulate contradictions.

Definition 1.24. *Let G^Ω be a group, a nontrivial block $\Delta \subset \Omega$ is* minimal block *if it contains no other nontrivial blocks, that is, if $\{\omega\} \subseteq \Gamma \subset \Delta$ and Γ is a block, then $\Gamma = \{\omega\}$.*

Δ is a maximal block *if it contained in no other nontrivial blocks, that is, if $\Delta \subset \Gamma \subseteq \Omega$ and Γ is a block, then $\Gamma = \Omega$.*

Similarly, a minimal (maximal) block system is a block system containing minimal (maximal) blocks.

1.3. Wreath products

The wreath product $H \wr G$ constructs a new permutation group out of permutation groups G and H. It allows for constructing both primitive and imprimitive actions.

Definition 1.25 (Semidirect product)**.** *Let G, H be groups, and let G act on H by $f_g(h) = g^h$ such that $f_g \in \mathrm{Aut}(H)$ for all $g \in G$. The* semidirect product $H \rtimes_f G$ *is the group with elements $H \times G$ and operation*

$$(a,x)(b,y) = (ab^{x^{-1}}, xy).$$

It is a simple check to see that this operation is associative, with identity $(1,1)$ and inverse $(a,x)^{-1} = ((a^{-1})^x, x^{-1})$

This is a generalisation of the direct product; the semidirect and direct products are always equal as sets, it is just the additional group structure that can differ. Indeed, if the action is trivial, that is, $b^{x^{-1}} = b$ for all $x \in G$, then the multiplication in each group are equivalent, and so $H \rtimes_f G = H \times G$.

Definition 1.26 (Wreath product)**.** *Let H and G^Γ be groups, the* wreath product *is $H \wr_\Gamma G := K \rtimes G$ where $K = \prod_{\gamma\in\Gamma} H_\gamma$ with $H_\gamma \cong H$, and the action of G on K is*

$$(h_\alpha, h_\beta, \dots)^{g^{-1}} = (h_{\alpha^g}, h_{\beta^g}, \dots),$$

noting the use of g^{-1} on the left-hand side.

It is clear that $|H \wr_\Gamma G| = |G|\,|H|^{|\Gamma|}$.

By the restriction of this essay to finite G, only wreath products where Γ is finite need consideration. Without loss of generality, this is $\Gamma = \{1, \dots, n\}$ for some $n \geq 1$. We rarely write elements of a wreath product $H \wr_\Gamma G$ explicitly, but when we do, we denote them $(k; g) = (h_1, \dots, h_n; g)$, where $h_i \in H$ and $g \in G$.

In this notation, the group operation is,

$$(h_1, \dots, h_n; g)(h'_1, \dots, h'_n; g') = (h_1 h'_{1^g}, \dots, h_n h'_{n^g}; gg'). \tag{1.27}$$

Let H act on Δ, and G on Γ, then the wreath product $H \wr_\Gamma G$ has two natural actions, one on $\Delta \times \Gamma$ and one on $\Delta^{|\Gamma|}$. It is a tedious but entirely mechanical process to check that the two following definitions are indeed actions, that is, that they satisfy Proposition 1.5.

Proposition 1.28. *The following defines an action of $H \wr_\Gamma G$ on $\Omega = \Delta \times \Gamma$.*

$$(\delta, \gamma)^{(h_1,\dots,h_n;g)} = (\delta^{h_\gamma}, \gamma^g) \tag{1.29}$$

Proposition 1.30. *Let $\Omega = \prod_{\gamma\in\Gamma} \Delta_\gamma = \Delta^{|\Gamma|}$, where each $\Delta_\gamma = \Delta$. The following is an action of $H \wr_\Gamma G$ on Ω, called the* product action*.*

$$(\delta_1, \dots, \delta_n)^{(h_1,\dots,h_n;g)} = (\delta_{1^\star}^{h_{1^\star}}, \dots, \delta_{n^\star}^{h_{n^\star}}) \tag{1.31}$$

where $m^\star = m^{(g^{-1})}$.

If $|\Delta|, |\Gamma| \geq 2$, the action (1.29) is imprimitive, with at least one nontrivial block system given by $\{\Delta \times \{\gamma\} \mid \gamma \in \Gamma\}$: a group element $(h_1, \dots, h_n; g)$ moves the set $\Delta \times \{\gamma\}$ to $\Delta \times \{\gamma^g\}$.

On the other hand, the action (1.31) of $H \wr_\Gamma G$ can be primitive, and this forms one of the key classes of primitive groups we will study later. [DM96, Section 2.7] discusses this primitive group construction in more detail, in particular, they prove the exact conditions under which it is primitive:

Theorem 1.32 ([DM96, Lemma 2.7A])**.** *Given H^Δ, G^Γ, the product action* (1.31) *of $H \wr_\Gamma G$ on $\Omega = \Delta^{|\Gamma|}$ is primitive if and only if H^Δ is primitive but nonregular and G^Γ is transitive.*

Example 1.33. Take S_3 acting on $\Delta = \{1,2,3\}$ in the usual way. This is clearly transitive, and primitive, however it is not regular, since $G_1 = \{1,(23)\}$. Take $\langle a\rangle \cong C_2 = S_2$ with its natural action on $\{1,2\}$. Let $G = S_3 \wr_\Gamma C_2$. This has order $|G| = 6^2 \cdot 2 = 72$, and acts on $\Omega = \{(x,y)\,|\,x,y \in \{1,2,3\}\}$ with the product action, with degree $|\Omega| = 9$. Blocks are of equal size and partition Ω, so, if they exist, the only nontrivial ones must be of size 3.

Suppose there is a block B, and that $|B| \geq 2$, that is, we can find distinct points $(1,1),(\alpha,\beta) \in B$. By symmetry, $\alpha \neq 1$ without loss of generality; in fact, we can assume $\alpha = 2$.

Firstly, $g = (1,1;a) \in G$ gives $(1,1)^g = (1,1)$ and $(\alpha,\beta)^g = (\beta,\alpha)$ hence $(\beta,\alpha) \in B$.

Now choose $x \in S_3$ such that $x \neq 1$ and $\alpha^x = \alpha$: this is always possible by the definition of (α,β) (this is using the nonregularity of S_3). For this particular example, we can choose $x = (13)$.

Therefore, choosing $g = (x,1;1) \in G$ we see

$$(1,1)^g = (3,1) \quad \text{and} \quad (\alpha,\beta)^g = (\alpha,\beta).$$

The latter is in B, implying the same about the former. The same consideration with $h = (x,1;a)$ and $(\alpha,\beta)^h = (\beta,\alpha) \in B$ implies $(1,3) \in B$.

We now have 4 (or 5) distinct elements of B: $(1,1)$, (α,β), $(3,1)$ and $(1,3)$ (and possibly (β,α) if $\beta \neq \alpha$, but this is not necessary for this consideration). Thus $|B| > 3$ and so B too large to be anything but the whole of Ω, and so every block is trivial: G is primitive.

Example 1.34. Conversely, let us look at an example where H is regular, say $H = \langle a\rangle$ and $K = \langle b\rangle$ with $H \cong K \cong S_2$. Define $G = H \wr_{\{1,2\}} K$. This has order $2^2 \cdot 2 = 8$ and acts on $\Delta = \{(1,1),(1,2),(2,1),(2,2)\}$.

The set $B = \{(1,1),(2,2)\}$ forms a nontrivial block, and so G is imprimitive: it is easy to check that $(1,1;\_)$ and $(a,a;\_)$ leave B fixed, and that $(1,a;\_)$ and $(a,1;\_)$ move B to $\{(1,2),(2,1)\}$, where $\_$ can be either 1 or b. For example, for $g = (a,1;b) \in G$, $(1,1)^g = (1^1,1^a) = (1,2)$ and $(2,2)^g = (2^1,2^a) = (2,1)$ and so $B \cap B^g = \emptyset$ in this case.

CHAPTER 2

Computational Notions

Computational group theory is the study of algorithms for computing with groups, as such, one must understand algorithmic ideas as well as the group theoretic concepts.

2.1. Algorithms and computational complexity

An algorithm is a series of steps to be executed successively to return some useful result. There are two important components of a good algorithm: being correct, and running as efficiently as possible. The former is obviously desirable and is proved in the manner of a conventional mathematical theorem, but the latter can be difficult to quantify.

One important measure of efficiency is the asymptotic behaviour: how does the algorithm behave as the input data increases in size (for whatever definition of size makes sense for the problem at hand). A standard notation that summarises asymptotic behaviour is big-O notation; as the name suggests, $O(f)$ is the set that occurs most often, but the four common sets are:

$$\begin{aligned}
O(f) &:= \left\{ g : \mathbb{N} \to \mathbb{R}^+ \;\middle|\; \limsup_{n\to\infty} \frac{g(n)}{f(n)} < \infty \right\} \\
o(f) &:= \left\{ g : \mathbb{N} \to \mathbb{R}^+ \;\middle|\; \limsup_{n\to\infty} \frac{g(n)}{f(n)} = 0 \right\} \\
\Omega(f) &:= \left\{ g : \mathbb{N} \to \mathbb{R}^+ \;\middle|\; \liminf_{n\to\infty} \frac{g(n)}{f(n)} > 0 \right\} \\
\Theta(f) &:= O(f) \cap \Omega(f)
\end{aligned}$$

In words, $g \in O(f)$ if, for n sufficiently large, $g(n)$ is bounded above by $Cf(n)$ for some constant $C < \infty$, that is, the rate of growth of f is an upper bound for that of g. $g \in o(f)$ if f grows strictly faster than g, and $g \in \Omega(f)$ if the growth of f is a lower bound for that of g. Lastly $\Theta(f)$ is the set of functions that grow at the same rate as f. In this scheme, multiplication by a nonzero constant and addition of slow-growing terms is not encoded.

The function defining the set is often written implicitly, as just an expression inside the $O(\cdot)$. For example, if $f(n) = 2n^2 + n$ then $f \in O(n^2)$ since $\limsup(2n^2+n)/n^2 = 2 < \infty$.

This notation is used to summarise the behaviour of an algorithm given parameters about its input; for example, multiplying two d digit integers via a naive algorithm requires $O(d^2)$ additions, or sorting an array of length n can require

$O(n \log n)$ comparisons and $O(n)$ additional memory. These examples highlight that one often focuses only on certain high-level operations that are relevant to the problem, rather than tracking each and every instruction executed in the course of the algorithm.

When comparing two algorithms under this asymptotic regime, it is often the case that the algorithm with better asymptotics has a significantly larger constant factor or large low-order terms and so is only faster in practice for very large inputs. That said, the asymptotics do play an important part in the behaviour of an algorithm, and it is extremely undesirable to have algorithms that are exponential in the size of the input n, that is, $O(c^n)$ for some constant c, and, in fact, anything significantly larger than linear is unfavourable. In this context, we quantify "significant" as follows.

Definition 2.1. *Define the notation $O^{\sim}(\cdot)$ by $g(n) \in O^{\sim}(f(n))$ if*

$$g(n) \in O(f(n) \log^c n)$$

for some c. If $f(n) = n$ we say that g is nearly linear.

We talk about an algorithm being nearly-linear time (or nearly-linear memory use) if the function f that describes the time (respectively memory use) is nearly-linear. There is a large suite of permutation group algorithms that are nearly linear in the degree of the group, and even more than are polynomial; [Ser03] gives a detailed overview, particularly in chapters 3 and 6. However, there are also many examples of questions about permutation groups that require *backtrack searches* to answer, and these can be exponential in the degree.

2.2. Randomised algorithms

In computational group theory, many tasks can be solved more efficiently by introducing randomness; we will see an example of this in the next section. An algorithm using randomness can come in a few forms, we briefly discuss two.

A randomised algorithm A is called *Monte Carlo* if it possibly returns a incorrect answer. Let p be a bound on the probability of returning the incorrect answer. Obviously, p should be as small as possible and certainly must satisfy $p < 1/2$. If that is satisfied, one can induce an n-fold Monte Carlo algorithm A_n that returns an incorrect answer with arbitrarily small probability by running A n times repeatedly and independently, returning the most common answer. This process will definitely succeed as a whole if A returns more successes than failures, the probability of this *not* happening for A_n is bounded by the following binomial sum (for simplicity, we assume n is even, but the odd case is analogous):

$$p_n = \sum_{i=n/2}^{n} \binom{n}{i} p^i (1-p)^{n-i}.$$

If we write $p = \frac{1}{2+\varepsilon}$ for some $\varepsilon > 0$ we have

$$p_n \leq \left(\frac{1}{2+\varepsilon}\right)^n \sum_{i=n/2}^{n} \binom{n}{i} (1+\varepsilon)^{n-i}$$

We can bounding all terms in the sum by the largest, that is, by the term for $i = n/2$, and use Stirling's approximation to see that, for some $c \geq 1$,

$$\begin{aligned} &\leq \left(\frac{1}{2+\varepsilon}\right)^n nc\sqrt{\frac{\pi}{2n}} 2^n (1+\varepsilon)^{n/2} \\ &= \left(\frac{1+\varepsilon}{(1+\varepsilon/2)^2}\right)^{n/2} C\sqrt{n} = C\sqrt{n}X^{n/2} \end{aligned}$$

where $C > 0$ is some constant and $X = (1+\varepsilon)/(1+\varepsilon+\varepsilon^2/4) < 1$. This quantity tends nearly-exponentially to 0 as n tends to infinity and hence n-fold Monte Carlo achieves only requires n (close to) logarithmic in the desired bound on the probability of failure.

On the other hand, an algorithm B that returns either a correct answer or indicates that it failed is called a *Las Vegas* algorithm. As before, let p be a bound on the probability of failure. It must satisfy $p < 1$ and should be as small as possible. Similar to the Monte Carlo case, one can induce an n-fold Las Vegas algorithm B_n by running B at most n times, returning any non-failure answer. The probability of failing every time is bounded by $p_n = p^n$, which decreases to 0 exponentially. Hence, n-fold Las Vegas also only requires n logarithmic in the desired bound on the probability of failure. This also allows one to induce an algorithm with probabilistic runtime, but probability 1 of returning an answer, by running a Las Vegas algorithm until it returns non-failure. As long as each run is independent, this has finite expectation of completing.

A Las Vegas algorithm is generally preferable to a Monte Carlo algorithm due to the guarantee of correctness. We can upgrade the latter to the former when there is an efficient way to check for correctness; that is, given a Monte Carlo algorithm A, a Las Vegas algorithm for the same task is: execute A, check the output for correctness and indicate failure if it is wrong.

2.3. Bases and strong generating sets

A major factor influencing the performance of many algorithms throughout computer science is the choice of data representation: a good choice of data structure can give large asymptotic speed-ups. Group-theoretic algorithms are no different, and data structures related to group actions are the basis of the most common representation used for permutation groups. As above, let Ω be a finite set and G^Ω be a permutation group.

Definition 2.2 (Base)**.** *A* base *for G is a sequence $B = (\beta_1, \ldots, \beta_m) \subseteq \Omega$ with β_i pairwise distinct such that the pointwise stabiliser $G_{(B)} = 1$.*

The action of a group element $g \in G$ on a base, called its *base image*, uniquely determines that group element: suppose $h \in G$ such that $\beta_i^g = \beta_i^h$ for all $1 \leq i \leq m$, then $\beta_i^{gh^{-1}} = \beta_i$, so $gh^{-1} \in G_{(B)} = 1$ and hence $h = g$. Representing an element in terms of its base image can be a significant memory saving over the naive permutation representation, since a base is often only a polynomial function of the logarithm in the degree (such groups are called *short-base groups*).

Define the stabilisers $G^{(i)} := G_{(\beta_1,\ldots,\beta_{i-1})}$, so that a base induces a chain of subgroups

$$G = G^{(1)} \geq G^{(2)} \geq \ldots \geq G^{(m)} \geq G^{(m+1)} = 1$$

Computationally, it is desirable to reduce work where possible, in particular, this means not recomputing knowledge already known, and not computing knowledge that is entirely unnecessary. For a base, this can occur if $G^{(i)} = G^{(i+1)}$, that is, the image of the β_i element under the action of G does not distinguish between any more elements of G than the images of $\beta_1, \ldots, \beta_{i-1}$. A base with $G^{(i)} > G^{(i+1)}$ is called *nonredundant*. Note that there is no guarantee that a nonredundant base is a shortest base for G^Ω.

A base by itself is not quite enough to compute efficiently with groups, since the elements B of Ω alone encodes no information about the action of G.

Definition 2.3 (Strong generating set)**.** *Given a base $B = (\beta_1, \ldots, \beta_m) \subset \Omega$, $S \subset G$ is* strong generating set *(SGS) relative to B if it generates G and satisfies*

$$\langle S \cap G^{(i)} \rangle = G^{(i)}$$

for $1 \leq i \leq m+1$

The pair consisting of a strong generating set and its base is often abbreviated to BSGS.

Example 2.4. Let $G = \langle a \rangle \times \langle b \rangle$ where $\langle a \rangle \cong \langle b \rangle \cong S_2$, acting on $\{1,2\}$ in the natural way. This induces a natural action of G on $\{1_a, 2_a, 1_b, 2_b\}$. We have $G_{1_a} = \{1, b\}$ and $G_{(1_a,1_b)} = 1$ so $B = (1_a, 1_b)$ is a base for G, and thus our chain of stabilisers is $\langle a, b \rangle \geq \langle b \rangle \geq 1$. It is easy to verify that the obvious choice $S = \{a, b\}$ forms a strong generating set relative to this base.

Example 2.5. Let $G = S_4$ act on $\Omega = \{1, \ldots, 4\}$ in the natural way. $B = (1,2,3)$ forms a base, and is of minimum size: suppose we had a shorter sequence C, there is at least two distinct elements $\alpha, \beta \in \Omega \setminus C$ so $g = (\alpha\beta) \neq 1 \in G$ does not move any element of C, that is, $g \in G_{(C)}$ and hence C cannot be a base. This is true of all symmetric groups: the shortest bases of S_n are of length $n-1$. The stabiliser chain is

$$G = S_4 = G^{(1)} \geq \mathrm{Sym}(\{2,3,4\}) = G^{(2)} \geq \mathrm{Sym}(\{3,4\}) = G^{(3)} \geq G^{(4)}$$

The set $S = \{(14), (24), (34)\}$ generates G, $S \cap G^{(2)} = \{(24), (34)\}$ generates $G^{(2)}$ and $S \cap G^{(3)} = \{(34)\}$ generates $G^{(3)}$. Hence S is a strong generating set relative to B.

Sims [Sim70; Sim71] introduced these concepts, as well as the Schreier-Sims algorithm for computing them. As one of the most fundamental tools for computing with permutation groups, bases, strong generating sets and the Schreier-Sims algorithm have received detailed treatment elsewhere, for example, [HEO05, Section 4.4] or [Ser03, Chapter 4].

2.3.1. The Schreier-Sims algorithm

We give high-level overview of the Schreier-Sims algorithm for computing a BSGS and refer the reader to the references above for more detailed treatment, including pseudocode and proofs of correctness. The algorithm is called with a group G^Ω and a possibly empty initial sequence $B \subseteq \Omega$ and extends B to a full base for G while also building an SGS relative to B. The Schreier theorem forms the mathematical backing for the algorithm.

Theorem 2.6. *Let G be a group with generators $X = \{x_1, \ldots, x_n\}$, and let H be a subgroup. Take a transversal $T = \{t_1, \ldots, t_r\}$ of (right) coset representatives for H in G, and, for $x \in G$, let $\overline{x}$ denote the representative t_i such that $Ht_i = Hx$. Then,*

$$T' = \left\{ tx(\overline{tx})^{-1} \,\middle|\, t \in T, x \in X \right\}$$

is a generating set for H.

The Schreier-Sims algorithm constructs a chain of stabilisers $G > G^{(2)} > \ldots > G^{(m)} > 1$ while also using this theorem to compute generating sets for each subgroup. Taking the union of these generating sets gives a strong generating set for the original G and the corresponding sequence of elements of Ω forms a base. Using the Schreier theorem to directly compute generators for each stabiliser in isolation will often give a very large and redundant set of strong generators, so the Schreier-Sims algorithm is carefully designed to "sift" a new proposed generator down the chain of stabilisers to ensure that it is not redundant.

This algorithm is a stalwart of computational treatments of permutation groups. Many other computations rely on BSGS for performance and so the Schreier-Sims algorithm has had many improvements and adjustments. [Ser03, Section 4.2] describes two deterministic implementation strategies which trade-off time against memory. Usually the algorithm with lower memory use is preferred, since memory constraints are met first in practice. Let G^Ω have generators T and degree $n = |\Omega|$, the asymptotic properties of the two choices are:

Implementation	*Group operations*	*Memory*
1	$O(n^2 \log \lvert G\rvert (\log^2 \lvert G\rvert + \lvert T\rvert))$	$O(n^2 \log \lvert G\rvert + \lvert T\rvert n)$
2	$O(n^3 \log \lvert G\rvert (\log^2 \lvert G\rvert + \lvert T\rvert))$	$O(n \log^2 \lvert G\rvert + \lvert T\rvert n)$

As often occurs in computational group theory, there are randomised algorithms that are more efficient than the deterministic ones. [Bab+95] gives a nearly-linear time Monte Carlo algorithm for constructing a SGS in small-base groups. The user chooses a bound on the probability of failure, and then the algorithm constructs an SGS for G using $O(n \log n \log^4 |G| + |T| n \log |G|)$ group operations and $O(n \log |G| + |T| n)$ memory.

CHAPTER 3

The Socle of a Group

For a group G, the socle, denoted $\operatorname{soc} G$, is the subgroup generated by the minimal normal subgroups. This object inherits significant structure from its composition of minimal normal subgroups, and has even more when G is primitive, due to the O'Nan–Scott Theorem.

