Minimum bases for permutation groups

Lawrence Chen

Supervised by A/Prof. Heiko Dietrich and Dr Santiago Barrera Acevedo

21 October 2022

Honours thesis in the School of Mathematics, Monash University

Abstract

A *permutation group* G of degree n is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ that acts on a set Ω of size n, where $\mathrm{Sym}(\Omega)$ is the group of bijections $\Omega \to \Omega$. An ordered list $B = [\beta_1, \ldots, \beta_r]$ of distinct elements of Ω is a *base* for G if the pointwise stabiliser $G_{(B)}$ is trivial; the minimal size of a base for G is denoted $b(G)$. Every base $B = [\beta_1, \ldots, \beta_r]$ has an associated *stabiliser chain* $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$, where each subgroup $G^i = G^{i-1}_{\beta_i}$ in the chain is a stabiliser of the previous subgroup; a *strong generating set* S for G relative to B is a generating set for G such that $G^i = \langle S \cap G^i \rangle$ for each i. The combined concept of a *BSGS (base and strong generating set)* allows us to easily perform various computations with permutation groups, such as membership testing and random element generation. In this thesis, we follow Blaha's proof in [3] that the *minimum base problem* is NP-hard even if restricted to cyclic groups or elementary abelian group, and discuss a greedy algorithm for computing a small base for G, which is not optimal but still useful in practice. We analyse the Rubik's group G, a permutation group of degree 48, and show that $b(G) = 18$. Subsequently, we discuss recent progress in bounding the minimal base size $b(G)$ for groups that are not *large base*: a permutation group G is large base if contains a power of an alternating group, and is itself embedded in a *wreath product* of certain symmetric groups. Finally, we investigate a question from Moscatiello and Roney-Dougal in [23], and using computational methods in GAP 4 and the greedy base algorithm, we show that there are very few primitive subgroups $G \leq \mathrm{Sym}(2^d)$, where $1 \leq d \leq 10$, such that $b(G) = d + 1$. These groups are subgroups of the *affine group* $\mathrm{AGL}_d(2)$, and there are none for $d = 1$, one for $d = 2$ and odd $3 \leq d \leq 9$, and two for even $4 \leq d \leq 10$, all up to conjugacy.

Acknowledgements

Firstly, I would like to express my gratitude to my supervisors Heiko and Santiago, who provided me with guidance and direction, and helped to cultivate my interest in group theory. I appreciate their tireless effort in imparting their knowledge, and for the hours spent reading over my thesis to give prompt and useful feedback, even on weekends and late at night. I would also like to thank Norm, Ian, Nick, Wenhui, Andrea, Todd, Jessica, Dionne, Tim and Eric, whose courses I have learned and received much from, and for the valuable feedback from coursework that has shaped my thesis.

I would also like to thank my friends in the Honours cohort, especially Jeremy, Will, Clayton and Jake, for their friendship and support over the year, for all the good memories, and for giving me useful tips for my thesis and presentation. For Puti too, who has helped me so much. This extends to various members of online communities – the Maths @ Monash and Chats & Reacts Discord servers, whose company I have been blessed with over this year.

I would like to thank my parents for the countless hours they have spent supporting me in every way at home to give me time and energy to maintain my busy schedule. I would also like to thank my friend Wes for being my greatest support through good and trying times this year, and giving me inspiration for my Honours presentation. To Chris, whose godly wisdom has shaped and sharpened me in so many ways this year. Also, to all my church group members and fellow leaders for their constant support and care in busy times.

Lastly, I would like to thank God for His guiding hand in my life, and for being the reason I am where I am today. In the midst of busyness and challenges this year, His presence has given me hope, rest and security. I am so grateful for His constant love, faithfulness, mercy and grace, and I thank Him for this Honours experience in this season of my life.

> "There is a time for everything,
> and a season for every activity under the heavens"
>
> — Ecclesiastes 3:1 (NIV)

Contents

Chapter 1

Introduction

1.1 Assumed knowledge

This thesis will assume knowledge of content covered in the (former) undergraduate unit MTH3121 – Algebra and number theory I, run at Monash University until 2021, in particular the group theory half of the unit. It covers basic group theoretic concepts, such as isomorphism, homomorphisms, subgroups, cosets, Lagrange's theorem, normal subgroups, quotient groups, and the first isomorphism theorem, and studies cyclic groups, dihedral groups, symmetric groups and alternating groups. It did not cover group actions, bases, and related topics, which are therefore included here in the following chapters.