3.1. Minimal normal subgroups

Definition 3.1 (Minimal normal subgroup)**.** *$N \trianglelefteq G$ is a* minimal normal subgroup *if the only normal subgroups of G contained in N are N itself and the trivial group.*

Minimality is a strong restriction, particularly due to how normality interacts with intersections, allowing us to easily deduce the following interesting properties.

Proposition 3.2. *Let G be a group, $N \trianglelefteq G$ minimal and $M \trianglelefteq G$ arbitrary, then*

(a) either $N \cap M = 1$ or $N \leq M$.
(b) if $N \not\leq M$, then $[N,M] = 1$.
(c) if $N \not\leq M$, then $\langle N,M \rangle = NM \cong N \times M$.

Proof. (a) $N \cap M \trianglelefteq G$, but N is minimal, so $N \cap M$ cannot lie strictly between 1 and N and hence must be exactly one of those two.

(b) Take $a \in N$, $b \in M$, which induce an element $[a,b] = a^{-1}b^{-1}ab \in [N,M]$. Now find $g \in G$, and, remembering the normality of N and M, we have

$$\begin{aligned} g^{-1}[a,b]g &= g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg \\ &= (a^g)^{-1}(b^g)^{-1}a^g b^g \in [N,M] \end{aligned}$$

and so $[N,M] \trianglelefteq G$. Again by normality, $b^{-1}ab \in N$, so $[a,b] \in N$ and hence $[N,M] \leq N$, and similarly for M, meaning $[N,M] \leq N \cap M = 1$.

(c) The groups satisfy $N \cap M = 1$ and $[N,M] = 1$; the first guarantees $\langle N,M \rangle = NM$ uniquely and the second $NM \cong N \times M$. □

As stated above, minimality gives a lot of information. In particular we have the following.

Theorem 3.3. *If $N \trianglelefteq G$ is minimal, then $N = S_1 \times \ldots \times S_n$ where $S_i \cong S$ for some simple group S.*

The proof of this is easy, after some intermediate steps.

Definition 3.4 (Characteristicity)**.** *A subgroup $H \leq G$ is* characteristic *in G, written $H \operatorname{char} G$, if $\varphi(H) \subseteq H$ for every $\varphi \in \operatorname{Aut}(G)$.*

This is similar to normality, except normality has $\mathrm{Inn}(G)$, the set of inner automorphisms (conjugation by an element of G), instead of $\mathrm{Aut}(G)$. Unlike normality, however, characteristicity is transitive, and preserves certain nice properties of subgroups. In particular, it preserves normality.

Proposition 3.5. *If K char H char G (respectively, K char $H \trianglelefteq G$) is a chain of subgroups of G, then K char G (resp. $K \trianglelefteq G$).*

Proof. If $\varphi \in \mathrm{Aut}(G)$, then $\varphi(H) = H$ and so the restriction $\varphi|_H \in \mathrm{Aut}(H)$, hence $\varphi(K) = \varphi|_H(K) = K$ and thus K char G.

For $H \trianglelefteq G$ replace $\mathrm{Aut}(G)$ by $\mathrm{Inn}(G)$ in the previous sentence. □

Just like the concept of simplicity describing the lack of normal subgroups, we have a notion to describe a lack of characteristic subgroups.

Definition 3.6. *A group G is* characteristically simple *if it contains no characteristic subgroups.*

Lemma 3.7. *If G is characteristically simple, $G = S_1 \times \ldots \times S_n$ where $S_i \cong S$ for some simple group S.*

Proof. Suppose $N \trianglelefteq G$ is a minimal normal subgroup. The group H generated by $\mathscr{N} = \{\varphi(N) \mid \varphi \in \mathrm{Aut}(G)\}$ is a characteristic subgroup of G, and so by the characteristic simplicity of G, $H = G$.

The automorphic groups $\mathscr{N}$ are all minimal normal: if any image $\varphi(N)$ of N had a subgroup M that was normal in G, then $\varphi^{-1}(M) \triangleleft G$ and $\varphi^{-1}(M) \leq N$, contradicting the minimality of N.

Hence, we can write $G = N_1 \times \ldots \times N_k$ for some N_i as follows: set $N_1 = N$ and let ℓ represent the length of the sequence of N_i, that is, $\ell = 1$ initially. Let $M = \langle N_1, \ldots, N_\ell \rangle = N_1 \times \ldots \times N_\ell$, this equality follows from Proposition 3.2 (c). If $M \neq G$, then find $N_{\ell+1}$ such that $N_{\ell+1} \not\leq M$ and repeat. There is a finite number of automorphic images of N, and they generate G so this is guaranteed to succeed: if $M \neq G$ then there must be some image N^* of N such that $\langle M, N^* \rangle \geq M$, hence Proposition 3.2 implies the direct-product property.

Now suppose $K \trianglelefteq N_i$, N_i is a direct factor of G so K injects naturally into G, and, K centralises all factors N_j with $j \neq i$, hence if we write $g \in G$ as $g = (x_1, \ldots, x_k)$ where $x_j \in N_j$, then $g^{-1}Kg = x_i^{-1}Kx_i = K$ by the normality of K. But, N_i is minimal, so $K = 1$ or $K = N_i$, that is, N_i is simple. The N_j are all images of the original subgroup N under automorphisms of a larger group, and so are all isomorphic by construction. □

Lemma 3.8. *A minimal normal subgroup $N \trianglelefteq G$ is characteristically simple.*

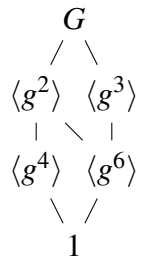
Proof. Suppose K char N. Take $g \in G$, N is normal in G so conjugation by g induces an automorphism φ_g of N (this is an inner automorphism of G, but the restriction to N is not necessarily inner in N). K is characteristic in N, so $\varphi_g(K) = g^{-1}Kg = K$, and hence $K \trianglelefteq G$. N is minimal normal, so we must have either $K = 1$ or $K = N$. □

Theorem 3.3 follows directly from the previous two lemmas.

3.2. The socle

Definition 3.9 (Socle)**.** *Let G be a group, the* socle *of G, denoted* $\operatorname{soc} G$*, is the subgroup generated by the minimal normal subgroups of G, or* 1 *if none exist.*

Example 3.10. Take $G = C_{12} = \langle g \rangle$ the cyclic group of order 12. G has 6 subgroups:



G is abelian so all subgroups are normal. The Hasse diagram demonstrates that neither $\langle g^2 \rangle$ nor $\langle g^3 \rangle$ are minimal, but that $H = \langle g^4 \rangle$ and $K = \langle g^6 \rangle$ are. Thus $\operatorname{soc} G = HK = \langle g^2 \rangle$. It is worth noting that $\operatorname{soc} G \cong C_3 \times C_2$ is a direct product of simple groups.

Proposition 3.11. *If G is finite, then* $\operatorname{soc} G > 1$.

Proof. G has a finite number of normal subgroups, so a maximal chain $G = N_0 > N_1 > N_2 \dots$ with $N_i \trianglelefteq G$ must be finite and terminates with $\dots > N_n > 1$ for some $n \geq 0$. Hence $\operatorname{soc} G \geq N_n \neq 1$. □

On the other hand, the socle of an infinite group has no such restriction.

Example 3.12. Take $G = \mathbb{Z}$. This is abelian so every subgroup is normal, and, every nontrivial subgroup is of the form $\langle n \rangle$ for some $n \geq 1$, however, $\langle n \rangle > \langle 2n \rangle$ and no subgroup can be minimal. Thus $\operatorname{soc} G = 1$.

Example 3.13 (Inspired by [DM96, Exercise 4.3.4])**.** Let $G = \prod_{i \in \mathbb{N}} G_i$ where $G_i = C_2$. This is also abelian with the property $x^2 = 1$ for all $x \in G$. Hence $N \triangleleft G$ is minimal if and only if $|N| = 2$: if $|N| = 2$ it clearly must be minimal, and if $|N| > 2$, take $x \in N$, then $\langle x \rangle = \{1, x\} < N$ is normal in G so N is not minimal. Hence, $\operatorname{soc} G$ is generated by the subgroups $\{1, x\}$ for each $x \in G$, and so $\operatorname{soc} G = G$.

From a computational perspective, knowing the socle of a group allows one to efficiently compute, for example, the chief and composition series of a group [CH97], automorphism groups and isomorphisms between groups [CH03] as well as conjugacy classes [CS97]. It is also useful for matrix group calculations, which are briefly reviewed in Chapter 7.

As hinted above, the socle has special structure which make it easier to work with and identify.

Proposition 3.14. *Let G be a finite group and let $N_1, \ldots, N_n$ be its minimal normal subgroups. There exists a sequence of indices i_j such that*

$$\operatorname{soc} G = N_{i_1} \times \ldots \times N_{i_k}$$

where $1 \leq i_1 < \ldots < i_k \leq n$.

Proof. This can be proved in a manner near-identical to the proof in Lemma 3.7 that a characteristically simple group G can be written $G = S_1 \times \ldots \times S_n$. The set $\mathscr{N}$ of automorphic images of a single minimal normal subgroup is replaced by the set of all minimal normal subgroups of G, and from there the same iterative construction works: the only two properties required are that $G = \langle \mathscr{N} \rangle$ and that the elements of $\mathscr{N}$ are minimal normal subgroups. □

In the adaptation of the proof of Lemma 3.7 to the previous proof, the discussion that the elements of $\mathscr{N}$ are simple and isomorphic must be omitted, since it is false, but we can combine the two lemmas to deduce a similar property.

Corollary 3.15. *Let G as above,*

$$\operatorname{soc} G = X_1 \times \ldots \times X_n$$

where each X_i is simple. The X_i are not necessarily isomorphic.

Proof. By Theorem 3.3, the minimal normal subgroup N_i can be written $S_1 \times \ldots \times S_m$ for $S_i \cong S$ with S simple. Expressing each N_{i_j} in Proposition 3.14 in this form gives the result. □

3.3. The O'Nan–Scott theorem

The study of socles of finite groups is deeply connected to primitive groups: the socle of a finite primitive group is the direct product of *isomorphic* simple groups. The O'Nan–Scott theorem provides a classification of primitive groups based on their socles, and vice versa: a classification of the possible socles of primitive groups.

This essay will list two characterisations of this theorem, focusing on the first, which is that given by [CH97], but there are many more: for example, Theorems 6.2.5 or 6.2.7 of [Ser03], or the version proved in [LPS88]. There is one definition required:

Definition 3.16 (Earns)**.** *Let G^Ω be a permutation group, $N \trianglelefteq G$ is an* earns *(elementary abelian regular normal subgroup) if N is elementary abelian, that is, $N \cong C_p^n$ for some prime p, and N^Ω is regular.*

Theorem 3.17 (O'Nan–Scott)**.** *Let $G \leq \operatorname{Sym}(\Omega)$ be primitive, with degree $|\Omega| = n$ and take $x \in \Omega$. Define $N := \operatorname{soc} G$, then $N = S_1 \times \ldots \times S_m$ where $S_i \cong S$ for some simple group S, and one of the following holds:*

I. $S \cong C_p$ for some prime p, and N is regular, that is, G has an elementary abelian regular normal subgroup (earns).
II. S is nonabelian. Let $\mathscr{F} = \{S_1, \ldots, S_m\}$. Exactly one of these holds:

(a) $\Omega = \Omega_1^m$, *G acts on Ω by the wreathed product action, and there is a faithful primitive permutation representation on Ω_1 of a group containing S_1 as a normal subgroup. G acts transitively by conjugation on $\mathscr{F}$.*

(b) $n = |S_1|^{(a-1)b}$ *for some integers a, b with $ab = m$, $a > 1$, $b \geq 1$, and $N_x = D_1 \times \ldots \times D_b$ where D_i is a diagonal subgroup of $S_{(i-1)a+1} \times \ldots \times S_{ia}$; and G acts transitively by conjugation on $\mathscr{F}$ with block system*

$$\left\{ \{S_{(i-1)a+1}, \ldots, S_{ia}\} \,\middle|\, i = 1, \ldots, b \right\}.$$

(c) $n = |S_1|^{m/2}$, $m > 1$, *N_x is as in II(b) with $a = 2$ and $b = m/2$, but G has two orbits on $\mathscr{F}$.*

(d) $n = |S_1|^m$, $m \geq 6$, $N_x = 1$ *and G acts transitively on $\mathscr{F}$.*

We will often refer to the case simply by its label, for example, unless otherwise stated, an isolated "case II(b)" refers to the first diagonal type case of the O'Nan–Scott theorem. We may also say that a group is of "type II(b)", meaning that the group falls into the stated case of the above theorem.

Proof. This statement of the theorem differs to that proved in [LPS88] or [DM96], so we reduce to the latter and refer the reader there to complete the proof. The statement of it is:

Theorem ([DM96, Theorem 4.1A])**.** *Let G be a finite primitive group of degree n and let H be the socle of G. Then either:*

(a) *H is a regular elementary abelian p-group for some prime p, $n = p^m := |H|$, and G is isomorphic to a subgroup of the affine group* $\mathrm{AGL}(m, p)$*; or*

(b) *H is isomorphic to a direct power T^m of a nonabelian simple group T and one of the following holds:*

  (i) *$m = 1$ and G is isomorphic to a subgroup of* $\mathrm{Aut}(T)$*;*

  (ii) *$m \geq 2$ and G is a group of "diagonal type" with $n = |T|^{m-1}$;*

  (iii) *$m \geq 2$ and for some proper divisor d of m and some primitive group U with a socle isomorphic to T^d, G is isomorphic to a subgroup of the wreath product $U \wr \mathrm{Sym}(m/d)$ with the product action, and $n = \ell^{m/d}$ where ℓ is the degree of U;*

  (iv) *$m \geq 6$, H is regular, and $n = |T|^m$*

All cases of Theorem 4.1A have $\mathrm{soc}\, G \cong S^m$ for some simple group S and some $m \geq 1$, so this assertion is true. It is clear that a group in case (a) falls into case I, indeed, they are essentially identical, except Theorem 4.1A gives us some additional information. See Chapter 5 for discussion of this case, in particular Theorem 5.10 which justifies the statement about being a subgroup of the affine group $\mathrm{AGL}(m, p)$.

Hence, suppose $H \cong T^m$ with T a nonabelian simple group; that is, case (b) and II of the respective theorems.

If $m = 1$ we must be in case (b)(i), and the only possibility is case II(a). The group $\mathrm{Aut}(T)$ isomorphically contains T as a normal subgroup, since

$$T/Z(T) \cong \mathrm{Inn}(T) \trianglelefteq \mathrm{Aut}(T),$$

and, in this case, T is nonabelian and simple, so $Z(T) = 1$ and hence $T \cong \mathrm{Inn}(T)$. Thus case (b)(i) falls into case II(a) with $m = 1$.

If G falls into case (b)(ii) of Theorem 4.1A, then we are in either case II(b) with $b = 1$ or II(c) with $m = 2$. [DM96, Theorem 4.5A] states that G is primitive if either $m = 2$ or $m \geq 3$ and G acts transitively by conjugation on the socle factors. Thus, the assertion about transitivity of the group action is satisfied, since there is only two socle factors: if they are left fixed by the action of G there are two orbits and G is of type II(c) or else the action is transitive and it is of type II(b). With $b = 1$, it is certainly true that the trivial block system $\{\{S_1, \ldots, S_m\}\}$ is a block system for this action in case II(b).

Suppose the socle $\mathrm{soc}\, G = H = N$ is regular, this places us into case (b)(iv) and II(d). The bound on m matches in the two cases, as does the value of $n = |T|^m = |S|^m$, hence it just remains to see that G acts transitively on $\{T_1, \ldots, T_m\}$ in Theorem 4.1A. [DM96, Theorem 4.7B] proves that $G_x < G$ acts transitively by conjugation on this set, so the full group must act transitively too, and we are done.

The most complicated case is (b)(iii). We can recursively apply the O'Nan–Scott theorem to the group U; the socle is nonabelian so it must lie in cases (b) and II. If U falls into case (b)(i), that is, $m = 1$, so $d = 1$, then we have $G \leq U \wr \mathrm{Sym}(m)$ with the product action. This construction fits exactly into case II(a) with $m \geq 2$. The subgroup component of $\mathrm{Sym}(m)$ must act transitively on the components of the wreath product for the group to be primitive, so the group is transitive by conjugation on $\mathscr{F}$.

If U falls into case (b)(ii), then it has the diagonal action, and falls into either case II(b) or II(c) with $b = d$. By the same Theorem 4.5A mentioned above, either $d = 2$ or $d \geq 3$ and U acts transitively by conjugation on the socle factors of U. Again, the $\mathrm{Sym}(m)$ component must act transitively on the components of the wreath product, thus, if U has two orbits on its socle factors then G has two orbits, otherwise, if U is transitive then G is transitive. These are the two only two possibilities and so classify the resulting groups G into case II(b) or II(c). If $G^{\mathscr{F}}$ is transitive, then the wreath product consists of m/d copies of U, say, U_i for $1 \leq i \leq m/d$, each of which has a set $\mathscr{F}_i$ of d simple socle factors. Conjugating the elements of one such $\mathscr{F}_i$ by an element $g = (k;h) \in G$ map the entirety of $\mathscr{F}_i$ to $\mathscr{F}_j$ for some j. This new set is either exactly $\mathscr{F}_i$ or it is disjoint. Therefore these sets $\mathscr{F}_i$ form blocks for $G^{\mathscr{F}}$, exactly as described by case II(b).

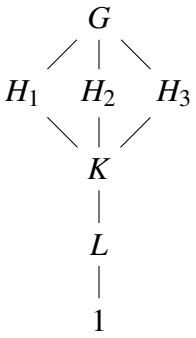
There are two remaining cases for U. It may lie in case (b)(iv), in which case $\mathrm{soc}\, G_\omega = (\mathrm{soc}\, U_\omega)^{m/d} = 1$, so the large group G also lies in case (b)(iv) and hence II(d). Lastly, it may recursively lie in case (b)(iii) itself, in which case the associating isomorphism $(U \wr H) \wr K \cong U \wr (H \wr K)$ can be applied to reduce to a case already handled. □

Groups G falling into case II(a) with $m = 1$ satisfy $\operatorname{soc} G = S_1 \trianglelefteq G \leq \operatorname{Aut}(S_1)$, that is, G is *almost simple*. The $G \leq \operatorname{Aut}(S_1)$ containment must occur, as S_1 is the unique minimal normal subgroup of G and so must be left setwise fixed by conjugation by G, an element $\sigma \in G \setminus \operatorname{Aut}(S_1)$ would necessarily have $S_1^\sigma \neq S_1$ and so cannot exist in G.

Example 3.18 (Case I)**.** Consider $G = S_3$. G contains a single normal subgroup $A_3 = C_3$, and thus $\operatorname{soc} G = C_3$. The group G is primitive, and so this socle demonstrates that it lies in case I.

Example 3.19 (Case II(a), with $m = 1$)**.** Take $G = S_5$. G has a unique normal subgroup A_5, which is not abelian (and thus not elementary abelian) so G is not in case I. Uniqueness shows $\operatorname{soc} G = A_5$. Approaching from the side of the O'Nan–Scott theorem, the unique non-abelian factor implies that G lies in case II with $m = 1$, and hence must be of type II(a). With a single socle factor it is certainly that G acts transitively by conjugation, and $\Omega_1 = \Omega$. This is the almost-simple case mentioned above; to just double check, $G \leq \operatorname{Aut}(A_5) = S_5$ as expected.

Example 3.20 (Case II(a), with $m > 1$)**.** Let $G = S_5 \wr C_2$ with the product action. This group has 7 normal subgroups, with the following relationships.



where $|G| = 2 \cdot 120^2$, $|H_1| = |H_2| = |H_3| = 120^2$, $|K| = 2 \cdot 60^2$ and $|L| = 60^2$. Thus $\operatorname{soc} G = L$ and so $L = A_5 \times A_5$, since it is definitely a direct product of simple groups and this is the only choice with the correct order.

Now, if we consider the O'Nan–Scott theorem, we can't be in case I since G does not have an earns. We have $n = 25 < 60 \leq |S_1|^k$ for any nonabelian simple group S_1 and $k \geq 1$, so we cannot be in any subcase of II except II(a).

Groups of diagonal type of diagonal type have less obvious constructions.

Example 3.21 (Case II(b) with $a = 2$, $b = 1$)**.** Let $G = A_5 \wr \langle x \rangle = (A_5 \times A_5) \rtimes \langle x \rangle$ where $x^2 = 1$ and x acts by exchanging the factors. Define the diagonal subgroup D of $A_5 \times A_5$ by $D = \{(g,g) \mid g \in A_5\}$ and induce the subgroup $H \leq G$ by $H = D \rtimes \langle x \rangle \cong D \times \langle x \rangle$. This isomorphism follows from the fact that the action of x is trivial on the diagonal subgroup.

Take $g = (t,u;v) \in G \setminus H$ and consider the subgroup $K = \langle g, H \rangle \leq G$. By construction, $t \neq u$, so $(tu^{-1}, 1; 1) = (t,u;v)(u^{-1}, u^{-1}; v^{-1}) \in K$ and it is not the identity. Conjugating this by all elements $(y,y;1) \in H$ generates the entirety of

$(A_5 \times 1) \rtimes 1$ since A_5 is simple. The remainder of G can be generated by conjugating by $(1,1;x) \in H$ to exchange the factors, giving $(A_5 \times A_5) \rtimes 1$, and multiplying by that element to change the $\ldots \rtimes 1$ to $\ldots \rtimes \langle x \rangle$. This demonstrates that H is a maximal subgroup of G.

The permutation action of G on the set of cosets $\Omega = \{Hg \,|\, g \in G\}$ is primitive by Corollary 1.20: the stabiliser is $G_{H\cdot 1} = H$ is maximal.

It is easy to see that $N = \operatorname{soc} G = A_5 \times A_5$ and hence stabiliser is $N_{H\cdot 1} = G_{H\cdot 1} \cap N = D$. The index $[G : H] = 60 = |A_5|$ and conjugation by $(1,1;x)$ swaps the socle factors, that is, $(g,1;1)^{(1,1;x)} = (1,g;1)$, so G is transitive on the set $\mathscr{F} = \{A_5 \times 1, 1 \times A_5\}$.

There are two socle factors, that is, $m = 2$ and the degree 60 is not a perfect square, so G is of O'Nan–Scott type II(b) or II(c), which matches the stabiliser N_α. It was demonstrated that $G^{\mathscr{F}}$ is transitive, so G must be of type II(b).

Example 3.22 (Case II(c) with $b = 1$)**.** Let $G = A_5 \times A_5$, acting on A_5 by $x^{(g,h)} = g^{-1}xh$ which is easy to verify as an action. We have that $A_5 \times 1$ and $1 \times A_5$ each act transitively, since $x^{(x,y)} = y$ for all $x, y \in A_5$, and regularly, since $x^{(g,1)} = x$ and $y^{(1,h)} = y$ if and only if $g = 1$ in each case. We also have that G^{A_5} is primitive: suppose we had a block $B \leq A_5$ containing 1. This must be a subgroup of A_5, if $b \in B$ then $b^{(1,b^{-1})} = 1 \in B$, so $1^{(1,b^{-1})} = b^{-1} \in B$, and if $a, b \in B$, then $(b^{-1})^{(1,b)} = 1 \in B$ implying $a^{(1,b)} = ab \in B$. The diagonal elements $(g,g) \in G$ act on $1 \in B$ by $1^{(g,g)} = g^{-1}g = 1$, and hence we must have $b^{(g,g)} = g^{-1}bg \in B$ for all $b \in B$, that is, $B \trianglelefteq A_5$ and so B is a trivial block, either $B = 1$ or $B = A_5$ since A_5 is simple.

The minimal normal subgroups of G are $A_5 \times 1$ and $1 \times A_5$, so $\operatorname{soc} G = G$ and the socle factors are $\mathscr{F} = \{A_5 \times 1, 1 \times A_5\}$. These factors are normal subgroups of G, so are fixed by G acting by conjugation. Case II(d) is clearly impossible, and if G lay in case II(a), $n = 60$ would require that $m = 1$ contradicting the existence of two socle factors, therefore, G is a group of diagonal type. The intransitivity (with two orbits) of $G^{\mathscr{F}}$ shows that G lies specifically in case II(c). To confirm the stated property of the stabiliser of $\operatorname{soc} G$, the stabiliser of 1 is

$$G_1 = \left\{ (g,h) \in G \,\middle|\, 1^{(g,h)} = g^{-1}h = 1 \right\}$$

and hence G_1 is the set of elements such that $g = h$: exactly the diagonal subgroup of G.

Examples of groups of diagonal type with larger m can be built from the above two sorts of groups via wreath products with the product action, as covered in the reduction in the proof of the O'Nan–Scott theorem. Another way to construct groups of type II(b) is replacing the wreath factor $\langle x \rangle$ with any primitive permutation group in Example 3.21. Case II(d) is the last case, and consists of very large groups: the degree is at least $|A_5|^6$ which does not fall into the degree bound of 10^7.

CHAPTER 4

Computing the socle of a primitive group

To begin the computation of the socle, the focus is on primitive groups. The O'Nan–Scott theorem (Theorem 3.17) detailed in the previous chapter gives a lot of information about primitive groups and the anatomy of the socle of such a group which suggests that this might be a productive approach.

As the socle is generated by minimal normal subgroups, one approach to finding it would be enumerating the normal subgroups, recording those that are minimal and then taking the subgroup that they generate. This could be done by iterating over group elements $z \in G$ and taking the normal closures $\langle z^G \rangle$: every minimal normal subgroup is sure to appear in this list. Of course, $|G|$ can be exponential (or close to) in the degree, so this approach would be rather inefficient, for example, $G = S_k \wr S_2$ with the product action is primitive for $k \geq 3$ by Theorem 1.32, and has degree $n = k^2$ but order $2(k!)^2 \in \Theta(n^{1/2} e^{\sqrt{n}(\log n - 2)})$, which is essentially exponential in n. That said, the approach of taking normal closures is useful, after restricting the search to a small subset, or even isolating a single element.

Fortunately, a naive approach like the above is entirely ignoring the additional information gained by the restriction on G that it is primitive, that is to say, by using this structure a more efficient algorithm can be devised.

[CH97] introduced a PRIMITIVESOCLE algorithm for computing the socle of a primitive group of degree at most 10^7, building off the COMPSER procedure of [Kan91] which computed compositions series of groups of degree at most 10^6. We give a revised version of the PRIMITIVESOCLE again limited to degree 10^7; the new procedure is given in Algorithm 1. It rectifies a few errors and handles an edge case that was missed in the original description; these rectifications are, for the most part, due to [Ung].

Similarly, the algorithm uses a table of the possibilities for the structure of the solvable residual in certain cases. The original table of [CH97] missed an entry, our table in Table 1 includes this missing value.

The socle of a primitive group is a direct product of isomorphic simple group. The exact structure of these simple groups is also important, that is, it is valuable for the S_i to be returned. [CH97] includes procedure PRIMITIVECHIEFSERIES for computing the chief series of a primitive group, and a similar one for corresponding composition. As demonstrated in Chapter 7, both of these utilise socle factors along with the O'Nan–Scott theorem.

4.1. PRIMITIVESOCLE is correct

There are two procedures that make up PRIMITIVESOCLE and the subprocedure REGULARFACTORS, listed in Algorithm 2. The latter is used to compute

Algorithm 1 The PRIMITIVESOCLE algorithm of [CH97] incorporating adjustments of [Ung]. This takes a primitive permutation group G^Ω with degree $|\Omega| \leq 10^7$ and computes $\operatorname{soc} G$ and, when $\operatorname{soc} G$ is nonabelian, $\mathscr{F} = \{S_1, \ldots, S_m\}$ where S_i are the simple factors of $\operatorname{soc} G$.

procedure PRIMITIVESOCLE(G, Ω)
  if G has an earns N **then return** N ▷ *Case I*

  Set $T \leftarrow O^\infty(G)$, the solvable residual of G.
  if $|\Omega| = 5^{10}$, and $60^i \mid |T|$ and $|T| \mid 2^{10}60^i$ for some $i \in \{11, 12\}$ and T is imprimitive **then** ▷ *Special case of II(a)*
    return $\operatorname{soc} T$
  if $|T|$ is the order of a finite simple group **then**
    return T, $\{T\}$ ▷ *Case II(a) with $m = 1$*

  Try to find t, u, s, $m \geq 5$ and n_1 such that $|T| = tus^m$, $n = n_1^m$, $s = |S|$ for some nonabelian simple group S that acts primitively on a set of size n_1, t is a divisor of $|\operatorname{Aut}(S)/S|^m$ and u is the order of a perfect transitive permutation group of degree m. (Possibilities listed in Table 1.)
  if t, u, s, m and n_1 exist **then** ▷ *Case II(a) with $m > 1$ and $|T/\operatorname{soc} G| > 1$*
    Take $\omega \in \Omega$.
    Set $A \leftarrow \alpha^{G_\omega}$ a shortest orbit of G_ω on $\Omega \setminus \{\omega\}$.
    Find a nontrivial block system Σ for G^A_ω such that $|\Sigma| = m$.
    Take a block $B \in \Sigma$.
    Set $R \leftarrow G_{x,(A \setminus B)}$.
    Set $N \leftarrow \langle (R')^G \rangle$.
    return N, $\left\{ \langle (R')^N \rangle^g \,\middle|\, g \in G \right\}$
  else ▷ $T = \operatorname{soc} G$
    $|T| = s^m$ where $s = |S|$ for some simple group S and some $m \geq 2$.
    if $m = 2$, $s = n$ **then** ▷ *Cases II(b) or II(c) with $m = 2$*
      return T, REGULARFACTORS(T, Ω)
    else
      Let K be the kernel of the action of T on a minimal block system Σ.
      if $n = s^{m/2}$ **then** ▷ *Case II(b) with $a = 2$ or Case II(c)*
        Take $\varphi : K \to K^B$ the action epimorphism on a block B
        Set $\{S_1, S_2\} \leftarrow$ REGULARFACTORS(K^B, Ω).
        return T, $\left\{ \varphi^{-1}(S_i)^g \,\middle|\, g \in G, i \in \{1,2\} \right\}$
      else ▷ *Case II(b) with $a \geq 3$, or case II(a) with $T = \operatorname{soc} G$.*
        return T, $\{K^g \mid g \in G\}$

Algorithm 2 An adjusted version of REGULARFACTORS of [CH97]. This computes S_1, S_2 for $G^\Omega = S_1 \times S_2$ primitive and in case II(b) or case II(c). This uses the fact that $C_G(\langle g^G \rangle)$ is now known to be able to be computed efficiently.

1: **procedure** REGULARFACTORS(G, Ω)
2: Write $|G| = s^2$.
3: Choose $\alpha \in \Omega$.
4: Find a shortest orbit $G_\alpha^{\Omega \setminus \{\alpha\}}$, with representative $\beta \in \Omega$.
5: Set $C = C_G(G_{\alpha,\beta})$.
6: Find $g \in C$ of prime order such that $\left|\langle g^G \rangle\right| = s$.
7: **return** $\{\langle g^G \rangle, C_G(\langle g^G \rangle)\}$.

the socle factors in a few special cases. Both procedures assume that a BSGS is known for G^Ω so that the calculations are efficient. We initially examine the second procedure since it is the least complicated.

4.1.1. REGULARFACTORS

This procedure works with a specific subset of primitive groups, groups of diagonal type where $\operatorname{soc} G = G$; more specifically, case II(b) of the O'Nan–Scott theorem with $a = 2$, $b = 1$, or case II(c) with $m = 2$.

This task could be accomplished by a direct search through G looking for elements that have the appropriately-sized normal closure but this is needlessly inefficient, as the search space can be efficiently reduced. The goal is to minimise the order of the subgroup C while ensuring that it contains elements of at least one of S_1 or S_2. The choice of β in a shortest orbit makes $G_{\alpha,\beta}$ as large as possible by the orbit-stabiliser theorem, which heuristically minimises the size of its centraliser C.

The implementation described here differs to that given in [CH97], since it is now known that for a normal subgroup $N \triangleleft G$, the centraliser $C_G(N)$ can be computed in nearly linear time. [Ser03, Section 6.1.4] describes an algorithm for this task. By definition, $\langle g^G \rangle$ is normal in G so this applies on line (7) of REGULARFACTORS.

Theorem 4.1. *Let G^Ω be a primitive group, such that $G = S_1 \times S_2$ where $S_1 \cong S_2 \cong S$ are simple and the stabiliser G_ω is the diagonal subgroup of G, that is, $G_\omega = \{(s,s) \mid s \in S\}$. Then,* REGULARFACTORS$(G, \Omega) = \{S_1, S_2\}$.

Proof. By definition, we must have $|G| = |S|^2$ so the statement on line (2) is valid.

G has two proper normal subgroups, S_1 and S_2, so if we can find an element g such that $\langle g^G \rangle < G$ we have one of the factors S_i.

S_1^Ω is transitive, so this is non-empty. Furthermore, S_1 (and S_2) is regular on Ω since, for any $\omega \in \Omega$, $(S_1)_\omega = S_1 \cap G_\omega$, and the only shared point between the diagonal subgroup G_ω and S_1 is exactly 1. Hence $1 = (S_1)_\beta = S_1 \cap G_\beta$, and similarly for S_2. This regularity justifies the name REGULARFACTORS. It also shows that there is a unique $x \in S_1$ such that $\alpha^x = \beta$. Conjugating by this element

n_1	s
5	
6	$\lvert A_5\rvert$
7	$\lvert \mathrm{PSL}(3,2)\rvert$
8	$\lvert \mathrm{PSL}(3,2)\rvert$
9	$\lvert \mathrm{PSL}(2,8)\rvert$
10	$\lvert A_5\rvert$; $\lvert A_6\rvert$
11	$\lvert \mathrm{PSL}(2,11)\rvert$; $\lvert M_{11}\rvert$
12	$\lvert \mathrm{PSL}(2,11)\rvert$; $\lvert M_{11}\rvert$; $\lvert M_{12}\rvert$
13	$\lvert \mathrm{PSL}(3,3)\rvert$
14	$\lvert \mathrm{PSL}(2,13)\rvert$
15	$\lvert A_6\rvert$; $\lvert A_7\rvert$; $\lvert A_8\rvert$
16	
17	$\lvert \mathrm{PSL}(2,16)\rvert$
18	$\lvert \mathrm{PSL}(2,17)\rvert$
19	
20	$\lvert \mathrm{PSL}(2,19)\rvert$
21	$\lvert A_7\rvert$; $\lvert \mathrm{PSL}(3,4)\rvert$; $\lvert \mathrm{PSL}(2,7)\rvert$
22	$\lvert M_{22}\rvert$
23	$\lvert M_{23}\rvert$
24	$\lvert \mathrm{PSL}(2,23)\rvert$; $\lvert M_{24}\rvert$
25	

m	u
5	
6	$\lvert A_5\rvert$
7	$\lvert \mathrm{PSL}(3,2)\rvert$
8	$\lvert \mathrm{PSL}(3,2)\rvert$; $\lvert \mathrm{AGL}(3,2)\rvert$
9	$\lvert \mathrm{PSL}(2,8)\rvert$
10	$\lvert A_5\rvert$; $2^4 \cdot \lvert A_5\rvert$; $\lvert A_6\rvert$

Table 1 – Tables of the possibilities for the variables on line (10) of PRIMITIVESOCLE. This differs to those given in [CH97] due to the inclusion of the extra entry $n_1 = 21$, $s = |\mathrm{PSL}(2,7)|$. For all n_1 and m, $s = |A_{n_1}|$ and $u = |A_m|$ are valid, but are omitted for clarity. An empty entry for a value of n_1 or m corresponds to those alternative groups being the only possibilities for s or u respectively.

gives $x^{-1}G_{\alpha,\beta}x \leq x^{-1}G_\alpha x = G_\beta$, implying $[x, G_{\alpha,\beta}] \leq G_\beta$. S_1 is normal in G, so $[x, G_{\alpha,\beta}] \leq S_1$ and hence $[x, G_{\alpha,\beta}] \leq G_\beta \cap S_1 = 1$. That is, S_1 (and similarly S_2) centralise $G_{\alpha,\beta}$, and thus $x \in C_G(G_{\alpha,\beta}) = C$.

From the above, $x \in C \cap S_1$, so the subgroup $C \cap S_1 \leq G$ is nontrivial, and hence it contains elements of prime order. Any non-identity element $g \in C \cap S_1$ has $\langle g^G \rangle = S_1$ and thus the statement on line (6) can be satisfied. The same holds for S_2 and $S_2 \cap C$.

The subgroups S_1 and S_2 are the only normal subgroups of G with order s, so if g has the property stated on line (6) then we have either $\langle g^G \rangle = S_1$ or $\langle g^G \rangle = S_2$. The two groups S_1 and S_2 are the unique simple minimal normal subgroups, so $C_G(S_1) \cap S_1 = Z(S_1) = 1$ and proving $C_G(S_1) = S_2$ and vice versa, hence the returned value on line (7) is exactly $\{S_1, S_2\}$ as desired. □

4.1.2. PRIMITIVESOCLE

The core algorithm in this chapter is PRIMITIVESOCLE. It takes an primitive permutation group G^Ω with degree $|\Omega| \leq 10^7$ and computes its socle.

At a high-level, PRIMITIVESOCLE is deciding the case of the O'Nan–Scott theorem in which G lies. For the most part, this is performed via purely arithmetic tests by examining and precomputing the possibilities for each step. This is possible due to the classification of finite simple group, since that ensures that enumerations can cover ever case.

Groups covered by case I of the O'Nan–Scott can be easily identified and handled by EARNS, as we will see in Chapter 5. For a nonabelian socle, it turns out that the solvable residual of G is the socle in many cases, this group is straightforward-to-compute.

Definition 4.2 (Solvable residual)**.** *Let G be a finite group. The* solvable residual *of G, written $O^\infty(G)$, is the last term of its derived series. That is, let $G^{(0)} := G$ and $G^{(i)} := G^{(i-1)'} = [G^{(i-1)}, G^{(i-1)}]$, then the derived series is*

$$G^{(0)} \triangleright G^{(1)} \triangleright \ldots \triangleright G^{(n)} = O^\infty(G),$$

where n is such that $G^{(n+1)} = G^{(n)}$.

There is good reason for the name "solvable residual", as the following result demonstrates. Recall that a group is solvable if all its composition factors are abelian.

Proposition 4.3. *$O^\infty(G)$ is the unique normal subgroup of G that is minimal with respect to the property that the quotient $G/O^\infty(G)$ is solvable.*

Proof. We assert that the derived series induces a subnormal series of $G/O^\infty(G)$, where every quotient is abelian. A composition series that refines this will satisfy the same property, that is, the composition factors are all abelian, proving $G/O^\infty(G)$ is solvable. To see the assertion, consider the series

$$G/O^\infty(G) \triangleright G^{(1)}/O^\infty(G) \triangleright \ldots \triangleright 1 = O^\infty(G)/O^\infty(G).$$

By the third isomorphism theorem for groups, the quotient of successive terms is

$$\left(G^{(i)}/O^\infty(G)\right) / \left(G^{(i+1)}/O^\infty(G)\right) \cong G^{(i)}/G^{(i+1)} = G^{(i)}/G^{(i)'}$$

which is abelian, by the definition of the derived subgroup.

Therefore, if $O^\infty(G) = 1$ the result is clearly true, so assume $O^\infty(G) > 1$.

Let $H = O^\infty(G)$ and let $K \trianglelefteq H$ be a subgroup such that H/K is simple, that is, the first term in a composition series for H. Take a subgroup $N \trianglelefteq G$ with

$N < O^\infty(G)$, a composition series for H/N can be lifted to one for G/N by placing it after a composition series for G/H lifted into G/N. Any composition series for H/N will include of these leading H/K factors and so such a factor will be included in the composition series for G/N. Thus, by showing that H/K is always non-abelian, we can deduce that G/N will be insolvable.

Suppose, by way of contradiction that H/K is abelian, then $(H/K)' = 1$. We also have $H' = H$ by construction. For any group L, a homomorphism $\varphi : H \to L$ satisfies $\varphi(H) = \varphi(H') \leq L'$: for any $g, h \in H$, $\varphi([g,h]) = [\varphi(g), \varphi(h)] \in L'$. In particular, if we take the quotient map $\varphi : H \to H/K$ we have $\varphi(H) = (H/K)'$ as φ is surjective. By definition, $\ker \varphi = K$ and hence $1 = (H/K)' \cong H/K$. We conclude that $H = K$ and so we have a contradiction, that is, every composition series for $O^\infty(G)$ starts with a nonabelian group.

To see uniqueness, suppose H and K are subgroups of G such that G/H and G/K are solvable. We claim that $H \cap K \triangleleft G$ also has a solvable quotient $G/(H \cap K)$. Indeed, the correspondence between normal subgroups of G and normal subgroups in a quotient of G implies that the composition factors between $G/(H \cap K)$ and $H/(H \cap K)$ are quotients of abelian groups and hence abelian themselves. For the other half, $H/(H \cap K) \cong HK/K$, and $HK \leq G$ so HK/K must be solvable. Chaining these together as $1 \triangleleft H/(H \cap K) \triangleleft G/(H \cap K)$ shows that $G/(H \cap K)$ is also solvable. □

The commutator subgroup of a group can be constructed efficiently (see, for example, [Ser03, Theorem 2.3.12]) so this offers a good avenue by which we can compute the socle, when it works. The O'Nan–Scott theorem allows us to deduce when $\operatorname{soc} G = O^\infty(G)$ and when this is not true. We can explicitly tabulate the violations of this $\operatorname{soc} G = O^\infty(G)$ "rule", which is done in Table 1. The degree bound is necessary due to this tabulation and enumeration component of the algorithm.

The degree bound also nontrivially reduces the number of possibilities implied by O'Nan–Scott theorem that can occur. In particular, it is completely impossible for PRIMITIVESOCLE to meet a group in case II(d), since that case stipulates that G has degree $|\Omega| = |S_1|^m$ with S_1 nonabelian and simple, and $m \geq 6$, hence the degree $|\Omega| \geq 60^6 \approx 46.7 \cdot 10^9 \geq 10^7$.

Similarly, the other nonabelian cases have small bounds on some parameters, although each of these cases is still possible with degree below 10^7.

(a) $\Omega = \Omega_1^m$, and S_1 is a simple subgroup of a group that acts faithful on Ω_1, thus, S_1 itself acts faithfully. The factor S_1 is at least as large as A_5, and, there is no faithful permutation representation (injection into S_n) of A_5 on a set with fewer than 5 elements, since $|S_4| = 24 < |A_5|$. Hence $n_1 = |\Omega_1| \geq 5$ and so $1 \leq m \leq \log_5 10^7 \approx 10.1$.

(b) $|\Omega| = |S_1|^{(a-1)b}$ with $ab = m$, $a > 1$ and $b \geq 1$. $|S_1| \geq 60$, so we have $(a-1)b \leq \log_{60} 10^7 \approx 3.9$. The only possibilities are $a = 2$, $b = 1, 2, 3$ or $a = 3, 4$, $b = 1$, which gives $m = 2, 3, 4, 6$.

(c) $|\Omega| = |S_1|^{m/2}$ with $m > 1$ even, so $m/2 \leq 3.9$ and hence $m = 2, 4, 6$.

In the latter two cases, for $m > 2$, the degree is $|\Omega| = |S_1|^k$ for some $k \geq 2$ and so there are also only 8 possibilities for S_1; when sorted by increasing order, the 9th nonabelian simple group (isomorphic to $\mathrm{PSL}(2,19)$) has order 3420, and hence the smallest degree associated with this group is $3240^2 > 10^7$. In those cases with $m = 2$ we have $|\Omega| = |S_1|$ and there are 97 simple groups with order below 10^7.