1.2 Motivation

Traditionally, a major goal of research in algebra has been to answer, in various ways, the question of finding all the algebraic structures that satisfy particular axioms, as noted in [8]. One such major result in this area was the famous classification of finite simple groups, which are finite groups whose only normal subgroups are the trivial ones. In [30], it is noted that around the year 2000, computational methods for groups were useful in calculating and classifying finite groups of various orders. This has all stemmed from the development of computational methods in algebra, especially in group theory, since the early 1970s, to compute information about groups for various purposes. In [8], Cannon and Havas note that the state of development of computational group theory is relatively advanced, and has seen applications not only in the study of groups, but also in many other branches of mathematics which use group theoretic methods, for example differential equations, graph theory, number theory and topology.

Cannon and Havas observe in [8] that the study of permutation groups is one of the areas in computational group theory that has traditionally seen high activity. A permutation group is a subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on some set $\Omega \neq \emptyset$, which is the group of all bijections $\Omega \to \Omega$ under composition. Permutation groups are particularly nice to work with computationally, as their elements can be explicitly identified as permutations on a set, and computations in the group can be easily performed by composing these permutations, say by a computer. Various computational packages such as GAP have been developed, which have implemented permutation groups computationally. Solomon observes in [30] that computational methods for permutation groups have been considered in the classification problem for finite simple groups, among other applications. Every finite group can be represented as a permutation group by Cayley's theorem, and the degree (size of the set being permuted) of a permutation group representation is often small, especially compared to the size of the group.

Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group. To study G, the notion of group actions is particularly useful, since elements of G are permutations of Ω, so G acts naturally on Ω by permutation. Actions with only one orbit are said to be *transitive*; if a transitive action has no nontrivial *blocks*, then it is *primitive*. This also allows us to explore the notion of bases and

stabiliser chains: a base B is a list of elements of Ω such that the identity $1_{\mathrm{Sym}(\Omega)}$ is the only permutation that fixes each element in B, and a stabiliser chain (as introduced and implemented by Sims in [27]) is a subgroup series, with each group in the series being the stabiliser of a base element in the preceding group. (See section 2.2 for details and examples.) These notions allow us to answer a few natural questions about permutation groups, in particular determining the order of G, finding a generating set for G when realised as a group of permutations of certain objects (for example, vertices of an n-gon and vertices in a graph), determining membership of arbitrary permutations $g \in \mathrm{Sym}(\Omega)$ in the subgroup G, and generating random elements of G. These preliminary questions are illustrated and addressed in this thesis.

Bases and stabiliser chains have been an instrumental tool in developing group theoretic algorithms, and effectively facilitate the storing and analysing of large permutation groups. Given the notion of bases and stabiliser chains, it is natural to ask about the possible sizes of a base, and if there are bounds on the size, perhaps if there is an efficient way to find a minimum (smallest) base. For instance, it can be easily seen that for $G = \mathrm{Sym}(n)$ the symmetric group on n elements $\Omega = \{1, \ldots, n\}$, a minimum base has size $b(G) = n - 1$. However, a natural permutation representation of a dihedral group $G = D_{2n}$ (that also acts on Ω) has minimal base size 2. Since every element in a permutation group is completely determined by its action on a base, a small base can reduce the space required to store the group.

In [3], Blaha discusses the question of whether a polynomial time greedy algorithm suggested in [5] always finds a minimum base for a permutation group G, to answer the question "for what r does a permutation group G have a base of size at most r?" He shows that this is not the case, and even when restricted to elementary abelian groups, the problem is NP-hard. However, Blaha shows that the algorithm presented produces a base of size $O(b(G) \log \log n)$ where $b(G)$ is the size of a minimum base for $G \leq \mathrm{Sym}(n)$, and that in the worst case, this bound, which is asymptotically larger than $b(G)$, is actually attained. (Note that all logarithms in this thesis are base-2.)

Another problem that has traditionally attracted much attention was bounding the order of a finite primitive (permutation) group of degree n, i.e. a permutation group on Ω whose natural action is transitive and such that no nontrivial partition of Ω is preserved by the action [23]. Since $|G| \leq n^{b(G)}$ (see Lemma 2.57), we can find upper bounds on $|G|$ by finding upper bounds on $b(G)$. In 1889, Bochert proved in [4] that for a primitive group G of degree n not containing the alternating group $\mathrm{Alt}(n)$, then $b(G) \leq n/2$; [23] notes that this was one of the first results in this direction.