The first case does not have a small restriction in this manner: $G = A_n$ falls into this case for any $n \geq 5$, and there are $10^7 - 5$ nonabelian simple groups of this form with natural degree bounded by 10^7. Fortunately, as we will show later, we do not need to enumerate such a large set of possibilities, because solvability considerations will show that we must have $m \geq 5$ for there to be a chance that $\operatorname{soc} G \neq O^\infty(G)$.

Case I, when the socle is elementary abelian, is handled by the EARNS algorithm detailed in Chapter 5. This procedure does not need the extra restriction available by imposing the degree bound, hence we do not consider it above.

We are now ready to prove PRIMITIVESOCLE is correct.

Theorem 4.4. *Let G^Ω be a finite primitive permutation group with degree $|\Omega| \leq 10^7$, then,* PRIMITIVESOCLE$(G,\Omega) = \operatorname{soc} G, \mathscr{F}$*, where $\mathscr{F}$ only exists if* $\operatorname{soc} G$ *is nonabelian.*

In the case that $\operatorname{soc} G$ *is nonabelian, $\mathscr{F}$ contains the simple factors of the socle, that is, $\mathscr{F} = \{S_1, \ldots, S_m\}$ where* $\operatorname{soc} G = S_1 \times \ldots \times S_m$ *and the S_i are isomorphic simple groups.*

We proceed by walking through the algorithm, justifying each step.

4.1.2.1. Line (2). A primitive group G has an earns N if and only if $\operatorname{soc} G = N$, and if and only if G falls into case I, so testing for the existence of an earns and returning it is a perfect way to completely cover groups of type I. This step is covered in far more detail in Chapter 5, in particular, the if-and-only-if assertions are proved as Corollary 5.11.

4.1.2.2. Line (4). If G does not have an earns, G cannot lie in case I and hence it must have a nonabelian socle factor; in particular, G contains a nonabelian simple group and so cannot be solvable: this simple group occurs in the composition factors. The conclusion is that the solvable residual $T = O^\infty(G) \neq 1$. Furthermore, every nonabelian simple subgroup of G lies in T, including those that form $\operatorname{soc} G$ and hence $\operatorname{soc} G \leq T$. Moreover, $\operatorname{soc} G \trianglelefteq G$ so $\operatorname{soc} G \trianglelefteq T$.

The rest of this subsection is devoted to proving some cases in which $\operatorname{soc} G = O^\infty(G)$, motivating the choice to examine this subgroup.

Lemma 4.5. *Let G^Ω be a primitive group falling into cases II(b) or II(c) of the O'Nan–Scott theorem with degree at most 10^7, then $G/\operatorname{soc} G$ is solvable.*

Proof. The group G permutes the set $\mathscr{F} = \{S_1, \ldots, S_m\}$ by conjugation. Let $\varphi : G \to G^{\mathscr{F}}$ be the action epimorphism. If $g \in G$, then $g \in \ker \varphi$ if and only

if $S_i^g = S_i$ for each $1 \leq i \leq m$, that is, if $g \in \mathrm{Aut}(S_1) \times \ldots \times \mathrm{Aut}(S_m)$. By the simplicity, it is true that $\mathrm{Aut}(S_i) \cong S_i.\mathrm{Out}(S_i)$; but it is not necessarily true that $\mathrm{Out}(S_i) \subseteq G$, so define $H_i = \mathrm{Out}(S_i) \cap G$ and then $\ker\varphi \leq (\mathrm{soc}\, G).H =: K$ where $H = \prod H_i$. Hence, we have

$$G/\mathrm{soc}\, G \leq (G/K).H \leq (G/\ker\varphi).H \leq \mathrm{Sym}(\mathscr{F}).H$$

Recall the Schreier conjecture (now a theorem by the classification of finite simple groups): $\mathrm{Out}(S)$ is solvable for any finite simple group S, hence the direct product H contains only solvable groups H_i. It only remains to see that the component $G^{\mathscr{F}} \cong G/\ker\varphi$ inside $\mathrm{Sym}(\mathscr{F})$ is solvable.

As listed above, the possibilities for m in the two diagonal type cases are $m = 2,3,4,6$. For $m \leq 4$ the covering group $\mathrm{Sym}(\mathscr{F})$ is solvable and so the proof is complete. Assume $m = 6$. Case II(b) has $a = 3$, $b = 2$ and hence $G^{\mathscr{F}}$ is imprimitive with block $\{S_1, S_2, S_3\}$ and so is solvable.

Case II(c) has $G^{\mathscr{F}}$ intransitive with two orbits. If $m = 6$, these orbits must be of length 3: suppose we had an orbit $\{S_1, S_2\}$ of length 2 (respectively, $\{S_1\}$ of length 1) then $N = S_1 \times S_2$ (respectively $N = S_1$) is normal in G. G is primitive so these must be transitive and hence $|N| = |S_1|^k \geq |\Omega| = |S_1|$ for either $k = 1$ or $k = 2$, a contradiction.

Hence $G^{\mathscr{F}} \leq S_3 \times S_3 \leq S_6$, and thus must be solvable. □

By near-identical reasoning, we have the following similar result for the other nonabelian case we consider. The restriction on $m = |\mathscr{F}|$ ensures that the $\mathrm{Sym}(\mathscr{F})$ component of the wreath product is solvable.

Lemma 4.6. *Let G^Ω be a primitive group falling into case II(a) of the O'Nan–Scott theorem with $m \leq 4$, then $G/\mathrm{soc}\, G$ is solvable.*

Corollary 4.7. *If G^Ω is as in either of the previous lemmas, then* $\mathrm{soc}\, G = O^\infty(G)$.

Proof. The facts $\mathrm{soc}\, G \trianglelefteq G$ and $G/\mathrm{soc}\, G$ solvable shows $\mathrm{soc}\, G \geq O^\infty(G)$ by Proposition 4.3. It was proved above that $\mathrm{soc}\, G \leq O^\infty(G)$. □

Therefore, with the degree bound of 10^7, the only possibility for $\mathrm{soc}\, G \neq O^\infty(G)$ is case II(a) with $m \geq 5$.

4.1.2.3. Lines (5-6). If G does lie in such an exceptional case, that is, if $T \neq \mathrm{soc}\, G$, having T^Ω primitive would give significant power. It can be verified computationally that the only possibilities for $T \neq \mathrm{soc}\, G$ imprimitive are the conditions checked on line (5). Since T only differs from G by solvable components, we have $\mathrm{soc}\, T = \mathrm{soc}\, G$ and hence a recursive call to SOCLE from Chapter 6 suffices to complete the computation. In this case, G is primitive and T is not, so $T < G$ is a strict subgroup and the mutual recursion will terminate.

Example 4.8. Let $G = A_5 \wr_\Gamma H$ with the product action, where $H = A_5 \wr C_2$ acts on

$$\Gamma = \{(1,1), \ldots, (5,1), (1,2), \ldots, (5,2)\}$$

with the imprimitive action (1.29). The overall group G has degree $5^{10} \leq 10^7$ and $\operatorname{soc} G = A_5^{10}$ since it is of O'Nan–Scott type II(a), but $O^\infty(G) = A_5 \wr (A_5 \times A_5)$. The direct product $A_5 \times A_5$ is intransitive on Γ, with two orbits $\{(1,\alpha),\ldots,(5,\alpha)\}$ for $\alpha = 1,2$, and so $O^\infty(G)$ is imprimitive by Theorem 1.32. This example is due to Unger.

After this check, the remainder of PRIMITIVESOCLE can assume that $T = \operatorname{soc} G$ or T is primitive.

4.1.2.4. Lines (7-8). Suppose $|T|$ is the order of a finite simple group; we wish to see that T must actually be a (nonabelian) finite simple group in this case, and hence see that it is the socle of G.

We state a simplified version of Cameron-Teague Power Order Theorem.

Theorem 4.9 ([Kim+90, Theorem 6.1])**.** *If S_1, S_2 are finite simple groups and n_1, n_2 are integers such that $|S_1|^{n_1} = |S_2|^{n_2}$, then $|S_1| = |S_2|$ and $n_1 = n_2$.*

Hence, if $T = \operatorname{soc} G$, we have $|T| = |S_1|^m = |S|$ for some simple S, and thus $|S_1| = |S|$ and $m = 1$. This m implies G must be of O'Nan–Scott type II(a) since the other cases require $m \geq 2$.

Hence, it only remains to consider the case $T \neq \operatorname{soc} G$, in this case G also lies in case II(a). [Kan91] gives two important lemmas relating to this case.

Lemma 4.10 ([Kan91, Lemma 1])**.** *If G^Ω lies in case II(a) of the O'Nan–Scott theorem, then $|G| = tu|S_1|^k$ where $u = \left|G^{\mathscr{F}}\right|$ and $t = |T|$ for some subgroup of $(\operatorname{Aut}(S_1)/S_1)^k \cong \operatorname{Out}(S_1)^k$.*

This lemma is relating the order of G to the order of the wreath products $S_1 \wr U$ and $\operatorname{Aut}(S_1) \wr U$, where $U^{\mathscr{F}} \cong G^{\mathscr{F}}$.

Lemma 4.11 ([Kan91, Lemma 3])**.** *There is no simple group H with $|H| = tus^m$ for t, u, s and m in Table 1 and either*

- *$t = 2^i$ for $i \leq m$, or*
- *$t = 2^i$ for $i \leq 2m$ when $s = 360 = |A_6|$, $n_1 = 10$ or $s = 4080 = |\mathrm{PSL}(2,16)|$, $n_1 = 17$, or*
- *$t = 3^i$ for $i \leq m$ when $s = 504 = |\mathrm{PSL}(2,8)|$, or*
- *$t = 2^i 3^j$ for $i, j \leq m$ when $s = 20160 = |\mathrm{PSL}(3,4)|$.*

The case $s = 20160$ was added by [CH97], and $s = 4080$ was added by [Ung]. These lie outside the degree bound of 10^6 that was considered in [Kan91]. The t quantities and their upper bounds reflect the size of the outer automorphism groups $\operatorname{Aut}(S)/S$, where S is a simple group with $|S| = s$.

We know that T is primitive, so it has order as described in the first lemma, and hence by the second lemma we cannot have $|T| = |S|$ for any simple group. We have thus shown that if T has order matching that of a simple group we must have $\operatorname{soc} G = T$ and $m = 1$, validating the socle and the $\mathscr{F}$ returned on line (8).

4.1.2.5. Line (10). We now detect when $T > \operatorname{soc} G$. The $m \geq 5$ restriction is justified above by Corollary 4.7, the equation for $|T|$ is justified by [Kan91, Lemma 1] listed above and the equation $n = n_1^m$ is clearly just rephrasing the relationship $\Omega = \Omega_1^m$ from the O'Nan–Scott theorem.

The important difference between the condition here and the condition in [Kan91, Lemma 1] is the addition of the criterion that the group U with order u is perfect, that is, that $[U,U] = U$. This criterion is related to the solvable residual T, and implies that repeated commutators will not eliminate the U factor of the wreath product, leaving $T > \operatorname{soc} G$. A list of possibilities was first tabulated by [Kan91] up to degree $n \leq 10^6$; Kantor extended this to degree $n \leq 10^7$, which was reproduced in [CH97], although this missed an entry, $n_1 = 21$, $s = \mathrm{PSL}(2,7)$. The corrected table appears as Table 1 and also as [Ser03, Table 6.8]. The requirement that $m \geq 5$ implies that $n_1^5 \leq 10^7$ and hence $n_1 \leq 25$.

Most groups with $\operatorname{soc} G > T$ have $|\mathrm{Out}(S_1)| = 2$, and hence $t = 2^i$ for some $i \leq m$, others have slightly larger outer automorphism groups. The full list of possibilities is given in Lemma 4.11. This can again be computed simply by enumerating the outer automorphism groups of the small number of simple groups S that satisfy the degree restriction.

Lastly, we just need to see that the existence of such t, u, s, m and n_1 implies that we are definitely in case II(a) with $T \neq \operatorname{soc} G$. That is, eliminate the possibility that we are direct computation of the possible order and degree of $T = \operatorname{soc} G$. It is possible for $|T| = tus^m$ in three cases with degree below 10^7: $T = A_5^6$, $tus^m = 1 \cdot 60 \cdot 60^5$, with free choice of $n_1 \in \{5,6,10\}$. However the degrees do not match, in either of the diagonal cases of the O'Nan–Scott theorem the degree n of T is $n = 60^3 \neq n_1^5$ for any of the possibilities for n_1.

4.1.2.6. Lines (11-18). In the case that $O^\infty(G) \neq \operatorname{soc} G$, G acts by the product action, and $m \geq 5$. [DM96, Theorem 4.3B] shows that G must have a unique minimal normal subgroup N in this case, and so finding the socle is equivalent to finding N, which can be performed by finding some element or set of elements that are definitely contained within N.

We have that G lies between $S \wr U$ and $\mathrm{Aut}(S) \wr U$ for some perfect transitive group U of degree m. Consider the point stabiliser G_ω by identifying $\omega = (\omega_1, \ldots, \omega_1) \in \Omega_1^m = \Omega$ for any $\omega_1 \in \Omega_1$. We can assume ω is homogeneous like this without loss of generality, because G is primitive and hence Theorem 1.32 implies that the components of the wreath product that comprise G are transitive.

For simplicity, we work with $G = S \wr U$ and cover the $G > S \wr U$ case below. In this case, G_ω is the set of elements $g = (s_1, \ldots, s_m; u) \in G$ such that

$$(\omega_1, \ldots, \omega_1)^g = (\omega_1^{s_1 \star}, \ldots, \omega_1^{s_m \star}) = (\omega_1, \ldots, \omega_1)$$

where $k^\star = k^{u^{-1}}$. This happens if and only if $s_i \in S_{\omega_1}$ for all $i \in \{1, \ldots, m\}$ and hence $G_\omega = S_{\omega_1} \wr U$. We note that $|S| \geq 60$ and $|\Omega_1| \leq 25$ and so S^{Ω_1} is far too large to be regular, meaning $S_{\omega_1} \neq 1$. Therefore, a shortest orbit A of G_ω on

$\Omega \setminus \{\omega\}$ is

$$A = (A', \omega_1, \ldots, \omega_1) \cup (\omega_1, A', \omega_1, \ldots, \omega_1) \cup \ldots \cup (\omega_1, \ldots, \omega_1, A') \tag{4.12}$$

where A' is a shortest orbit of S_{ω_1} on $\Omega_1 \setminus \{\omega_1\}$. It is clear that each component $(\ldots, A', \ldots)$ forms a block of the action of the stabiliser on A, and it that there are m components. Hence the block system Σ on line (14) exists.

If $G > S \wr U$, the reasoning above still applies, since the whole group $G \leq \mathrm{Aut}(S) \wr U$ acts by the product action so the extension above $S \wr U$ cannot perturb the block structure.

We note that it is often the case that G^Σ_ω is primitive. This action is precisely that of U, the factor of the wreath product, [Kan91] states that one should be able to find U primitive with a degree bound of 10^6; but increasing the bound to 10^7 introduces a single new entry $m = 10$, $u = 2^4 |A_5|$ of Table 1 which can be imprimitive. In summary, one can compute Σ by finding a block system such that G^Σ_ω is primitive, unless $n_1 = 5$, $m = 10$ and $u = 2^4 |A_5|$ or $u = |A_5|$ with $2^4 \mid t$, in which case the block system of size m has to be found by other means.

Without loss of generality, we can assume that the block B chosen was the first term of (4.12), and hence the stabiliser $R = G_{\omega,(A \setminus B)}$ consists of only those elements that do not move any of the remaining blocks, in particular, $(S_1)_\omega \leq R \leq \mathrm{Aut}(S_1)_\omega$ where S_1 is the first term of the direct product in the semidirect product that makes up the wreath product and the exact group between S_1 and $\mathrm{Aut}(S_1)$ depends on the nature of the extension above $S \wr U$ that makes up G. In either case, the derived subgroup $R' \leq S_1$. A direct computational check of each possibility in Table 1 shows that S_ω is always nonabelian, and so $1 < S'_\omega \leq R'$ and hence $R' \neq 1$.

Therefore, $R' \leq S_1 \leq \mathrm{soc}\, G$, and thus the normal closure $N = \langle R'^G \rangle$ must be the minimal normal subgroup $\mathrm{soc}\, G$ and so line (17) is correct. The group S_1 is one of the simple factors of $\mathrm{soc}\, G$, and hence is one of its minimal normal subgroup, implying that we can find one socle factor via $S_1 = \langle R'^{\mathrm{soc}\, G} \rangle$. This case of the O'Nan–Scott theorem has that G acts transitively by conjugation on the socle factors, so computing the remaining factors is a matter of computing the G conjugates of S_1. This justifies line (18) as correct.

4.1.2.7. Line (20). We are guaranteed that $T = \mathrm{soc}\, G$, and so could return immediately if that were all that was desired. If the set of socle factors $\mathscr{F}$ is also wanted PRIMITIVESOCLE must continue. Since it is the socle, $|T| = |S|^m$ for some simple group S and integer m, and by Lemma 4.9, this pair is unique. The case $m = 1$ was eliminated on line (7), so the assertion $m \geq 2$ holds.

4.1.2.8. Lines (21-22). In the case that $m = 2$ and $s = n$, it is clear that $T = S_1 \times S_2$. We will see that T itself is primitive and that it falls into either of the two diagonal type cases. Hence, T^Ω satisfies the preconditions for REGULAR-FACTORS and so we can compute S_1, S_2 directly via that. It just remains to prove the properties of T.

Lemma 4.13. *If G^Ω is primitive with $\operatorname{soc} G = S_1 \times S_2$ where $S_1 \cong S_2$ are non-abelian simple groups and $|S_i| = |\Omega| \leq 10^7$ then G is not of product type, that is, G does not lie in case II(a).*

Proof. Assume we are in case II(a) with socle factor S_1 acting on a set Ω_1; we must have $|\Omega| = |S_1| = |\Omega_1|^2$. Hence, the socle factor must have order that is a square. By the classification of finite simple groups, the only such simple groups with order less than 10^{20} are two of the projective symplectic groups:

$$|\mathrm{PSp}_4(7)| = 2^8 3^2 5^2 7^4 \approx 1.4 \cdot 10^8$$
$$|\mathrm{PSp}_4(41)| = 2^8 3^2 5^2 7^2 29^2 41^4 \approx 6.3 \cdot 10^{15}$$

Hence, there is no possibility to be in case II(a) with the degree bound of $|\Omega| \leq 10^7$ as those two options are larger than that, and any others are even larger. □

Thus, G is of diagonal type, and hence [DM96, Theorem 4.5A (i)] guarantees that T is primitive since $m = 2$.

4.1.2.9. Line (24). If PRIMITIVESOCLE has reached this point, that is, if $O^\infty(G) = \operatorname{soc} G$ with $m \neq 2$ or $s \neq n$ then the following must be true.

Lemma 4.14. *If* PRIMITIVESOCLE *reaches line (24), T^Ω is imprimitive.*

Proof. Recall that $S_i \trianglelefteq T$. The case $m = 1$ has been eliminated by line (7). If G is of O'Nan–Scott type II(a) with $m \geq 2$, each S_i acts on a set $\Omega_1 \subset \Omega$, so S_i is not transitive on Ω and thus T^Ω cannot be primitive due to the normality of S_i.

If G does not lie in case II(a), it must be of diagonal type. It is guaranteed that $s = n$ if G is of diagonal type and $m = 2$, so the previous section eliminates this case entirely, leaving only $m \geq 3$. If T were primitive, it would be of diagonal type with $\operatorname{soc} T = T$ and socle factors S_i. The normality of S_i inside T means that T acts with $m \geq 3$ orbits on $\mathscr{F}$, and so T cannot satisfy either of the diagonal type cases which mandate only 1 or 2 orbits. Hence, T cannot be primitive if G is of diagonal type. □

The socle T is normal in G, so T^Ω is transitive by Corollary 1.22. Thus, the assertion on line (24) is valid: a minimal block system Σ exists.

4.1.2.10. Lines (25-28). Suppose we have $|\Omega| = n = s^{m/2}$ where s is the order of some simple group. We will show that G must be of diagonal type. Similarly to the $m = 2$, $s = n$ case, if G has the wreathed product action, we have $n = s^{m/2} = |\Omega_1|^m$ for some set Ω_1, hence, taking $m/2$-th roots, we have $s = |\Omega_1|^2$. The same reasoning as in the proof of Lemma 4.13 proves no such s exists and hence G cannot lie in case II(a). We note that the largest order s that satisfies our degree bound is $10^{14/m} \leq 10^7$ so the logic in that proof still applies.

The kernel K of the block action is, essentially, the stabiliser of a block. The stabiliser of a block must contain the group stabiliser as a maximal subgroup or else there will be a nontrivial block n strictly contained within Σ but this was

constructed to be minimal. Hence, the stabiliser is

$$(S_1 \times S_2) \times D_2 \times \ldots \times D_b.$$

The kernel K is the largest normal subgroup of T contained within that, the *core*. Thus, $K = S_1 \times S_2$ since the diagonal groups D_i cannot contain any nontrivial normal subgroups of T. The restriction K^B acts primitively on B, again by the minimality of Σ, hence, the preconditions for REGULARFACTORS are satisfied and so it can be used to compute S_1 and S_2 directly, as done on line (27). As seen by the correspondence between [DM96, Theorem 4.1A(b)(iii)] and case II(c) of Theorem 3.17 in the proof of the latter, G acts transitively by conjugation on the D_i, so $\mathscr{F}$ is the set of conjugates of S_1 and S_2 and hence line (28) is correct.

4.1.2.11. Line (30). If PRIMITIVESOCLE falls through to the very last case, G is in case II(a) or case II(b) with $a \geq 3$ and hence $b = 1$. As above, the kernel K is the core of the stabiliser of a block. We will break into those two remaining cases of the O'Nan–Scott theorem to show that this core is one of the simple factors S_1, and then the transitivity of the conjugation action of G on $\mathscr{F}$ proves line (30) correct.

We take a similar approach to the previous section, by expanding the point stabiliser. In case II(a), the stabiliser of a point $\omega = (\omega_1, \ldots, \omega_m)$ will be $(S_1)_{\omega_1} \times \ldots \times (S_m)_{\omega_m}$ and the stabiliser of a block is that same expression with $(S_1)_{\omega_1}$ replaced by S_1. The stabilisers are strictly smaller than their transitive parent group S_i and so contain no normal subgroups since that parent group is simple, hence the core K is exactly S_1.

The second case (II(b)) is similar to the previous section with the block stabiliser $S_1 \times D$ where D is the diagonal subgroup of $S_2 \times \ldots \times S_m$. For the same reasons, this has core $K = S_1$.

Therefore, we have shown that PRIMITIVESOCLE is correct.

CHAPTER 5

Groups of Affine Type and EARNS

For a vector space V, we construct the *affine group* $\mathrm{AGL}(V)$ via

$$\mathrm{AGL}(V) = V \rtimes \mathrm{GL}(V),$$

considering V with its abelian group structure and $\mathrm{GL}(V)$ with its natural action of left multiplication on V. Concretely, $\mathrm{AGL}(V)$ is the Cartesian product of sets $V \times \mathrm{GL}(V)$ with operation

$$(v,A)(w,B) = (v + Aw, AB)$$

It is a straight-forward check that $(0,I)$ is the identity and $(v,A)^{-1} = (-A^{-1}v, A^{-1})$ is the inverse of (v,A).

A group G is *of affine type* if $G \leq \mathrm{AGL}(V)$, which we can characterise by $G = W \rtimes M$ for some subspace $W \subseteq V$ and $M \leq \mathrm{GL}(W)$. Without loss of generality, only the case where V is minimal, that is, $W = V$, needs consideration; if this is not true, then we can just write $G \leq \mathrm{AGL}(W)$.

In this chapter, we consider only the finite vector space $V = \mathbb{F}_p^n$ where $\mathbb{F}_p$ is the field with p elements, for some prime power p, which we abbreviate as

$$\mathrm{AGL}(n,p) := \mathbb{F}_p^n \rtimes \mathrm{GL}(n,p)$$

Example 5.1. Elementary abelian groups are of affine type. Let $G = C_p^n \cong \mathbb{F}_p^n$ be such a group, then G can be identified with the subgroup $\mathbb{F}_p^n \rtimes \{I_n\} < \mathrm{AGL}(n,p)$.

Proposition 5.2. *The affine group* $\mathrm{AGL}(n,p)$ *has an faithful action on* $\mathbb{F}_p^n$*, defined by*

$$x^{(v,A)} = A^{-1}(x+v) \tag{5.3}$$

for $x \in \mathbb{F}_p^n$ *and* $(v,A) \in \mathrm{AGL}(n,p)$.

Proof. We proceed directly; take $(w,B) \in \mathrm{AGL}(n,p)$, then

$$\begin{aligned}\left(x^{(v,A)}\right)^{(w,B)} &= \left(A^{-1}(x+v)\right)^{(w,B)} = B^{-1}\left(A^{-1}(x+v)+w\right) \\ &= B^{-1}A^{-1}(x+(v+Aw)) = x^{(x+Aw,AB)} = x^{(x,A)(w,B)}\end{aligned}$$

Now take an arbitrary $(v,A) \in \mathrm{AGL}(n,p)$ such that $x^{(v,A)} = x$ for all $x \in \mathbb{F}_p^n$, in particular, it is true for $x = -v$, which gives $-v = (-v)^{(v,A)} = A^{-1}(-v+v) = 0$. Therefore, A must satisfy $A^{-1}x = x$ for all $x \in \mathbb{F}_p^n$ and meaning $A = I_n$. Thus the kernel of the action of $\mathrm{AGL}(n,p)$ on $\mathbb{F}_n^p$ is trivial and so $\mathrm{AGL}(n,p)^{\mathbb{F}_n^p}$ is faithful. □

Any group G of affine type thus has a faithful action on $\mathbb{F}_p^n$ by restricting (5.3) to G. This gives a permutation representation of degree $\left|\mathbb{F}_p^n\right| = p^n$ for $\mathrm{AGL}(n,p)$ and its subgroups.

Since $\mathbb{F}_p^n$ acts transitively by addition on itself, any group G of affine type inside $\mathrm{AGL}(n,p)$ also acts transitively on $\mathbb{F}_p^n$, since $\mathbb{F}_p^n$ is a subgroup of G. This will be proved to be the earns and socle of G and is the object that needs to be computed. However it is unfortunately nontrivial to calculate efficiently. On the other hand, the matrix factor is also clearly a subgroup, but is significantly easier to compute.

Proposition 5.4. *If $G = \mathbb{F}_p^n \rtimes M \leq \mathrm{AGL}(n,p)$, then $M \cong G_\alpha$ for any $\alpha \in \mathbb{F}_p^n$.*

Proof. G is transitive, so we can assume $\alpha = 0$. If $(v,A) \in G_0$, we must have $0 = 0^{(v,A)} = A^{-1}(0+v) = A^{-1}v$ and so $v = 0$. There is no restriction on A, so $G_0 = \{0\} \rtimes M \cong M$. □

5.1. Primitive groups of affine type

It is productive to study the primitive groups of affine types, since we have the restriction to primitive groups for the base case of computing the socle, which is when these considerations are most relevant. In this section, the group G is primitive and of affine type, unless otherwise stated.

Definition 5.5. *If V is a vector space over a field k, a matrix group $M \leq \mathrm{GL}(V)$ is* irreducible *if the only M-invariant subspaces of V are $\{0\}$ and V.*

Equivalently, M is called irreducible if V is an irreducible kM-module.

This concept provides an accurate characterisation of groups of affine type, since invariant subspaces corresponds to blocks.

Proposition 5.6. *A group of affine type $G = \mathbb{F}_p^n \rtimes M \leq \mathrm{AGL}(n,p)$ is primitive in its action on $\mathbb{F}_p^n$ if and only if $M \leq \mathrm{GL}(n,p)$ is irreducible.*

Proof. Suppose M is irreducible. Take a block B containing 0; if this is the unique element then B is a trivial block, otherwise, find $v \neq 0 \in B$. M is irreducible, so Mv is a generating set of $\mathbb{F}_p^n$, furthermore, $M0 = 0 \in B$, so $Mv \subseteq B$. Now, if $w \in B$, then $0^w = 0 + w = w \in B$ and so $w^w = w + w \in B$ implying $mw \in B$ for all $m \in \mathbb{F}_p$. This shows that B can only be a trivial block, since any such B with $|B| > 1$ is the entirety of $\mathbb{F}_p^n$.

Conversely, suppose M is reducible, find a nontrivial M invariant subspace $V \subset \mathbb{F}_p^n$. We claim this a nontrivial block for $G^{\mathbb{F}_p^n}$. Take $g = (v,A) \in G$, and let $W = V^{(v,A)}$. By the M-invariance of V, we have

$$W = A^{-1}(V+v) = V + A^{-1}v.$$

If we can find $w \in W \cap V$, then there is some $v' \in V$ such that $w = v' + A^{-1}v$, and hence $A^{-1}v \in V$ and so $W = V$. Our choice g was arbitrary, so either $V^g = V$ or $V^g \cap V = \emptyset$, and hence V is a block. □

We now wish to get a handle on the structure of the subgroups of G, in particular, of its normal subgroups. G is primitive so the normal subgroups must be transitive by Corollary 1.22. Hence, any regular normal subgroup of G is in fact

a minimal normal subgroup by Proposition 1.13, which motivates the following proposition.

Proposition 5.7. *If $G \leq \mathrm{AGL}(n,p)$ is primitive of affine type, then $V = \mathbb{F}_p^n \cong \mathbb{F}_p^n \rtimes \{I_n\} < G$ is normal, transitive and regular.*

Proof. Take $(v,I_n) \in V$, given an arbitrary element $g = (w,A) \in G$,

$$g^{-1}(v,I_n)g = (-A^{-1}w,A^{-1})(v,I_n)(w,A) = (A^{-1}(-w+v+w),I_n)$$

In particular, this lies in $\mathbb{F}_p^n$. Hence $\mathbb{F}_p^n$ is a normal subgroup of G, and is thus transitive.

The groups G and V act on $\Omega = \mathbb{F}_p^n$ and we have $|V| = |\Omega|$. By the Orbit-Stabiliser theorem, $|V| = \left|\omega^V\right| |V_\omega|$, but $\omega^V = \Omega$, so $\left|\omega^V\right| = |V|$ and thus $|V_\omega| = 1$. □

By the discussion above, it is easy to see the following corollary.

Corollary 5.8. *$\mathbb{F}_p^n \trianglelefteq G$ is a minimal normal subgroup.*

There is one additional useful piece in the puzzle of groups of affine type: what do any other minimal normal subgroups look like? It turns out there are no others.

Take $h = (w,B) \in C_G(\mathbb{F}_p^n)$, by definition, we have

$$(0,I) = [g,h] = (-v,I)(-B^{-1}w,B^{-1})(v,I)(w,B) = (-v+B^{-1}v,I)$$

for all $g = (v,I) \in \mathbb{F}_p^n \leq G$. That is, we must have the linear transformation B satisfy $Bv = v$ for all $v \in \mathbb{F}_p^n$ and hence B can only be the identity. Therefore, $C_G(\mathbb{F}_p^n) = \mathbb{F}_p^n$. Proposition 3.2 implies that $[\mathbb{F}_p^n, M] = 1$ for any minimal normal subgroup $M \neq \mathbb{F}_p^n$, showing that $M \leq C_G(\mathbb{F}_p^n) = \mathbb{F}_p^n$. This contradicts $M \neq \mathbb{F}_p^n$, and so we have the following result.

Corollary 5.9. *$\mathbb{F}_p^n \trianglelefteq G$ is the unique minimal normal subgroup.*

Computationally, this is a valuable property as the problem of finding the unique minimal normal subgroup (and thus the socle) becomes a matter of finding a single element of $\mathbb{F}_p^n$ inside G and computing its normal closure.

There is another form of uniqueness that is again highly valuable computationally, especially in the light of the structure we know about primitive groups. In particular, primitive groups of affine type completely describe all possibilities for case I of the O'Nan–Scott theorem:

Theorem 5.10. *Let G^Ω be primitive, G has an earns N if and only if it is of affine type, that is, if and only if $G \leq \mathrm{AGL}(n,p)$ for some n, p.*

Proof. We've seen above that groups of affine type have an earns, so it just remains to prove the converse.

Assume N is an earns of G, N acts regularly, so $G_\alpha \cap N = N_\alpha = 1$. Furthermore, $G_\alpha \leq G$ so G_α has a natural action on N by conjugation. If $g \in G_\alpha$ is in the

kernel of the action, then $h = h^g = g^{-1}hg$ for all $h \in N$ and vice versa, that is, the kernel is of the action G_α^N is $C_{G_\alpha}(N)$.

This condition is equivalent to $hgh^{-1} = g$, and so we must have $\alpha = \alpha^g = \alpha^{hgh^{-1}}$. Suppose g is not the identity, then there is some β such that $\beta^g = \gamma \neq \beta$. N is transitive on Ω so we can choose h such that $\alpha^h = \beta$, and hence we must have $\alpha = \beta^{gh^{-1}} = \gamma^{h^{-1}}$, which is a contradiction, since it implies $\alpha^h = \beta = \gamma$. Hence, the kernel $C_{G_\alpha}(N) = 1$ and thus the action of G_α on N is faithful.

G is primitive, so, by Corollary 1.20, G_α is maximal, meaning there can be no nontrivial G_α-invariant subgroup of N: suppose there is such a subgroup, that is, $M < N$ such that $M \neq 1$ and $g^{-1}Mg = M$ for all $g \in G_\alpha$; we have $M \cap G_\alpha \subseteq N \cap G_\alpha = 1$, and so

$$G_\alpha < \langle M, G_\alpha \rangle = MG_\alpha < NG_\alpha = G,$$

contradicting the maximality of G_α.

By assumption, we can identify N as a vector space, specifically, $N = \mathbb{F}_p^n$ for some p and n, and the action of G_α on N is precisely that of invertible linear transformations: if $v, w \in N$, then $(v+w)^g = v^g + w^g$ and hence $(kv)^g = (v + \ldots + v)^g = v^g + \ldots + v^g = kv$ for $k \in \mathbb{F}_p$. Therefore, G_α can be identified with some subgroup of $\mathrm{GL}(n,p)$ and so $G = \mathbb{F}_p^n \rtimes G_\alpha$, that is, it is of affine type. □

Corollary 5.11. *If primitive group G^Ω has an earns N, then* $\operatorname{soc} G = N$. *If* $\operatorname{soc} G$ *is elementary abelian, then it is an earns of G.*

Proof. Suppose G^Ω has an earns N; G is of affine type by the previous theorem and so $N \cong \mathbb{F}_p^n$ for some n, p is the unique minimal normal subgroup, by Corollary 5.9. Hence $\operatorname{soc} G = N$.

Conversely, $\operatorname{soc} G$ is always normal in G, and it is abelian so must also be regular and hence $\operatorname{soc} G$ is an earns of G. □

The converse statement in the corollary mainly serves to make it clear that the relationship between primitive groups, groups of affine type and the existence of elementary abelian normal subgroups is one of necessity and sufficiency. In any case, this corollary shows that primitive groups of affine type completely classify the possibilities for case I of the O'Nan–Scott theorem.

5.2. Computing the earns

We have considered the direct properties of groups of affine type, and now turn to the question of identifying them. That is, given a primitive permutation group G, is it possible to identify if it is a group of affine type? And, if so, is it possible to find the base vector space (the elementary abelian regular normal subgroup $\mathbb{F}_p^n$)?

Answering the second question answers the first, due to Theorem 5.10, so nothing is lost by just trying to answer that that directly, returning a negative if this turns out to be impossible.

One approach would be to just search for the earns directly, using the fact that it is the unique minimal normal subgroup. That is to say, a possible algorithm would be simply the following.

procedure SLOWEARNS(G, Ω)
  for $z \in G$ **do**
    if $\langle z^G \rangle^\Omega$ is regular and Abelian **then return** $\langle z^G \rangle$
  return false

Of course, a direct naive search through *all* group elements (as will happen in SLOWEARNS if G is not of affine type) is neither feasible nor sensible. For example, consider $G = A_{20} \wr C_2$; this is primitive, not of affine type and has degree $|\Omega| = 400$ under the product action, but has order $|G| = 2 \cdot (20!/2)^2 \approx 3 \cdot 10^{36}$, and iterating over this many elements just to return **false** is unreasonable.

On the other hand, a loop like the one in SLOWEARNS can be reasonable if the iteration is over a small subgroup (or even just subset) of G that is guaranteed to include at least one element in the earns. There are some easy ways to eliminate possibilities, short-circuit and otherwise reduce work:

- recall Proposition 1.13: a set Ω can only admit a regular permutation representation of a group H if $|H| = |\Omega|$. Thus, we can discard G^Ω for which Ω is not a prime power, as the regular group H we desire is elementary abelian.
- if we have G^Ω with $|\Omega|$ a prime power, then $G_\alpha = 1$ implies that G itself is regular and hence must be elementary abelian, and thus G is the earns we are seeking.
- the earns is (by definition) elementary abelian, so every non-identity element has order p, hence we only need to search elements that have this order.
- if G is of affine type, then, for α, G is a split extension of the earns H and G_α that is, $G = HG_\alpha$, in particular, $H \cap G_\alpha = 1$, so we do not need to search elements lying in a stabiliser (that is, if $\mathrm{Fix}(z) \neq \emptyset$ we can omit it from the search).

The last point is not directly useful in practice, but does hint at one fruitful approach: construct subgroups of G with known relationships to the earns.

The EARNS algorithm [Neu87] uses the properties of groups of affine type to check for the existence of an elementary abelian regular normal subgroup and compute it if it exists. The algorithm is detailed in Algorithm 3. The procedure takes an arbitrary primitive group G^Ω and returns the elementary abelian regular normal subgroup of G if it exists, or **false** if G is not of affine type. It is assumed that a BSGS for G^Ω is known, so that, for example, the stabiliser calculations are efficient.

The loop on line (35) is essentially SLOWEARNS. If G is of affine type, this will find an element $z \in \mathbb{F}_p^n$, the rest of the function is just cutting down on how much work is required there, or avoiding it entirely. The important difference of this loop to SLOWEARNS that makes EARNS feasible is that the search space

Algorithm 3 The EARNS algorithm of [Neu87]. G^{Ω} is a primitive permutation group.

procedure EARNS(G, Ω)
  if $|\Omega|$ is not a prime power **then return false**
  Write $|\Omega| = p^n$.
  if $|G| \nmid |\mathrm{AGL}(n,p)|$ **then return false**
  if $G_\alpha = 1$ **then**
    return G
  else if $G_{\alpha,\beta} = 1$ for all $\beta \in \Omega \setminus \{\alpha\}$ **then** ▷ *G is a Frobenius group*
    Find $a \in Z(G_\alpha)$ with $a \neq 1$
    Find $b \in G \setminus G_\alpha$
    return $\langle [a,b]^G \rangle$

  Choose $\beta \in \Omega \setminus \alpha$ such that $G_{\alpha,\beta} \neq 1$
  Set $\Gamma \leftarrow \mathrm{Fix}_\Omega(G_{\alpha,\beta})$
  if $|\Gamma|$ is not a power of p **then return false**

  Set $C \leftarrow C_G(G_{\alpha,\beta})$
  Let $f : C \to C^\Gamma$ be the natural homomorphism.
  Set $P \leftarrow O_p(C^\Gamma)$
  if P^Γ is intransitive **then return false**

  Set $Q \leftarrow$ the Sylow p-subgroup of $Z(G_{\alpha,\beta})$
  Set $R \leftarrow$ the Sylow p-subgroup of $f^{-1}(Z(P))$
  if $Q = 1$ **then**
    Find $r \in R$ with $r \neq 1$
    if $\langle r^G \rangle^\Omega$ is regular **then return** $\langle r^G \rangle$
    else return false

  if $R \not\leq Z(C)$ **then**
    Find $r \in R$, $c \in C$ such that $z \leftarrow [r,c] \neq 1$
    if $\langle z^G \rangle^\Omega$ is regular **then return** $\langle z^G \rangle$
    else return false

  if $|Q| > p^{d-1}$ **then return false**
  Set $Q_0 \leftarrow \Omega_1(Q)$, $R_0 = \Omega_1(R)$ and choose $y \in R_0 \setminus Q_0$
  for $z \in yQ_0$ **do**
    if $\langle z^G \rangle^\Omega$ is regular **then return** $\langle z^G \rangle$
  return false

yQ_0 is significantly smaller than the whole group G.

More concretely, if $G \leq \mathrm{AGL}(n,p)$, then G has size at least p^n, and can be as as large as $|AGL(n,p)| = p^n(p^n-1)\cdots(p^n-p^{n-1})$; on the other hand, we know that Q can be at most p^{n-1} for a group of affine type and the search is over Q_0, which can be smaller still.

In performance terms, the branches on lines (23) and (28) are optional, but they save that potentially expensive loop. In general, calculating the centraliser of a non-normal subgroup like $G_{\alpha,\beta}$ is slow and requires a backtrack search, however, the extra structure of having a two-point stabiliser $G_{\alpha,\beta}$ means this is achievable in polynomial time, although it is still a nontrivial computation.

To complete the description of the algorithm we need to define all the terms used; in particular the p-core $O_p(\,\cdot\,)$, and the subgroup $\Omega_1(\,\cdot\,)$.

Definition 5.12 (p-core)**.** *Let G be a group, the* p-core*, written $O_p(G)$, is the largest normal p-subgroup inside G.*

This is unique and contains all normal p-subgroups of G: if there was a p-subgroup $N \trianglelefteq G$ such that $N \not\leq O_p(N)$, the subgroup $\langle N, O_p(G)\rangle$ is normal in G and is a p-subgroup, contradicting maximality of $O_p(N)$.

Definition 5.13 (Omega subgroup)**.** *If G is a p-group, the* Omega subgroups *are*

$$\Omega_j(G) = \left\langle g \in G \,\middle|\, g^{p^j} = 1 \right\rangle,$$

for $j \geq 1$.

EARNS only requires $\Omega_j(G)$ for $j = 1$, which is always nontrivial, by Sylow's theorem. For abelian G, $\Omega_j(G) = \{g \in G \,|\, g^{p^j} = 1\}$, that is, the elements with order that divides p^j are closed under the group operation.

5.2.1. Correctness of EARNS

An incorrect algorithm is not useful, so we must ensure that EARNS actually does what we have asserted without proof. In the following let G^Ω be primitive, and let V refer to the underlying vector space that is the earns, if it exists.

We focus on the properties that G, V and Ω must have if G is of affine type, particularly the properties that arise from the linear-algebra grounding of affine groups. If any of these properties are violated, it is immediately known that G is not of affine type and so EARNS can stop all work and inform the caller. In this setting, we will refer to some elements of G as linear transformations, and some as vectors, and regard the G-set Ω as a vector space, isomorphic to V.

5.2.1.1. Line (2). As discussed previously, if G is to have an earns, we must have $|\Omega| = p^n$ for some prime p, or else there is no way that an elementary abelian group can be regular by Proposition 1.13. Hence, the check and short-circuit on line (2) is valid, and then we can assume $\Omega = \mathbb{F}_p^n$, as sets.