In 1984, Liebeck proved in [20] that if G is a primitive group of degree n that is not "large base" (in the sense of containing a power of an alternating group as a subgroup), then $b(G) < 9 \log n$. The result was proven in context improving lower bounds on $\mu(G)$, the minimal degree of G, which is the smallest number of points moved by any non-identity element in G. This proof utilised the O'Nan-Scott theorem, which classifies primitive groups according to the structures of their *socles*, and also the classification of finite simple groups (which was recently completed at the time), and was able to achieve a much tighter lower bound of $\mu(G) > n/(9 \log n)$ than the best result that was previously available, which was $\mu(G) > (1/2)(\sqrt{n} - 1)$ and due to Babai in [2].

In 2021, building on more recent results, Moscatiello and Roney-Dougal proved in [23] that if G is a primitive group of degree n that is not large base, then either G is the Mathieu group M_{24}, or $b(G) \leq \lceil \log n \rceil + 1$; moreover, there are infinitely many groups for which $b(G) > \log n + 1$. The Mathieu group M_{24} is a member of the first family of sporadic simple groups discovered as part of the classification of finite simple groups, which are 26 finite simple groups that do not fit into the three infinite families (cyclic, alternating, Lie type).

The authors of [23] then present a question, which asks to identify primitive groups G of degree n that satisfy $b(G) = \log n + 1$. They note that G must be a subgroup of the affine group $\mathrm{AGL}_d(2)$ of affine transformations of $\mathbb{F}_2^d$ for some d, and that if d is even then groups such as the split extension $2^d : \mathrm{Sp}(d, 2)$ have this property. Upon investigation using a recursive approach for $d \leq 10$, we found that apart from the affine group $\mathrm{AGL}_d(2)$, there were no other primitive groups for odd d, and for even d, the only other example found was $2^d : \mathrm{Sp}(d, 2)$. Consequently, we conjecture in this thesis that these are the only groups satisfying this property. Limitations of this approach include memory and computational time, since the group found for $d = 10$ has order $25\,410\,822\,678\,459\,187\,200 \approx 2.5 \cdot 10^{19}$ and thus has many subgroups.

The first part of this thesis largely builds up to a discussion of the results about the NP-hardness of the minimum base problem in [3]. Firstly, a detailed introduction to group-theoretic concepts such as group actions, bases and stabiliser chains is presented. We apply the concepts of bases, transitivity and primitivity to the Rubik's group G, a permutation

group of degree 48 that describes valid moves for the Rubik's cube, and show that $b(G) = 18$. Necessary concepts from complexity theory are introduced for a detailed discussion of [3] that expands on Blaha's proof that finding a minimum base is NP-hard (even for groups with bounded orbits), and we summarise the results on sharp bounds for nonredundant and greedy bases. Afterwards, we review classification results for permutation groups, including the classification of finite simple groups, semidirect and wreath products, affine groups, and the influential O'Nan-Scott theorem for primitive groups. Finally, we discuss improvements in bounds on $b(G)$ for non-large-base primitive groups G as found by Liebeck in [20] and Moscatiello and Roney-Dougal in [23], and investigate the question posed on primitive groups of degree n that satisfy $b(G) = \log n + 1$. Future directions include more investigation into the question from [23] and the conjecture presented in this thesis, collecting various known results and bounds for base sizes of large-base primitive groups and imprimitive permutation groups, and identifying special classes of examples where specific bounds or results can be newly found in relation to the NP-hardness of the minimum base problem and analysis of the greedy base algorithm.

Chapter 2

Preliminary concepts from permutation groups

Permutation groups, which are groups whose elements are realised as permutations of some (nonempty) set Ω, play a central role in **computational group theory**, which uses computational methods to compute and store information about groups.

The notion of a *group action* arises naturally from the concept of permutation groups, since group actions encode group elements as permutations: every permutation group on Ω naturally induces an action on Ω, and a permutation group arises from every group action. Let G be a group and $\alpha \in \Omega$; the notions of an *orbit* and *stabiliser* of α can be defined for G-actions on Ω. (The stabiliser of α comprises elements $g \in G$ whose associated permutations fix α.)