5.2.1.2. Line (4). If G is to have an earns, then it must be of affine type, that is, a subgroup of $\mathrm{AGL}(n,p)$ by Theorem 5.10; hence, G cannot have an earns if the order of G does not divide $|\mathrm{AGL}(n,p)| = p^n(p^n-1)\cdots(p^n-p^{n-1})$, as tested on line (4).

5.2.1.3. Lines (5-6): G regular. Regularity and primitivity imply that $G = C_p$ and hence the earns of G is exactly G. When examining G_α, G is transitive, so the choice of $\alpha \in \Omega$ is irrelevant. This choice is identifying $\alpha = 0 \in \mathbb{F}_p^n$ and G_α with the group of matrices in the semidirect product that makes up G, if it is of affine type.

5.2.1.4. Lines (7-10): G Frobenius. If the check on line (7) succeeds, we have $G_\alpha \neq 1$ and $G_{\alpha,\beta} = 1$. Note, there is no guarantee that G_α is transitive on $\Omega \setminus \{\alpha\}$ meaning there can be more than one β to check: a representative from each orbit from each orbit of G_α.

In this case, G has very restricted structure, which guarantees that it has an earns, and makes the computation of its earns straightforward.

Definition 5.14. *A transitive group G^Ω is a* Frobenius group *if $G_\alpha \neq 1$ and $G_{\alpha,\beta} = 1$ for all $\alpha, \beta \in \Omega$.*

Detailed information is known about the structure of Frobenius groups, some of which are summarised in the following theorem. Proofs of the parts can be found in Sections 8, 17 and 18 of [Pas68].

Theorem 5.15. *If G is a Frobenius group, we can write $G = KG_\alpha$, where*

- *$K \trianglelefteq G$,*
- *G_α and G_α^g are either identical or intersect trivially.*
- *$K \cap G_\alpha = 1$, in fact, a theorem due to Frobenius gives $K = \{1\} \cup (G \setminus \bigcup_{g \in G} G_\alpha^g)$,*
- *$N_G(G_\alpha) = G_\alpha$,*

K is known as the Frobenius kernel *of G and G_α a* Frobenius complement.

Its trivial intersection with a point stabiliser of G implies that $K_\alpha = 1$ so K is regular, and is hence a minimal normal subgroup of G by Corollary 1.23.

Definition 5.16. *A finite group G is* nilpotent *if the lower central series*

$$G = G_0 \trianglerighteq [G, G_0] = G_1 \trianglerighteq [G, G_1] = G_2 \trianglerighteq \dots,$$

reaches the trivial group.

Recall our discussion of the derived series and solvable residuals in Definition 4.2 and Proposition 4.3. In particular the derived series of a group G is

$$G = G^{(0)} \trianglerighteq [G^{(0)}, G^{(0)}] = G^{(1)} \trianglerighteq [G^{(1)}, G^{(1)}] = G^{(2)} \trianglerighteq \dots$$

and hence the two series are very similar, with $G^{(i)} \leq G_i$, since the former is the latter after replacing the G in the commutator with a subgroup of G. This gives us the following easy result.

Proposition 5.17. *If a group G is nilpotent, then it is solvable.*

Proof. We have $G_i = 1$ for some finite i, and $G^{(i)} \leq G_i$, hence G is solvable, for example, by Proposition 4.3. □

For Frobenius groups specifically, the following theorem of Thompson is useful. See, for example, [Pas68, Theorem 17.4] for a proof.

Theorem 5.18. *The Frobenius kernel K is nilpotent.*

Corollary 5.19. *Let G^Ω is a primitive Frobenius group, G falls into case I of the O'Nan–Scott theorem, and* $\operatorname{soc} G = K$ *where K is the Frobenius kernel of G.*

Proof. It was proved above that the kernel K is a (minimal) normal subgroup of G, and by the previous proposition and theorem, K is solvable. In particular, K does not contain any nonabelian simple groups and so the only possibility is for G to lie in case I. The unique minimal normal subgroup K must be the socle. □

In summary, a primitive Frobenius group must be a group of affine type, and its Frobenius kernel is guaranteed to be the earns, that is, the underlying vector space when considered as a subgroup of an affine group. Thus, computing the earns can be rephrased as a matter of finding an element of the Frobenius kernel, which is exactly what this subsection of EARNS does. We embark on justifying the algorithm used for this task.

Lemma 5.20. *Let G^Ω be a Frobenius group and $\alpha \in \Omega$, then $Z(G_\alpha) \neq 1$.*

Proof. We consider two cases separately, splitting on the parity of the order of G_α.

If $|G_\alpha|$ is even, then there is a unique element z of order 2 by [Pas68, Theorem 18.1] and so $z \in Z(G_\alpha)$, since $\left|g^{-1}zg\right| = |z| = 2$ and therefore $g^{-1}zg = z$ for any $g \in G_\alpha$.

If $|G_\alpha|$ is odd, then, by Zassenhaus, every element of order p is central, where p is any prime divisor of $|G_\alpha : G'_\alpha|$. We are guaranteed that G_α is not perfect by the Feit-Thompson theorem [FT63]: all finite groups of odd order are solvable. This shows $G'_\alpha < G_\alpha$ and so such a p exists. Hence $Z(G_\alpha) \neq 1$ since $p \mid G_\alpha$ and the Sylow theorems guarantee the existence of elements with such p as their order. □

Lemma 5.21. *Let G^Ω be a Frobenius group with Frobenius kernel K and $\alpha \in \Omega$, choose $a \in Z(G_\alpha)$, $b \in G \setminus G_\alpha$ such that $a \neq 1$, then $[a,b] \in K$ and $[a,b] \neq 1$.*

Proof. By Proposition 5.15, we can write $b = kg$ for some $k \in K$ and $g \in G_\alpha$, with $k \neq 1$, since $b \notin G_\alpha$. Hence, since a is central in G_α, we have

$$[a,b] = a^{-1}g^{-1}k^{-1}akg = g^{-1}a^{-1}k^{-1}akg.$$

The kernel K is normal in G, so $k' := a^{-1}k^{-1}a \in K$, and thus $[a,b] = g^{-1}k'kg \in K$, again by normality.

The identity is in a conjugacy class of its own, so to see $[a,b] \neq 1$ we just need to see $k'k \neq 1$ which is equivalent to $a^{-1}k^{-1}a \neq k^{-1}$ which is equivalent to $ak \neq ka$. As stated above $k \neq 1$ so the regularity of K implies $\beta = \alpha^k \neq \alpha$ and hence $\beta^a \neq \beta$ since $G_{\alpha,\beta} = 1$ and $a \neq 1$, thus

$$\alpha^{ak} = \alpha^k = \beta \neq \beta^a = \alpha^{ka},$$

therefore, $ak \neq ka$ as required. □

Thus, we've shown that a is guaranteed to exist, and that $[a,b]$ is a nontrivial element of the minimal normal subgroup that is the earns of G, hence the normal closure on line (10) computes this earns, as desired.

5.2.1.5. Line (14). If G is neither regular nor Frobenius, we can find $\beta \neq \alpha$ such that $G_{\alpha,\beta} \neq 1$.

Lemma 5.22. *If G^Ω is of affine type and $G_{\alpha,\beta} \neq 1$, $|\Gamma| = \left|\mathrm{Fix}_\Omega(G_{\alpha,\beta})\right| = p^m$ for some integer $m \geq 1$.*

Proof. By identifying $\alpha = 0$ and β as a vector, the subgroup $G_{\alpha,\beta}$ is the set $G \cap \mathrm{GL}(n,p)$ of linear transformations of $\mathbb{F}_p^n$ that have β in their 1-eigenspace, and $\Gamma := \mathrm{Fix}_\Omega(G_{\alpha,\beta})$ is the intersection of the 1-eigenspaces of the elements of $G_{\alpha,\beta}$; this certainly contains α and β, and indeed the whole subspace spanned by β. In fact, as the intersection of subspaces, Γ is a subspace of $\Omega = \mathbb{F}_p^n$, and hence $|\Gamma| = p^m$ for some integer $m \leq n$.

$\alpha \neq \beta \in \Gamma$, so $|\Gamma| \neq 1$ and hence $m \geq 1$. □

We immediately deduce that if $|\Gamma| \neq p^m$ for any m then G cannot be of affine type and so can exit immediately, as performed by line (14).

5.2.1.6. Line (19). The subspace $\Gamma \subseteq \mathbb{F}_p^n$, can be identified with a subgroup of $V \leq G$, via the natural embedding $\gamma \mapsto (\gamma, I)$.

Lemma 5.23. *$\Gamma \leq C$, specifically, $\Gamma = V \cap C \trianglelefteq C$.*

Proof. $G_{\alpha,\beta}$ consists of elements of the form $(0,A)$, with $A\gamma = \gamma$ for each $\gamma \in \Gamma$, so

$$(0,A)(\gamma,I) = (A\gamma,A) = (\gamma,A) = (\gamma,I)(0,A). \tag{5.24}$$

and thus $\Gamma \leq C$ and hence $\Gamma \leq V \cap C$.

Conversely, if $x = (v,I) \in V \cap C$ then (5.24) must be satisfied, that is, $Av = v$ for all $A \in G_{\alpha,\beta}$, hence $v \in \Gamma$ and thus $V \cap C \subseteq \Gamma$. The normality follows directly from $V \trianglelefteq G$. □

The group C restricts to C^Γ naturally; call this associated map f. Denote $f(H) = H^\Gamma$ for $H \leq C$. The algorithm handles preimages under f in several places, so the following result is salient.

Lemma 5.25. $\ker f = Z(G_{\alpha,\beta}) = C_{\alpha,\beta} = C \cap G_{\alpha,\beta} \leq Z(C)$.

Proof. C is the centraliser of $G_{\alpha,\beta}$, so $[G_{\alpha,\beta},C]=1$, and hence $G_{\alpha,\beta}\leq C_G(C)$. Thus

$$Z(G_{\alpha,\beta})=G_{\alpha,\beta}\cap C\leq C_G(C)\cap C=Z(C)$$

An element is in $\ker f$ if and only if it fixes all of Γ, the set $G_{\alpha,\beta}$ is the set of all such elements in G, and so those that lie in C are exactly $C\cap G_{\alpha,\beta}$ and so this subgroup is precisely $\ker f$. □

We now return to the consideration of the subspace Γ itself.

Lemma 5.26. *$\Gamma^\Gamma\leq P=O_p(C^\Gamma)$ if G is of affine type.*

Proof. Γ is a p-group by Lemma 5.22. The normality of Γ in C implies the normality of the image: $\Gamma^\Gamma\trianglelefteq C^\Gamma$.

Recall the subgroup $P=O_p(C^\Gamma)$ is the largest normal p-subgroup of C^Γ, and this is unique, meaning it contains all other normal p-groups, proving $\Gamma^\Gamma\leq O_p(C^\Gamma)$. □

It is clear that $V\cap\ker f\subseteq V\cap G_\alpha=1$, and hence $\Gamma^\Gamma\cong\Gamma^\Omega$. The subgroup Γ is transitive on itself, since $0^\gamma=\gamma$ for any $\gamma\in\Gamma$. It is contained within P and so P must also be transitive on Γ. Therefore, the test on line (19) is guaranteed to be true only if G is not of affine type.

There remains the question of actually computing $P=O_p(C^\Gamma)$. [Neu87] also introduced an algorithm for computing the p-core when describing EARNS, and [Ung06] gives an improved algorithm for this task; the latter is the state-of-the-art version implemented in MAGMA. Both of these algorithms require computing the earns of (subgroups of) the input and hence there is mutual recursion between them and EARNS. Fortunately, C^Γ is small, in particular, it is smaller than G, and so the recursion always makes progress and is permissible.

The assertion $\left|C^\Gamma\right|<|G|$ requires proof. By way of contradiction, assume this is not true; $C\leq G$ along with the equality of order implies $C=G$, in other words, every element of G commutes with $G_{\alpha,\beta}$. That is, for each $(v,A)\in G$ and $(0,B)\in G_{\alpha,\beta}$,

$$(v,A)(0,B)=(v,AB)=(Bv,BA)=(0,B)(v,A),$$

showing that the entirety of V lies in the 1-eigenspace of each linear transformation in $G_{\alpha,\beta}$. There is exactly one linear transformation of V for which this is possible, the identity, so $G_{\alpha,\beta}=1$. This case was detected and eliminated earlier, and hence this reaches a contradiction, implying $\left|C^\Gamma\right|<G$.

5.2.1.7. Lines (21-22). The choice of Q and R may seem a little arbitrary, but they have useful relationships to the earns V, if it exists, as the last of the following lemmas demonstrate.

Lemma 5.27. *If G is a finite nilpotent group and $H<G$, then $H<N_G(H)$, that is, the usual normaliser containment is strict.*

Proof. G is nilpotent, so the lower central series

$$G = G_0 \trianglerighteq [G,G_0] = G_1 \trianglerighteq [G,G_1] = G_2 \trianglerighteq \dots$$

terminates in 1. In particular, there is a first G_i such that $G_i \leq H$, and $i \geq 1$, since H is a proper subgroup of G. The previous group in the chain G_{i-1} exists, includes elements outside H, and satisfies $[H,G_{i-1}] \leq [G,G_{i-1}] = G_i \leq H$, so $G_{i-1} \leq N_G(H)$ and hence the result follows. □

Lemma 5.28. *Let G be a finite group with Sylow p-subgroup P, then $M := N_G(N_G(P)) = N_G(P) =: N$.*

Proof. A normal Sylow p-subgroup is unique, and P is a normal in $N_G(P)$ by definition, so $N_G(P)$ contains exactly one Sylow p-subgroup of G, namely G. Thus, if $g \in M$ then $N^g = N$ and so $P^g = P$ hence $g \in N$. We always automatically have that $M \geq N$ so the result follows. □

Corollary 5.29. *A Sylow p-subgroup P of a nilpotent group G is unique.*

Proof. By the first lemma, if $N_G(P) < G$ then $N_G(N_G(P)) > N_G(P)$, but the second lemma requires that $N_G(N_G(P)) = N_G(P)$ and hence $N_G(P) = G$, that is, $P \trianglelefteq G$ and so is unique. □

We now can return to the specific subgroups in which we are interested for EARNS.

Lemma 5.30. *The Sylow p-subgroups Q and R of $Z(G_{\alpha,\beta})$ and $f^{-1}(Z(P))$ respectively are unique.*

Proof. $Z(G_{\alpha,\beta})$ is abelian, and hence is nilpotent, so Corollary 5.29 applies to prove the result for Q.

Denote $H = f^{-1}(Z(P))$, then

$$f(H') = f([H,H]) = [f(H),f(H)] = [Z(P),Z(P)] = 1,$$

and so $H' \leq \ker f = Z(G_{\alpha,\beta})$, therefore the second term of the lower central series is $[H,H'] = [H,Z(G_{\alpha,\beta})]$. By definition, H is inside the domain C of f, and hence $[H,Z(G_{\alpha,\beta})] \leq [C,G_{\alpha,\beta}]$ and this is trivial by definition. Thus, H is nilpotent and the same corollary used for Q gives the result for R. □

This lemma justifies speaking about *the* Sylow p-subgroup, rather than a Sylow p-subgroup, and it also demonstrates that we do not have to consider any sort of algorithmic choice. With the background of the previous two lemmas, we can now tackle the following result of Neumann for which we were aiming.

Lemma 5.31 ([Neu87, Lemma 3.3])**.** *If Q and R are the Sylow subgroups chosen above, then*

(a) $Q \leq R$.
(b) $R \leq \Gamma \times Q$,
(c) $R \cap \Gamma \neq 1$,
(d) $[R,C] \leq \Gamma$.

Proof. Lemma 5.25 gave us $\ker f = Z(G_{\alpha,\beta})$ so $f(Z(G_{\alpha,\beta})) = 1 \leq Z(P)$, hence $Z(G_{\alpha,\beta}) \leq f^{-1}(Z(P))$. Any p-subgroup of $Z(G_{\alpha,\beta})$ is certainly a p-subgroup of the right-hand side and the largest p-subgroup R of the right-hand side is unique, so $Q \leq R$ which is (a).

Lemma 5.26 showed $\Gamma^\Gamma \leq P$ and it is clear that it is regular. The latter point means $C_{\mathrm{Sym}(\Gamma)}(\Gamma) = \Gamma$ by [DM96, Theorem 4.2A] and so

$$Z(P) = P \cap C_{C^\Gamma}(P) \leq P \cap C_{\mathrm{Sym}(\Gamma)}(\Gamma) = \Gamma.$$

Taking the preimage gives $f^{-1}(Z(P)) \leq f^{-1}(\Gamma^\Gamma) = \langle \Gamma, \ker f \rangle$. It was proved above that $\ker f = Z(G_{\alpha,\beta}) \leq G_{\alpha,\beta}$, so $\ker f \cap \Gamma = 1$, leaving us with

$$f^{-1}(Z(P)) \leq \Gamma \times Z(G_{\alpha,\beta}).$$

The Sylow p-group of the right-hand side is $\Gamma \times Q$, since Γ is a p-group, and the Sylow p-group R of the left-hand side will be inside this. This proves (b).

We can write $R = R \cap (\Gamma \times Q) = (R \cap \Gamma) \times Q$, since $R \cap Q = Q$. By definition, $Q \leq \ker f$, so

$$f(R) = f(R \cap \Gamma) = Z(P) \cap \Gamma^\Gamma.$$

The p-core P is a p-group by definition, so the intersection of the nontrivial normal subgroup Γ^Γ with the centre must be nontrivial. Hence $f(R \cap \Gamma) \neq 1$ and therefore $R \cap \Gamma \neq 1$, completing (c).

Using (b), we have $[R, C] \leq [\Gamma \times Q, C] \leq [\Gamma, C]$, since $Q \leq Z(C)$ by Lemma 5.25. $\Gamma \trianglelefteq C$, so $[\Gamma, C] \leq \Gamma$ and (d) follows. □

As we will see, this lemma justifies the two special cases on lines (23) and (28).

5.2.1.8. Lines (23-26). If $Q = 1$, then the previous lemma implies $R \leq \Gamma$ and $R = R \cap \Gamma \neq 1$, so the normal closure of any non-identity element is the earns we desire. The primitivity of G and size of Ω implies that the regularity of a subgroup $H < G$ guarantees that H is elementary abelian.

5.2.1.9. Lines (28-31). If there is $r \in R$, $c \in C$ such that $z = [r, c] \neq 1$, it must be that $z \in \Gamma$ by Lemma 5.31 (d) and hence the earns of G is the normal closure of z in G. The justification of the regularity check in the previous branch applies here too.

Such r and c exist if and only if $R \not\leq Z(C)$: by construction $R \leq C$ so that dictates if $[R, C] = 1$ or not. Hence the check and implementation are correct.

5.2.1.10. Lines (35-37). This loop is the fallback brute-force search similar to SLOWEARNS. One possible optimisation over that naive search is noticing that every element of V is of order p, meaning $\Gamma \cap R \leq V \cap R \leq \Omega_1(R)$, and hence the computation of R_0 is a valid way to reduce the search space; that is, we could traverse R_0 and still be guaranteed to find the earns. However, we can do even better than that:

Lemma 5.32. *Let yQ be a Q-coset of R such that $yQ \neq Q$, that is, such that $y \notin Q$, then $yQ \cap V = \{\gamma\} \neq \emptyset$ for some $\gamma \in \Gamma$, if G is of affine type.*

Proof. By (b) of Lemma 5.31, $R \leq \Gamma \times Q$, so we can write $y = \gamma q$ for some $\gamma \neq 1 \in \Gamma$ and $q \in Q$, hence $yQ = \gamma Q$ and thus $\gamma \in yQ \cap V$. The expression $y = \gamma q$ is unique, so this γ is the unique element of the intersection. □

Item (c) of that same lemma guarantees that such a Q-coset exists, and, in fact, guarantees that the containment $Q < R$ is strict.

The same restriction of R to R_0 mentioned in the hypothetical procedure at the beginning of this subsection applies here, for the same reasons described there. Of course, in this restricted case, only the cosets of $Q \cap R_0 = Q_0$ matter. This search through a coset is a search through $Q_0 < R_0$ and so certainly involves traversing fewer elements than a search through R_0 itself. As with the two special-case branches, regularity of the normal closure will guarantee that it is an earns and the lemma shows that if there is an earns, we will find it.

Thus, we've proved:

Theorem 5.33. EARNS *is correct: it returns the earns of G if it exists or* **false** *otherwise.*

5.2.2. Examples of EARNS

We will now discuss some examples of groups for the execution of EARNS is illustrative or informative.

Example 5.34 (Necessity of regularity checks)**.** Consider $G = S_8$ acting on $\Omega = \{1,\ldots,8\}$ in the natural way, $|\Gamma| = 8$ and so $p = 2$. This group is definitely not regular or Frobenius, and it is clear that $\Gamma = \mathrm{Fix}(G_{\alpha,\beta}) = \{\alpha,\beta\}$ and so $|\Gamma|$ is a power of p. By symmetry, we can assume $\alpha = 1$ and $\beta = 2$, meaning $G_{\alpha,\beta} = \mathrm{Sym}(\{3,\ldots,8\})$. It's not hard to see that $C = C_G(G_{\alpha,\beta}) = \{1,(12)\} = \mathrm{Sym}(\{1,2\})$: any element that acts nontrivially on an element $\gamma \in \{3,\ldots,8\}$ will not commute with at least one element of $G_{\alpha,\beta}$ that also moves γ. Thus $C^\Gamma = C$ and $O_p(C^\Gamma) = C$, C is transitive on $\{1,2\}$ so we fall through to computing Q and R. We have $Z(G_{\alpha,\beta}) = G_{\alpha,\beta} \cap C = 1$ and $f^{-1}(Z(P)) = C$, so $Q = 1$ and $R = C$. Thus we enter the branch on line (23), and have a single choice $r = (12)$. r is not contained in the unique normal subgroup $A_8 \trianglelefteq S_8$ so $M = \langle r^G \rangle = S_8$ which is not regular on Ω. That said, the precise group of M does not matter, since neither of the only two normal subgroups A_8 or S_8 are regular.

Hence, the check that $\langle z^G \rangle$ on line (26) is necessary, or else EARNS would return something other than **false** for a group that is not of affine type.

Example 5.35 (Large number of loop iterations)**.** The group of affine type $G = \mathbb{F}_{2^k}^2 \rtimes \mathrm{SL}(2,2^k) \leq \mathrm{AGL}(2,2^k)$ with $\Omega = \mathbb{F}_{2^k}^2$ is an example due to Unger that displays particularly bad behaviour. It executes the loop on line (35) with $|Q_0| = 2^k$, that is, the search is, on average, $O(\sqrt{n})$ in the degree $n = 2^{2k}$. This group is definitely of affine type so all tests checking this will succeed and hence we omit discussion of them. We choose $\alpha = 0$, so $G_\alpha \cong \mathrm{SL}(2,2^k)$, and $G_{\alpha,\beta}$ is the matrices in $\mathrm{SL}(2,2^k)$ that fix the vector β, which can be chosen to be $\beta = (1,0)$;

$G_\alpha = \mathrm{SL}(2,2^k)$ is transitive so this is done without loss of generality. It is not hard to see that the determinant restriction implied by $\mathrm{SL}(2,2^k)$ means that we have

$$G_{\alpha,\beta} = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \middle| \, b \in \mathbb{F}_{2^k} \right\}. \tag{5.36}$$

Hence, $\Gamma = \mathrm{Fix}_\Omega(G_{\alpha,\beta}) = \{(a,0) \,|\, a \in \mathbb{F}_{2^k}\}$ is one dimensional, with 2^k elements. $G_{\alpha,\beta}$ is clearly abelian. Explicitly listing the elements $(v,A) \in G$ that commute with $(0,B) \in G_{\alpha,\beta}$ shows that $C = C_G(G_{\alpha,\beta}) = \Gamma \times G_{\alpha,\beta}$. Thus, since $C_{\alpha,\beta} = G_{\alpha,\beta}$ is the kernel of the restriction map f, the restriction $C^\Gamma \cong C/G_{\alpha,\beta} \cong \Gamma$ and so $P = O_2(C^\Gamma) = C^\Gamma$ as Γ is a 2-group. This shows that $f^{-1}(P) = C$, which is also a 2-group so the Sylow 2-subgroup R is exactly C. For the subgroup Q, $G_{\alpha,\beta}$ is abelian, so the centre is itself, and it is a 2-group, so $Q = G_{\alpha,\beta} \neq 1$.

The above demonstrates that G does not fall into the branch $Q = 1$ covered by line (23), and $R = C = Z(C)$ since C is abelian, so G also does not fall into the branch on line (28), resulting in the loop being taken. The explicit form in (5.36) allows one to easily see that every element of $Q = G_{\alpha,\beta}$ has order 2, implying $Q_0 = G_{\alpha,\beta}$ and hence $|Q_0| = 2^k$. By Lemma 5.32, there is exactly one element of Q_0 with the required property, so the search will be of length $2^k/2$ on average, which has the asymptotics stated above.

CHAPTER 6

Computing the socle of a general group

Computing the socle of an arbitrary permutation group G might initially look like a difficult task. With no restriction on the structure of the group a naive procedure like that sketched at the start of Chapter 4 might seem like the only possibility. However this is fortunately not the case, it is possible to recursively reduce to primitive subgroups and primitive quotients of G, compute their socles via the PRIMITIVESOCLE algorithm described in Chapter 4 and use these to deduce $\operatorname{soc} G$.

This procedure SOCLE is listed in Algorithm 4 and is mainly due to [CH97] but incorporates corrections and improvements from [Ung]. As with the previous procedures, SOCLE assumes that there is a BSGS known for G^{Ω}.

6.1. SOCLE is correct

As should be the case, we have the following result, for which we reproduce and rephrase the proof given in [CH97] and [Ung].

Theorem 6.1. *Let G^{Ω} be an finite permutation group, then* $\text{SOCLE}(G,\Omega) = \operatorname{soc} G$.

SOCLE groups the set of finite permutation groups into four cases: intransitive, two disjoint class of imprimitive, and primitive. It is clear that these are all disjoint and cover every possibility possibilities for G.

6.1.1. G^{Ω} primitive

We handle the last, and easiest, case first. If SOCLE reaches lines (34-35) then G^{Ω} must be transitive and have no nontrivial minimal block systems, that is, it is primitive, so calling PRIMITIVESOCLE is valid and will return $\operatorname{soc} G$ as desired, by Theorem 4.4.

6.1.2. G^{Ω} intransitive or imprimitive with two minimal block systems

The two cases on lines (2) and (8) are very similar. In either case, we use the intransitivity or imprimitivity to construct quotient groups of G with permutation actions, and then pull back the socle of each of those.

In the intransitive case the H_i act on Δ_i and by construction $|\Delta_i| < |\Omega|$. In the imprimitive case, the H_i act on the block systems Σ_i, and due to nontriviality $|\Sigma_i| < |\Omega|$. Therefore, the recursion of SOCLE is permissible, because the degree of each of the H_i is less than that of G, so the algorithm will terminate.

It just remains to see that the intersection of the inverse images of the $\operatorname{soc} H_i$ gives the desired subgroup of G. These results and proof that follows mirrors that in [CH97, Section 5]. In all of them we denote G^{Ω} a finite permutation group.

Algorithm 4 The SOCLE algorithm of [CH97]. This takes a permutation group G^Ω with $|\Omega| \leq 10^7$ and returns $\operatorname{soc} G$.

procedure SOCLE(G, Ω)
  if G^Ω is intransitive **then**
    Take an nonempty set $\Delta_1 \subset \Omega$ fixed by G (e.g. an orbit).
    Set $\Delta_2 \leftarrow \Omega/\Delta_1$ its complement.
    Let $H_i = G^{\Delta_i}$ with epimorphism $\varphi_i : G \to H_i$.
    return $\varphi_1^{-1}(\operatorname{soc} H_1) \cap \varphi_2^{-1}(\operatorname{soc} H_2)$

  else if G^Ω is imprimitive with minimal block systems Σ_1, Σ_2 **then**
    Let H_i be the action of G on Σ_i, with epimorphism $\varphi_i : G \to H_i$.
    return $\varphi_1^{-1}(\operatorname{soc} H_1) \cap \varphi_2^{-1}(\operatorname{soc} H_2)$

  else if G^Ω is imprimitive with one minimal block system Σ **then**
    Let H be the action of G on Σ, with epimorphism $\varphi : G \to H$
    Set $K \leftarrow \ker \varphi$ and $J \leftarrow \varphi^{-1}(\operatorname{soc} H)$
    if $K = 1$ **then return** J

    Set $L \leftarrow \operatorname{soc} K$, this is a direct power of some simple group.
    Check if $K \neq L$ or $|K| \nmid |\Delta|^d$ for $\Delta \in \Sigma$, d the largest proper divisor of $|\Sigma|$, if so, $\operatorname{soc} G \leq L$.
    if L is nonabelian and it is known $\operatorname{soc} G \leq L$ **then return** L
    Set $C \leftarrow C_G(K)$.
    if L is nonabelian **then return** $\varphi^{-1}(\operatorname{soc} \varphi(C))$.

    if it is known $\operatorname{soc} G \leq L$ **then**
      Set $E \leftarrow L$.
    else
      Set $E \leftarrow \Omega_1(Z(\varphi^{-1}(O_p(\operatorname{soc} H))))$.
    E is elementary abelian p group, regard as G-module over $\mathbb{F}_p$, take $E' \leq G$ generated by the minimal submodules of E (this is the abelian part of $\operatorname{soc} G$).
    Set $M \leftarrow C \cap J$.
    $M/(K \cap M)$ is a direct product of simple groups.
    Let $M_i/(K \cap M)$ be the simple factors and set $M_i' = [M_i, M_i]$.
    Set $M' \leftarrow \langle M_i' \mid M_i' \text{ is simple} \rangle$
    return $E' \times M'$

  else ▷ G^Ω *is primitive*
    return PRIMITIVESOCLE(G, Ω)

The following lemma will eventually be proved, but it will be used to justify SOCLE first.

Lemma 6.2 ([CH97, Lemma 5.6])**.** *Let $\varphi_1 : G \to H_1$, $\varphi_2 : G \to H_2$ be epimorphisms with $K_i := \ker \varphi_i$ such that $K_1 \cap K_2 = 1$ then $\operatorname{soc} G = \varphi_1^{-1}(\operatorname{soc} H_1) \cap \varphi_2^{-1}(\operatorname{soc} H_2)$.*

Given this, it just remains to see that $\ker \varphi_1 \cap \ker \varphi_2 = 1$ to prove the algorithm correct. To prove this, split the consideration of G^Ω into its two natural cases.

When G^Ω is intransitive, $g \in \ker \varphi_1 \cap \ker \varphi_2$ if and only if it fixes all points of the chosen sets Δ_1 and Δ_2, but $\Omega = \Delta_1 \cup \Delta_2$, so $g = 1$, since G is faithful.

The other case is when G^Ω is transitive but has two distinct minimal block systems. Assume $K = \ker \varphi_1 \cap \ker \varphi_2 \neq 1$, this subgroup is $K \trianglelefteq G$ is strictly smaller than either kernel, since neither contains the other, and so the orbits $\{\alpha^K\}$ form a nontrivial block system, that is contained in both Σ_1 and Σ_2, contradicting minimality.

We now embark on a proof of Lemma 6.2.

Lemma 6.3 ([CH97, Lemma 5.2])**.** *If $N \trianglelefteq G$ with $N \leq \operatorname{soc} G$ then $\operatorname{soc} G = N \times M$ for some $M \trianglelefteq G$.*

Proof. Set $N_0 = N$. If there is some minimal normal subgroup $K_1 \trianglelefteq G$ such that $K \not\leq N$, $N \cap K_1 = 1$ and $[N, K_1] = 1$ by Proposition 3.2. Thus, $NK_1 = N \times K_1 \trianglelefteq G$ is contained in $\operatorname{soc} G$. In this case, replace N_0 it by $N_1 = N_0 \times K_1$ and repeat to find $K_2, \ldots, K_k$ and the corresponding $N_2, \ldots, N_k$ until there are no minimal normal subgroups outside N_k. G is finite, so there are finitely many minimal normal subgroups, and hence this iteration will terminate.

If N_k contains all minimal normal subgroups of G, it contains the subgroup generated by them, that is, $\operatorname{soc} G \leq N_k$. At each stage $N_i \leq \operatorname{soc} G$, showing $\operatorname{soc} G = N_k$. Thus, $\operatorname{soc} G = N \times K_1 \times \ldots \times K_k$ and hence $M = K_1 \times \ldots \times K_k$ is the complement of N in $\operatorname{soc} G$. □

Lemma 6.4 ([CH97, Lemma 5.3])**.** *If $N \trianglelefteq G$ and $N \leq \operatorname{soc} G$ then $N = M_1 \times \ldots \times M_n$ for some minimal normal subgroups $M_i \trianglelefteq G$.*

Proof. We can write $\operatorname{soc} G = N \times N^*$ for some $N^* \trianglelefteq G$ by Lemma 6.3. By the construction in the proof of that lemma $N^* = K_1 \times \ldots \times K_k$ for minimal normal subgroups $K_i \trianglelefteq G$. Consider the minimal normal subgroups not inside N^* and let M be the subgroup that they generate. All these minimal normal subgroups must lie in N, and hence $M \leq N$, furthermore, $\operatorname{soc} G = MN^*$ by construction, so $N \cong \operatorname{soc} G / N^* \cong M$, and therefore $N = M$ by the finiteness of G.

Proposition 3.2 (c) shows that $N = M$ is a direct product. □

Lemma 6.5 ([CH97, Lemma 5.4])**.** *Let $\varphi : G \to G/K$ be an epimorphism with $K := \ker \varphi$, then $\varphi(\operatorname{soc} G) \leq \operatorname{soc} \varphi(G)$ and $K \cap \operatorname{soc} G \leq \operatorname{soc} K$.*

Proof. If $N \trianglelefteq G$ is a minimal normal subgroup, then $\varphi(N) = NK/K \cong N/(N \cap K)$ is either trivial, if $N \leq K$, or isomorphic to itself, if $N \cap K = 1$. In either case $\varphi(N) \leq \operatorname{soc} \varphi(G)$ and hence $\varphi(\operatorname{soc} G) \leq \operatorname{soc} \varphi(G)$.

We clearly have $\operatorname{soc} G \cap \operatorname{soc} K \leq \operatorname{soc} G \cap K \leq \operatorname{soc} G$, and all these groups are normal in G. Hence, by Lemma 6.4 they are all generated by minimal normal subgroups of G, and so we can write

$$\operatorname{soc} G \cap K = (\operatorname{soc} G \cap \operatorname{soc} K) \times M$$

for some subgroup $M \trianglelefteq G$ generated by the minimal normal subgroups of G inside $\operatorname{soc} G \cap K$ but not $\operatorname{soc} G \cap \operatorname{soc} K$; more specifically,

$$M \cap (\operatorname{soc} G \cap \operatorname{soc} K) = 1. \tag{6.6}$$

By construction, $M \leq \operatorname{soc} G$ and $M \trianglelefteq K$; the former implies $M \cap \operatorname{soc} G = M$ and the latter shows that M is either trivial or contains a minimal normal subgroup of K. The former deduction and (6.6) together imply that $M \cap \operatorname{soc} K = 1$, and so $M = 1$ by the latter. Putting it all together gives $\operatorname{soc} G \cap K = \operatorname{soc} G \cap \operatorname{soc} K \leq \operatorname{soc} K$. □

Lemma 6.7 ([CH97, Lemma 5.5])**.** *Let $\varphi : G \to G/N$ be an epimorphism, where $N := \ker \varphi$, and $M \trianglelefteq G$ such that $N \cap M = 1$ then $\varphi(M) \leq \operatorname{soc} \varphi(G)$ implies $M \leq \operatorname{soc} G$.*

Proof. Suppose $\varphi(M) \leq \operatorname{soc} \varphi(G)$. The image $\varphi(M) = MN/N \trianglelefteq \varphi(G) = G/N$ so MN/N is generated by minimal normal subgroups of G/N by Lemma 6.4. By the second isomorphism theorem for groups, $MN/N \cong M/(M \cap N)$ and this isomorphism induces a bijection between normal subgroups $L \trianglelefteq G/N$ such that $L \leq MN/N$ and normal subgroups $K \trianglelefteq G/(M \cap N) \cong G$ such that $K \leq M/(M \cap N)$. By assumption, $M \cap N = 1$, so $K \leq M$.

Therefore, the isomorphism $MN/N \cong M/(M \cap N)$ lifts the minimal normal subgroups of G/N that generate MN/N to minimal normal subgroups of G that must generate M and hence $M \leq \operatorname{soc} G$. □

It is now feasible to tackle the overall result that was used to justify the correctness of SOCLE.

Proof of Lemma 6.2. Let $N_i = \varphi_i^{-1}(\operatorname{soc} H_i)$. By Lemma 6.5, it is true that $\operatorname{soc} G \leq N_i$ for both $i = 1, 2$ and hence it lies in the intersection of interest. It just remains to prove the opposite inclusion.

$\varphi_1(N_1 \cap K_2) \leq \varphi_1(N_1) = \operatorname{soc} H_1$ so we can use Lemma 6.3 to write $\operatorname{soc} H_1 = \varphi_1(N_1 \cap K_2) \times N^*$ for some $N^* \trianglelefteq H_1$. Similarly $\varphi_1(N_1 \cap N_2) \leq \operatorname{soc} H_1$. Intersecting this the direct product shows that

$$\varphi_1(N_1 \cap N_2) = \varphi_1(N_1 \cap K_2) \times \varphi_1(M) \tag{6.8}$$

for some $M \leq \varphi_1^{-1}(N^*)$. Taking the inverse image of that equation under φ_1 and intersecting with $N_1 \cap N_2$ gives

$$N_1 \cap N_2 = (N_1 \cap K_2)((MK_1 \cap N_1) \cap N_2) = (N_1 \cap K_2)(M \cap N_1 \cap N_2)$$

since $N_1 \cap K_2 \leq N_1 \cap N_2$ and $K_1 \leq N_1$. We will show that these two factors are each contained in $\operatorname{soc} G$.

The subgroup $\varphi_1(N_1 \cap K_2) = (N_1 \cap K_2)K_1/K_1$ is normal in H_1 and is contained in $\operatorname{soc} H_1$. We have

$$N_1 \cap K_2 \cap \ker \varphi_1 \subseteq K_1 \cap K_2 = 1,$$

and thus we can apply Lemma 6.7 to see that $N_1 \cap K_2 \leq \operatorname{soc} G$.

The direct product in (6.8) implies $\varphi_1(N_1 \cap K_2) \cap \varphi_1(M) = 1$, that is, $N_1 \cap K_2 \cap M \leq \ker \varphi_1 = K_1$. Therefore, using the $K_1 \cap K_2 = 1$ assumption,

$$N_1 \cap K_2 \cap M \leq K_1 \cap K_2 = 1.$$

We have $\varphi_2(N_1 \cap M) \leq \operatorname{soc} H_2$, so using Lemma 6.7 again, we can see $N_1 \cap M \leq \operatorname{soc} G$ which is still true after intersecting the left-hand side with N_2.

Thus, the two generating components of $N_1 \cap N_2$ lie in $\operatorname{soc} G$ and so $N_1 \cap N_2 \leq \operatorname{soc} G$, proving equality. □

6.1.3. G^Ω imprimitive with one minimal block system

Our last case to handle is when G is imprimitive with only one minimal block system Σ. In this case, one cannot easily construct a pair of quotient groups via actions, and so finding a pair of subgroups to intersect in the same manner as the previous section is impossible. That said, we do have the ability to construct one such quotient group, $H = \varphi(G)$, via our block system Σ.

This section is the most significant departure from the procedure given in [CH97] and has the highest proportion of the adjustments of [Ung].

6.1.3.1. Line (15). It may be the case that $H \cong G$ and φ is the explicit isomorphism; this occurs if and only if $K = \ker \varphi = 1$. If this is the case, we must have $\operatorname{soc} G = \varphi^{-1}(\operatorname{soc} H) = J$ and so the handling on line (15) is correct.

6.1.3.2. Line (17). By Corollary 3.15, $L = S_1 \times \ldots \times S_m$ for some simple groups S_i, so it only remains to see that the S_i are all isomorphic to some simple group S to prove the assertion on line (17). In the manner of [CH97], suppose this is not true, and that we have, without loss of generality, $S_1 \ncong S_2$. Let the subgroups $N_1, N_2 \leq L$ be the direct product of all the simple groups S_i isomorphic to S_1 and S_2 respectively. We must have that $N_1 \cap N_2 = 1$ and $[N_1, N_2] = 1$ by Proposition 3.2. Furthermore, $N_i \operatorname{char} L \operatorname{char} K \trianglelefteq G$ and hence $N_i \operatorname{char} K \trianglelefteq G$ and thus $N_i \trianglelefteq G$, both by Proposition 3.5.

By Proposition 1.21, orbits of N_i^Ω form nontrivial blocks of Ω, and so each N_i must be transitive on each block B of Σ. Suppose this was not the case and for $\omega \in B$, $\omega^{N_i} \cap B \neq B$, the block ω^{N_i} is hence not a union of blocks of Σ. Every block is the union of blocks of some minimal block system, so if the assumption was true, there is a minimal block system for G^Ω that is not Σ, a contradiction. Hence [DM96, Theorem 4.2A] tells us that $N_1 \cong N_2$ since they are transitive and centralise each other. This contradicts the hypothesis $S_1 \ncong S_2$ and hence there is a single isomorphism class of the S_i.

6.1.3.3. Line (18). Let $d < |\Sigma|$ be the largest proper divisor of $|\Sigma|$, and take a block $\Delta \in \Sigma$. We wish to see that either of $K \neq L$ or $|K| \nmid |\Delta|^d$ is sufficient for

$\operatorname{soc} G \leq L$. This lemma and proof is due to [Ung].

Lemma 6.9. *If* $\operatorname{soc} G \not\leq L$ *then* $L = K$ *and* $|K| \mid |\Delta|^d$ *where* $\Delta \in \Sigma$ *and* d *is the largest proper divisor of* $|\Sigma|$.

Proof. If $\operatorname{soc} G \not\leq L$, then there must be some minimal normal subgroup $N \triangleleft G$ such that $N \not\subseteq L$. This induces a block system Σ' of its orbits, from which we can choose some $\Delta' \in \Sigma'$.

We have $K \trianglelefteq G$, so the orbits of K also form blocks of Ω. By construction, we certainly have $\omega^K \subseteq \Delta$ for $\omega \in \Delta \in \Sigma$, the minimality of Σ and faithfulness of G^Ω implies we must either have $K = 1$ or equality. The $K = 1$ case was eliminated earlier, so K is transitive on Δ for any $\Delta \subseteq \Sigma$ and hence the orbits of K are exactly the blocks of Σ. We have $L = \operatorname{soc} K \operatorname{char} K \trianglelefteq G$ and hence $L \trianglelefteq G$ by Proposition 3.5. We are guaranteed $L \neq 1$ since $K \neq 1$ is a finite group. The orbits of L are contained in those of K, and by identical reasoning to that for K, we can conclude the orbits of L are exactly the blocks of Σ too.