A *base* is an ordered list B of elements of Ω such that only the identity element $1 \in G$ fixes every element of B pointwise; a base gives rise naturally to a series of stabiliser subgroups called the *stabiliser chain*, and a generating set that respects this structure is called a *strong generating set*; these are used in numerous algorithms across computational group theory. We now approach this formally.

Definition 2.1. Let Ω be a set. The **symmetric group** $\mathrm{Sym}(\Omega)$ on Ω consists of *permutations* of Ω (bijections $\Omega \to \Omega$) under composition. A **permutation group** on Ω is a subgroup of $\mathrm{Sym}(\Omega)$; its **degree** is $|\Omega|$.

When $\Omega = [n] := \{1, \ldots, n\}$, we instead write $\mathrm{Sym}(n)$ for the **symmetric group of degree** n**.** (A similar notation is $\mathrm{Alt}(n)$ for the **alternating group of degree** n of even permutations of n, i.e. permutations that can only be written as a composition of an even, but not odd, number of transpositions.) In this thesis, we use the following conventions: for $\alpha \in \Omega$ and $g, h \in \mathrm{Sym}(\Omega)$, write α^g for the image of α under g (instead of $g(\alpha)$ or $g\alpha$), and we perform g then h in the composition (product) gh, so that $\alpha^{gh} = (\alpha^g)^h$. Also, for the trivial subgroup we write $1 = \{1\} \leq G$.

As permutations are a central object of study, we recall the *disjoint cycle notation*. Let Ω be a set; if $\alpha_1, \ldots, \alpha_r$ are distinct elements of Ω, we write $\sigma = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ for the cycle $\sigma \in \mathrm{Sym}(\Omega)$ with $\alpha_i^\sigma = \alpha_{i+1}$ for $1 \leq i < r$, $\alpha_r^\sigma = \alpha_1$, and $\alpha^\sigma = \alpha$ for $\alpha \in \Omega \setminus \{\alpha_1, \ldots, \alpha_r\}$. If Ω is finite, then every permutation can be decomposed into a product of disjoint cycles; we generally omit fixed points (cycles of length 1). The lengths of these cycles give the *cycle type* of σ. The identity permutation Id_Ω is written as $1_{\mathrm{Sym}(\Omega)}$, $()$, or just 1 when context is clear.

A group G is **generated by a set** X if every $g \in G$ can be written as $g = x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k}$ with each $x_i \in X$, $\varepsilon_i = \pm 1$, and $k \in \mathbb{N}$; if $k = 0$ then we have the empty product $g = 1$. We write $G = \langle X \rangle$. When $G = \langle X \rangle$ for some finite X, G is **finitely generated**. When $X, Y \subseteq G$, we write $\langle X, Y \rangle = \langle X \cup Y \rangle \leq G$ as the subgroup generated by X and Y; this notion naturally extends to any finite number of subsets of G.

The forms of the statements of Lagrange's theorem and the first isomorphism theorem that are used in this thesis are:

Theorem 2.2 (Lagrange). *If G is a group and $H \leq G$, let $H\backslash G$ be the set of right cosets of H in G. Assuming the axiom of choice, the map $H \times (H\backslash G) \to G$ given by $(h, Hg) \mapsto hg$ is a bijection. (This yields $|G| = |G : H||H|$, where $|G : H| := |H\backslash G|$*

*is the **index** of H in G.)* □

This is a form that applies for infinite groups G and H.

Theorem 2.3 (First isomorphism theorem). *If G, H are groups and $\varphi : G \to H$ is a homomorphism, then $K := \operatorname{Ker}\varphi \trianglelefteq G$ and $G/K \cong \varphi[G]$ via the map $G/K \to \varphi[G]$ with $gK \mapsto \varphi(g)$.* □

2.1 Group actions

The following section is largely adapted from Holt [15], with original examples and illustrations.

We often think of D_{2n}, the dihedral group of order $2n$, as the symmetry group of a regular n-gon. But abstractly, $D_{2n} = \langle r, s \mid r^n, s^2, srsr \rangle$ is defined by a presentation, a set of generators and relations. The precise way in which elements of D_{2n} "are" symmetries is given by an *action* of D_{2n} on say the vertex set Ω of a regular n-gon; each element of D_{2n} permutes Ω, and the product in D_{2n} mirrors compositions of corresponding permutations. The following definition formalises this idea and extends it to other groups.

Definition 2.4. Let G be a group and $\Omega \neq \emptyset$ be a set. A **(group) action** of G on Ω is a homomorphism $G \to \operatorname{Sym}(\Omega)$. The **degree** of the action is $|\Omega|$.

If we have an action, we say that G *acts* on Ω. Immediately, we see that the image of an action is a permutation group; an action gives a way of describing how a group G permutes a set Ω in a way that respects the structure of G. If φ is an action as defined above, then $\varphi(g)$ is a permutation of Ω for each $g \in G$. If φ is fixed or implied, we usually write $\alpha^g := \alpha^{\varphi(g)}$ for the action of $\varphi(g)$ on $\alpha \in \Omega$. (Implicit in this notation is that we think of $g \in G$ as acting on elements of Ω from the right.) When we omit the action φ, its image $\varphi[G]$ is denoted G^Ω, which is a *permutation group* on Ω. By the first isomorphism theorem, $\varphi[G] \cong G/\ker\varphi$ is isomorphic to a quotient of G.

Note that since φ is a homomorphism, this translates to the property that

$$\alpha^{gh} = \alpha^{\varphi(gh)} = \alpha^{\varphi(g)\varphi(h)} = (\alpha^{\varphi(g)})^{\varphi(h)} = (\alpha^g)^h$$

for $g, h \in G$ and $\alpha \in \Omega$. Also, since $\varphi(1) = 1_{\operatorname{Sym}(\Omega)} = \mathrm{Id}_\Omega$, we see that $\alpha^1 = \alpha$ for $\alpha \in \Omega$. Indeed, one can verify that these two properties characterise actions of G on Ω.

Lemma 2.5. *The map $\varphi : G \to \operatorname{Sym}(\Omega)$ is an action of G on Ω if and only if (1), $\alpha^1 = \alpha$ and (2), $\alpha^{gh} = (\alpha^g)^h$ for all $g, h \in G$ and $\alpha \in \Omega$. (Recall the convention $\alpha^g := \alpha^{\varphi(g)}$.)* □

Another useful property of actions is that if $\alpha^g = \beta$ for $g \in G$ and $\alpha, \beta \in \Omega$, then $\beta^{g^{-1}} = \alpha$; this follows from the fact that $\varphi(g^{-1}) = \varphi(g)^{-1}$ for the group homomorphism φ. We now provide some examples of actions on groups.

Example 2.6 (trivial action). An element $g \in G$ **acts trivially** (on Ω) if $\alpha^g = \alpha$ for all $\alpha \in \Omega$, i.e. $g \mapsto 1 \in \operatorname{Sym}(\Omega)$. If every $g \in G$ acts trivially, then we have the **trivial action** on G, and we say that G **acts trivially** on Ω.

Example 2.7 (right regular action). Let G be a group and $\Omega = G$, the underlying set of G. Let $g \in G$ act on $\alpha \in G$ (via $\mathcal{R} : G \to \operatorname{Sym}(G)$) by $\alpha^g := \alpha g$. Then $\mathcal{R}$ is an action by Lemma 2.5: (1), we have $\alpha^1 = \alpha 1 = \alpha$ for $\alpha \in G$; and (2), for $g, h \in G$ and $\alpha \in G$, $\alpha^{gh} = \alpha gh = (\alpha g)h = (\alpha^g)^h$, so that $\mathcal{R}(gh) = \mathcal{R}(g)\mathcal{R}(h)$. This is the **right regular action** $\mathcal{R}$ on G; here G acts on itself by right-multiplication. The image $G^\Omega = \mathcal{R}[G] \leq \operatorname{Sym}(G)$ is the **right regular permutation representation** of G.

Example 2.8 (representations). Let G be a group and $\Omega = V$, a K-vector space with K a field. Let $\rho : G \to \operatorname{Sym}(V)$ be a homomorphism with $\rho[G] \leq \mathrm{GL}(V) = \operatorname{Aut}(V)$, the invertible linear maps $V \to V$. Then ρ is an action of G on V, but we typically write $\rho : G \to \mathrm{GL}(V)$ and call it a **representation** of G; these are studied in a branch of mathematics called representation theory, which analyses G using linear actions on a vector space, whose properties are well-known.

There is a natural notion of equivalence of actions on a fixed group G.