The kernel K fixes each block of Σ setwise, so the restriction $K \to K^{\Delta'}$ is well-defined and is a homomorphism. $N^{\Delta'}$ is transitive, and we have $[K,N] = 1$ and hence $[K^{\Delta'}, N^{\Delta'}] = 1$. These imply that $K^{\Delta'} \leq C_{\operatorname{Sym}(\Delta')}(N^{\Delta'})$ is semiregular by [DM96, Theorem 4.2A], that is, that $K^{\Delta'}_\delta = 1$ for any $\delta \in \Delta'$. Clearly the subgroup $L^{\Delta'} \leq K^{\Delta'}$ must also be semiregular. From the reasoning above, the orbits of the two groups are equal and so semiregularity of each implies $L^{\Delta'} = K^{\Delta'}$. The socle L is a direct product of simple groups, and so the restriction $L^{\Delta'}$ must have that form. These are all minimal normal subgroups and so $\operatorname{soc} K^{\Delta'} = K^{\Delta'}$.

Suppose $g \in \ker \varphi_{\Delta'}$ for all $\Delta' \in \Sigma'$. This implies that $\alpha^g = \alpha$ for all $\alpha \in \bigcup \Delta' = \Omega$, and so $g = 1$ since the action G^Ω is faithful. Hence, the kernels of the maps $\varphi_{\Delta'}$ intersect trivially, and so that component of each pull-back disappears in the intersection.

By inducing on the number of subgroups K_i in Lemma 6.2 it is possible to write the socle $L = \operatorname{soc} K$ as the intersection of the socles on the orbits. This induction works for this case by the trivial-intersection property proved in the previous paragraph: one can write $K_1 = \ker \varphi_{\Delta'}$ and $K_2 = \bigcap \ker \varphi_{\Delta''}$ where the latter ranges over the blocks $\Delta'' \neq \Delta'$. That is,

$$L = \operatorname{soc} K = \bigcap_{\Delta' \in \Sigma'} \varphi_{\Delta'}^{-1}(\operatorname{soc} K^{\Delta'}) = \bigcap_{\Delta' \in \Sigma'} \varphi_{\Delta'}^{-1}(K^{\Delta'}) = \bigcap K = K$$

The action K^Δ on an orbit $\Delta \in \Sigma$ is regular, since it is transitive and transitive as discussed above. This shows that $|K^\Delta| = |\Delta|$ and hence, since the Δ form orbits of $K^{\Delta'}$, it must be that $|K^{\Delta'}| = |\Delta|$ or else semiregularity would be violated. Since the Δ' partition Ω, the groups $K^{\Delta'}$ capture the entirety of K, that is, $K \leq \prod_{\Delta' \in \Sigma'} K^{\Delta'}$ and hence, taking orders of each side, $|K| \mid |\Delta|^c$ where $c = |\Sigma'|$.

The minimal normal subgroup N of G chosen above has $K \cap N = 1$ by construction, and so N^Σ is faithful (recall that K is the kernel of the action on Σ), and hence the minimality of Σ implies that each $\Delta' \in \Sigma'$ must be the union of some

equal number of blocks of Σ, so $c \mid |\Sigma|$. It is impossible to have $\Sigma = \Sigma'$ as that would require $N \leq K$, a contradiction. This shows $c < |\Sigma|$ and so there is a bound $c \leq d$ where d is the largest proper divisor of $|\Sigma|$. □

Line (18) is the contrapositive of the statement of this lemma and hence is correct.

6.1.3.4. Lines (19-21): S nonabelian. Recall that L is a direct power of a simple group, so that simple factor of L is nonabelian if and only if L is nonabelian. If this is the case, the following result applies.

Lemma 6.10. *If $N \trianglelefteq G$ and $N = S_1 \times \ldots \times S_m$ where the S_i are simple and nonabelian, then $N \leq \operatorname{soc} G$.*

Proof. G permutes the S_i via conjugation and they are nonabelian, so the direct product of the elements within an orbit of this action form a minimal normal subgroup of G. The S_i commute, and so these direct products commute, and hence N is generated by these minimal normal subgroups, meaning $N \leq \operatorname{soc} G$. □

This shows that a nonabelian L satisfies $L \leq \operatorname{soc} G$. If the earlier check for $\operatorname{soc} G \leq L$ succeeded, then $L = \operatorname{soc} G$ and so line (19) is correct.

On the other hand, if the $\operatorname{soc} G \leq L$ check on line (18) failed, that is, we have that $L = K$ and $|K| \mid |\Delta|^d$. It just remains to see that $\operatorname{soc} G = \varphi^{-1}(\operatorname{soc} \varphi(C))$ as stated on line (21). L is the direct product of nonabelian simple groups, so $Z(K) = 1$, or else there would be some abelian minimal normal subgroup of C which then must appear in the socle L. This gives $K \cap C = Z(K) = 1$, and hence $\varphi(C) \cong C$, thus $\operatorname{soc} C \cong \operatorname{soc} \varphi(C)$ and $\varphi^{-1}(\operatorname{soc} \varphi(C)) = K \operatorname{soc} C$.

Since distinct minimal normal subgroups commute, it is certainly true that $\operatorname{soc} G \leq K \operatorname{soc} C$, that is, C contains all minimal normal subgroups of G not inside K. We assert that $K \operatorname{soc} C$ is the direct product of nonabelian simple groups, so that Lemma 6.10 implies $\operatorname{soc} G \geq K \operatorname{soc} C$ and hence we have the desired equality.

To justify that assertion, we just need to show that the simple factors of $\operatorname{soc} C$ are nonabelian, since this is already known for $K = \operatorname{soc} K = L$ by assumption. Take a minimal normal subgroup $N \not\leq K$ of G as in the proof of Lemma 6.9. As stated there if Δ' is an orbit for N then $N^{\Delta'}$ is transitive. If $N^{\Delta'}$ were abelian, then [DM96, Theorem 4.2A (v)] implies that $C_{\operatorname{Sym}(N^{\Delta'})}(N^{\Delta'}) = N^{\Delta'}$, but, as we saw above, $K^{\Delta'}$ centralises $N^{\Delta'}$, which would give $K^{\Delta'} \leq N^{\Delta'}$, a contradiction. Therefore $N^{\Delta'}$ is nonabelian and so all minimal normal subgroups of G are nonabelian.

The only thing that remains is the validity of the recursion to compute $\operatorname{soc} \varphi(C)$: we have $K \cap C = 1$ so $\varphi(C) \cong C < G$ is a strict subgroup, and, we also have that the degree $|\Sigma|$ of $\varphi(C)$ is smaller than the degree $|\Omega|$ of G. Either of these individually is enough to guarantee that the recursion will terminate.

6.1.3.5. Lines (23-32): S abelian. If S is abelian, we have $S = C_p$ for some prime p. In this case, Lemma 6.10 does not always hold and so simply applying $\varphi^{-1}(\operatorname{soc} \varphi(\cdot))$ does not give the desired result.

The main idea is to compute the abelian and nonabelian parts of the socle separately, that is, write $\operatorname{soc} G = E^\dagger \times M^\dagger$ where $E^\dagger$ is a direct product of abelian simple groups and $M^\dagger$ is a direct product of nonabelian simple groups. The socle is always the direct product of simple groups so this partitioning is always possible. To compute the abelian part, we find some subgroup $E \leq G$ that definitely contains $E^\dagger$, and find the appropriate minimal normal subgroups within that. This computation is that described by [Ung].

6.1.3.6. Lines (23-26). If $\operatorname{soc} G \leq L$ then clearly $E^\dagger \leq L$, so $E = L$ is a perfectly good choice. We need more complicated handling if we do not know that $\operatorname{soc} G \leq L$, that is, if the test on line (18) does not succeed.

First, we consider the following result, which holds regardless of whether $\operatorname{soc} G \leq L$ or not.

Lemma 6.11. *If G^Ω is such that* SOCLE *reaches line (23), then the abelian part $E^\dagger$ of $\operatorname{soc} G$ is an elementary abelian p-group.*

Proof. If $E^\dagger \leq K$ then $E^\dagger \leq L$ and so $E^\dagger$ is an elementary abelian p-group, since L is.

On the other hand, if $E^\dagger \not\leq K$, we can find some abelian minimal normal subgroup N of G outside K. Take some orbit Δ' of N, $N^{\Delta'}$ is transitive, and by similar reasoning to the proof of Lemma 6.9, $[L^{\Delta'}, N^{\Delta'}] = 1$. Hence $L^{\Delta'} \leq C_{G^{\Delta'}}(N^{\Delta'})$, however, we know that

$$C_{G^{\Delta'}}(N^{\Delta'}) \leq C_{\mathrm{Sym}(\Delta')}(N^{\Delta'}) = N^{\Delta'},$$

by [DM96, Theorem 4.2A (v)] since $N^{\Delta'}$ is transitive and abelian.

That is, we've shown $L^{\Delta'} \leq N^{\Delta'}$. Again, mirroring of the proof of Lemma 6.9, we have $L^{\Delta'} \neq 1$, and it must be a p-group. N is a direct power of C_q for some prime q by Theorem 3.3. The inclusion above shows $N^{\Delta'}$ is a p-group, and so we must have $q = p$, and hence $E^\dagger$ is elementary abelian in this case too. □

The above gives sufficient information to justify the handling of the case when it is unknown if $\operatorname{soc} G \leq L$.

Lemma 6.12. *With the notation as above, the abelian part $E^\dagger$ of $\operatorname{soc} G$ satisfies*

$$E^\dagger \leq E = \Omega_1(Z(\varphi^{-1}(O_p(\operatorname{soc} H)))).$$

Proof. Recall that $O_p(T)$ is the (unique) largest normal p-subgroup of T. It was shown in Lemma 6.5 that $\varphi(\operatorname{soc} G) \leq \operatorname{soc} H$, and $E^\dagger \trianglelefteq \operatorname{soc} G$ is known to be a p-group, so $\varphi(E^\dagger) \leq O_p(\operatorname{soc} H) =: P$, in other words $E^\dagger \leq \varphi^{-1}(P)$.

The kernel K of φ has socle L which is a p-group, and so must be a p-group itself. Thus, $\varphi^{-1}(P)$ is a p-group. Hence, it has nontrivial centre, and, any normal subgroup has nontrivial intersection with the center. This includes any minimal normal p-subgroup N: it satisfies $N \cap Z(\varphi^{-1}(P)) \neq 1$. The minimum normality of N shows $N \leq Z(\varphi^{-1}(P))$. By the previous lemma, all abelian minimal normal subgroups of G are p-groups, implying $E^\dagger \leq Z(\varphi^{-1}(P))$.

That lemma also shows that $E^\dagger$ is not only a p-group, but that it is elementary abelian. Therefore, all non-identity elements have order p, and so only considering elements of order p reduces the size of the covering group E with no risk of losing any elements of $E^\dagger$. This is precisely the choice

$$E = \Omega_1(Z(\varphi^{-1}(O_p(\operatorname{soc} H)))).$$ □

6.1.3.7. Line (27). For either choice of E, it is elementary abelian: if $E = L$, L is be the direct product of isomorphic simple groups, and is abelian, so the only choice is for those simple groups to be C_p for some fixed p. E is clearly elementary abelian by definition in the other branch.

The group E can be regarded as the vector space $\mathbb{F}_p^n$ for some n. There is a natural action of G on E, by conjugation, and so this vector space is a G-module. The minimal submodules of E are exactly the minimal normal subgroups of G that lie in E, and hence $E^\dagger$ is generated by these. Thus, the definition of E' is exactly the abelian part of $\operatorname{soc} G$.

6.1.3.8. Lines (29-32). It just remains to compute the nonabelian part. We wish to show that the M' computed on line (31) is equal to our nonabelian part $M^\dagger$ of the socle. This procedure is now the approach taken by [CH97].

Lemma 6.13. *$M/(K \cap M)$ is the direct product of simple groups (asserted on line (29)).*

Proof. Recall that $J = \varphi^{-1}(\operatorname{soc} H)$, where $H = G^\Sigma$.

There is a natural isomorphism $M/(M \cap K) \cong MK/K$. We claim that $MK/K \trianglelefteq J/K$: take $mkK \in MK/K$ with $m \in M$, $k \in K$, and $jK \in J/K$; conjugating mkK gives

$$(j^{-1}K)(mkK)(jK) = (j^{-1}mj \cdot j^{-1}kj)K = (m^j k^j)K.$$

It just remains to prove to see that $m^j \in M$ and $k^j \in K$; that is, that conjugation leaves MK/K fixed setwise.

$K \trianglelefteq G$ so $k^j \in K$, and, again by normality, $m^j \in C_G(K) = C$ since

$$j^{-1}mj \cdot k = j^{-1}mk^{j^{-1}}j = j^{-1}k^{j^{-1}}mj = k \cdot j^{-1}mj.$$

It is clear that $m^j \in J$ and thus $m^j \in C \cap J = M$, proving the claim.

$K = \ker\varphi \geq \ker\varphi|_J$ so $J/K \cong \operatorname{soc} H/K^*$ for some $K^* \trianglelefteq \operatorname{soc} H$, thus J/K is the direct product of simple groups and so any normal subgroup must be isomorphic to a similar direct product. □

The focus is only on the nonabelian factors of $M/(K \cap M)$: any abelian factors can easily be annihilated by taking the derived subgroup.

Recall that $M^\dagger = T_1 \times \ldots \times T_k$ for some nonabelian simple groups T_i. At this point, $[M^\dagger, K] = 1$ since $\operatorname{soc} K$ is abelian and so cannot contain any of the T_i, hence $M^\dagger \leq C_G(K) = C$. It is clear that $M^\dagger \leq \operatorname{soc} G \leq J$. These together show that $T_i \leq M^\dagger \leq M = C \cap J$. Each T_i is a nonabelian simple group so

$$T_i \cap (M \cap K) \leq T_i \cap Z(K) = 1,$$

and hence, under the quotient map into $M/(M \cap K)$, each T_i maps to a unique simple factor, say $M_i/(K \cap M)$. Hence, for these nonabelian factors can be written $M_i = T_i \times (K \cap M)$ and the intersection satisfies

$$K \cap M = K \cap C_G(K) \cap J \leq Z(K).$$

This shows that taking the derived subgroup of an M_i eliminates this extraneous factor, that is: $M_i' = [M_i, M_i] = T_i$. Therefore, there is a labelling of the M_i such that $T_i = M_i'$ for all i and hence $T_i \leq M'$. This shows that $M^\dagger \leq M'$.

On the other hand, each $M_i' \trianglelefteq M'$ is a nonabelian simple minimal normal subgroup of M' so M' is the direct product of nonabelian simple groups. Thus, by Lemma 6.10, $M' \leq \operatorname{soc} G$. However, M' is made up entirely of nonabelian simple groups, so $M' \leq M^\dagger$. We conclude $M' = M^\dagger$ and hence SOCLE is correct.

CHAPTER 7

What's Next?

The socle is one of the key subgroups in the modern approach to computing with groups. It is part of an important series of characteristic subgroups of G,

$$1 \leq L \leq M \leq K \leq G \tag{7.1}$$

where $L = O_\infty(G)$ is the largest normal solvable subgroup, the *solvable radical*, M is the full inverse of the socle of G/L, that is, $M/L = \mathrm{soc}(G/L)$, and K is the kernel of the action of G on the simple factors of M. This characteristic series is a useful tool in the study of group, and matrix groups in particular.

The quotients of its terms display the power of this series, and also the utility of the socle: M/L is the direct product of (nonabelian) simple groups, K/M is a solvable subgroup of the direct product of the automorphism groups of the simple factors of M and the top layer G/K faithfully permutes the set of simple factors of M. This set is small so G/K can be represented as a low-degree permutation group, meaning the large body of permutation group algorithms can be applied. Hence, this chain allows for reducing a question about a general group to one about the solvable component L and the quotients listed above.

Matrix groups are subgroups of $\mathrm{GL}(n,q)$ for some n, q, and even for moderate n and q the minimal degree of a permutation representation can easily be too large for conventional permutation group approaches to be effective. [BBS09] or [Bää+14] are examples of the culmination of 25 years of work on methods of computing and using the series (7.1) in matrix groups via *composition trees*. These trees serve the same role as a BSGS (see Section 2.3) in matrix groups, where even the shortest orbits can be extremely large, making the Schreier-Sims algorithm unusable.

Returning to permutation groups, we give an example of how knowledge of $\mathrm{soc}\,G$ can be used to compute other properties of G. [CH97] introduced algorithms for computing chief and composition series that build on their socle algorithm. Recall that a chief series is a normal series $1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$ such that $G_i \trianglelefteq G$ and G_{i+1}/G_i is a minimal normal subgroup of G/G_i for each $i < n$. As with the socle algorithm, the algorithm for a chief series reduces to the case that G is primitive. In this case, compute the socle of G and, if G is not of affine type, the nonabelian simple factors. In the case that it is of affine type, compute a chief series of a point stabiliser and lift this to one for G by multiplying with the socle. In the case that it is not, take the action $H = G^{\mathscr{F}}$ of G on the set $\mathscr{F}$ of simple factors of the socle. A chief series for H can be lifted to G via the inverse of the action epimorphism $\varphi : G \to H$. This lifted series is not necessarily exactly the desired chief series but it is close, the algorithm distinguishes four cases with slightly different handling for each. For example, if G lies in case II(c), the union of one of the orbits of G on $\mathscr{F}$ is a normal subgroup of G strictly contained in

$\operatorname{soc} G$, and so this forms an additional term in the chief series.

The composition series algorithm is similar (so similar that [CH97] elides a separate description of it), but the use of the socle factors becomes even more obvious. In the chief series algorithm, the socle factors are used to possibly add an additional term; for a composition series, one can recursively a composition series for $G/\operatorname{soc} G$, lift it to G, and use the socle factors to fill in the remaining terms of the composition series for G starting at $\operatorname{soc} G$:

$$\operatorname{soc} G \rhd \langle S_1, \ldots, S_{m-1} \rangle \rhd \ldots \rhd \langle S_1, S_2 \rangle \rhd S_1 \rhd 1.$$

These generated subgroups are direct products, making computation of them trivial, and case-by-case handling required is not required for this.

References

[Bää+14] H. Bäärnhielm et al. “A practical model for computation with matrix groups”. In: *Journal of Symbolic Computation* (2014). To appear.

[Bab+95] L. Babai et al. “Fast Monte Carlo Algorithms for Permutation Groups”. In: *Journal of Computer and System Sciences* 50.2 (1995), pp. 296–308.

[BBS09] L. Babai, R. Beals, and Á. Seress. “Polynomial-time Theory of Matrix Groups”. In: *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*. STOC ’09. Bethesda, MD, USA: ACM, 2009, pp. 55–64.

[BCP97] W. Bosma, J. J. Cannon, and C. Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[But91] G. Butler. “Implementing some algorithms of Kantor”. English. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Ed. by H. Mattson, T. Mora, and T. Rao. Vol. 539. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1991, pp. 82–93.

[CH03] J. J. Cannon and D. F. Holt. “Automorphism group computation and isomorphism testing in finite groups”. In: *Journal of Symbolic Computation* 35.3 (2003), pp. 241–267.

[CH97] J. J. Cannon and D. F. Holt. “Computing Chief Series, Composition Series and Socles in Large Permutation Groups”. In: *J. Symb. Comput.* 24.3-4 (Oct. 1997), pp. 285–301.

[CS97] J. J. Cannon and B. Souvignier. “On the Computation of Conjugacy Classes in Permutation Groups”. In: *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*. ISSAC ’97. Kihei, Maui, Hawaii, USA: ACM, 1997, pp. 392–399.

[DM96] J. Dixon and B. Mortimer. *Permutation Groups*. Graduate Texts in Mathematics. Springer New York, 1996.

[FT63] W. Feit and J. Thompson. “Solvability of groups of odd order”. In: *Pacific Journal of Mathematics* 13.3 (1963), pp. 775–787.

[GAP] *GAP – Groups, Algorithms, and Programming, Version 4.7.5*. The GAP Group. 2014.

[HEO05] D. Holt, B. Eick, and E. O’Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and Its Applications. Taylor & Francis, 2005.

[Kan85] W. M. Kantor. “Sylow’s theorem in polynomial time”. In: *Journal of Computer and System Sciences* 30.3 (1985), pp. 359–394.

[Kan91] W. M. Kantor. “Finding Composition Factors of Permutation Groups of Degree $n \leq 10^6$”. In: *J. Symb. Comput.* 12.4-5 (Oct. 1991), pp. 517–526.

[Kim+90] W. Kimmerle et al. “Composition factors from the group ring and Artin’s theorem on orders of simple groups”. In: *Proc. London Math. Soc* 3 (1990), pp. 89–122.

[LPS88] M. W. Liebeck, C. E. Praeger, and J. Saxl. “On the O’Nan-Scott theorem for finite primitive permutation groups”. In: *J. Austral. Math. Soc. Ser. A* 44.3 (1988), pp. 389–396.

[Neu87] P. Neumann. “Some algorithms for computing with finite permutation groups”. In: *Proceedings of Groups St Andrews 1985*. Ed. by E. F. Robertson and C. M. Campbell. Cambridge Books Online. Cambridge University Press, 1987, pp. 59–92.

[Pas68] D. Passman. *Permutation groups*. Mathematics lecture note series. W. A. Benjamin, 1968.

[Ser03] Á. Seress. *Permutation Group Algorithms*. Cambridge Books Online. Cambridge University Press, 2003.

[Sim70] C. C. Sims. “Computational methods in the study of permutation groups”. In: *Computational problems in abstract algebra*. Oxford: Pergamon Press, 1970, pp. 169–183.

[Sim71] C. C. Sims. “Computation with Permutation Groups”. In: *Proceedings of the Second ACM Symposium on Symbolic and Algebraic Manipulation*. SYMSAC ’71. Los Angeles, California, USA: ACM, 1971, pp. 23–28.

[Ung] W. R. Unger. “Notes on the Cannon-Holt socle algorithm”. In preparation.

[Ung06] W. R. Unger. “Computing the soluble radical of a permutation group”. In: *Journal of Algebra* 300.1 (2006). Computational Algebra Special Issue Celebrating the 65th birthday of Charles Leedham-Green, pp. 305–315.

[Wie64] H. Wielandt. *Finite permutation groups*. Academic paperbacks. Academic Press, 1964.