Definition 2.9. Two *actions* $\varphi, \tilde{\varphi}$ of G on $\Omega, \tilde{\Omega}$ are **equivalent** if there is a bijection $\tau : \Omega \to \tilde{\Omega}$ such that $\tau(\alpha^{\varphi(g)}) = \tau(\alpha)^{\tilde{\varphi}(g)}$ (or equivalently, $\tau(\alpha^g) = \tau(\alpha)^g$) for all $g \in G$ and $\alpha \in \Omega$.

This notion of equivalence says that applying φ then relabelling Ω via τ is the same as relabelling Ω via τ then applying $\tilde{\varphi}$. In other words, the following diagram commutes for all $g \in G$:

$$\begin{array}{ccc} \Omega & \xrightarrow{\varphi(g)} & \Omega \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ \tilde{\Omega} & \xrightarrow{\tilde{\varphi}(g)} & \tilde{\Omega} \end{array}$$

There is a similar notion of isomorphic permutation groups, where the natural action is preserved:

Definition 2.10. Two permutation groups $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\tilde{\Omega})$ are **permutation isomorphic** if there is a bijection $\tau : \Omega \to \tilde{\Omega}$ and an isomorphism $\psi : G \to H$ such that $\tau(\alpha^g) = \tau(\alpha)^{\psi(g)}$ for all $g \in G$ and $\alpha \in \Omega$.

The pair (τ, ψ) is a **permutation isomorphism** from G to H; then (τ^{-1}, ψ^{-1}) is a permutation isomorphism from H to G (so that permutation isomorphism is an equivalence relation). The condition on τ, ψ says that the following diagram commutes for all $g \in G$:

$$\begin{array}{ccc} \Omega & \xrightarrow{g \in G} & \Omega \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ \tilde{\Omega} & \xrightarrow{\psi(g) \in H} & \tilde{\Omega} \end{array}$$

In the special case that $G = H$ and $\psi = \mathrm{Id}_G$, then permutation isomorphism yields equivalence: for $g \in G$ and $\alpha \in \Omega$, since G, H are permutation isomorphic, we have $\tau(\alpha^g) = \tau(\alpha)^{\mathrm{Id}_G(g)} = \tau(\alpha)^g$ for all $g \in G$, so the actions are equivalent via τ.

Next, we define what it means for an action to be *faithful*.

Definition 2.11. An *action* φ of G on Ω is **faithful** if $\ker \varphi = 1$. In other words, if $\alpha^g = \alpha$ for all $\alpha \in \Omega$, then $g = 1$.

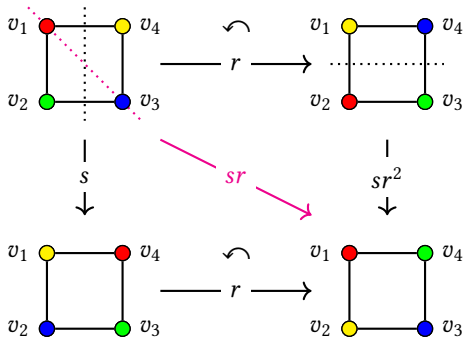
If φ is faithful, then 1 is the only element of G that does not permute any elements in Ω. This also says that G embeds into $\mathrm{Sym}(\Omega)$ via φ: $G \cong G/1 = G/\ker\varphi \cong G^\Omega$ by the first isomorphism theorem. A natural question arises: is there a faithful action for any group G? If this were true, then every group would be isomorphic to a permutation group. This is answered in the affirmative by Cayley's theorem, which is part of Fact 2 in [3].

Theorem 2.12 (Cayley). *Let G be a group and $\mathcal{R}$ be the right regular action of G. Then G is isomorphic to the permutation group $\mathcal{R}[G] \leq \mathrm{Sym}(G)$. In the case that $|G| = n$ is finite, then G is isomorphic to a subgroup of* $\mathrm{Sym}(n)$.

Proof. Recall the right regular action $\mathcal{R}$ as defined in Example 2.7. From above, it suffices to show that $\mathcal{R}$ is faithful: let $\alpha \in G$ and suppose $\alpha^g = \alpha$. Then $\alpha g = \alpha$, so left multiplication by α^{-1} gives $g = 1$, as required. □

Example 2.13 (natural action). Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group. The **natural action** $\varphi : G \to \mathrm{Sym}(\Omega)$ of G on Ω is given by the inclusion map $g \mapsto g$ (so that for $\alpha \in \Omega$ and $g \in G$, $\alpha^{\varphi(g)} := \alpha^g$, the image of α under g); this is faithful. (Note that the image $G^\Omega \leq \mathrm{Sym}(\Omega)$ of an arbitrary G-action on Ω takes the natural action; it yields a homomorphism $G \to G^\Omega$, and G^Ω is a *homomorphic image* of G that acts faithfully on Ω.)

Example 2.14. Consider $D_8 = \langle r, s \rangle = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, the dihedral group of order 8. It "is" the symmetry group of a square S (with vertices $V = \{v_1, v_2, v_3, v_4\}$ labelled anticlockwise) in the following sense: let $r \mapsto (v_1, v_2, v_3, v_4)$ and $s \mapsto (v_1, v_4)(v_2, v_3)$ generate the (faithful) action of D_8 on V. Then r represents anticlockwise rotation by $\pi/2$ and s represents horizontal reflection; the product in D_8 mimics composition of these symmetries. For example, $v_4^{sr} = (v_4^s)^r = v_1^r = v_2$. Below is a diagram that visualises this D_8-action on V; the element $g \in D_8$ sends vertex v_i to v_i^g (follow the colours; note that $sr \mapsto (v_2, v_4)$ and $sr^2 \mapsto (v_1, v_2)(v_3, v_4)$).



By renaming elements of V, we see that this action is equivalent to the action of D_8 on the set $\{1,2,3,4\}$ defined by $r \mapsto (1,2,3,4)$ and $s \mapsto (1,4)(2,3)$, so we see that D_8 is isomorphic to a subgroup of $\mathrm{Sym}(4)$.

Now let $D = \{d_1, d_2\}$ be the set of diagonals of S, where d_1 joins v_1 and v_3, and d_2 joins v_2 and v_4. A corresponding action φ of D_8 on D is given by $\varphi(r) = \varphi(s) = (d_1, d_2)$: for example, $d_1^{rs} = (d_1^r)^s = d_2^s = d_1$. Then the kernel of φ is $\{1, r^2, sr, sr^3\} \trianglelefteq D_8$; the action is not faithful.

Now consider the corresponding action of D_8 on $\Omega = \{S, v\}$, where v is the centre of S. Every symmetry of S fixes S and its centre, so $S^g = S$ and $v^g = v$ for all $g \in D_8$, so D_8 acts trivially on Ω.

Example 2.15 (quotient action). Let G act on Ω via φ. If $N \trianglelefteq G$ is contained in $\mathrm{Ker}\,\varphi$, then the quotient group G/N acts on Ω by $\alpha^{gN} := \alpha^g$ for $\alpha \in \Omega$ and $gN \in G/N$. This is well-defined: if $\alpha \in \Omega$ and $gN = hN$ then $gh^{-1} \in N$ (since N is normal in G), so $gh^{-1} \in \ker\varphi$, so $\alpha^{gh^{-1}} = \alpha$, which implies $\alpha^g = \alpha^h$. Also, we verify that $\alpha^{1_{G/N}} = \alpha^{1N} = \alpha^1 = \alpha$ and $(\alpha^{gN})^{hN} = (\alpha^g)^h = \alpha^{gh} = \alpha^{ghN} = \alpha^{(gN)(hN)}$ for $\alpha \in \Omega$ and $gN, hN \in G/N$.

Note that the G/N-action $\hat{\varphi}$ on Ω is faithful if and only if $N = \mathrm{Ker}\,\varphi$. This is because

$$\mathrm{Ker}\,\hat{\varphi} = \{gN \in G/N : \alpha^{gN} = \alpha^g = \alpha \text{ for all } \alpha \in \Omega\} = \{gN \in G/N : g \in \mathrm{Ker}\,\varphi\} = \mathrm{Ker}\,\varphi/N,$$

and $\mathrm{Ker}\,\varphi/N = 1$ if and only if $N = \mathrm{Ker}\,\varphi$. (Then if $K = \mathrm{Ker}\,\varphi$, then G/K and $G^\Omega \leq \mathrm{Sym}(\Omega)$ are permutation isomorphic, via the identity relabelling $\tau : \Omega \to \Omega$ and the natural isomorphism $\psi : G/K \to G^\Omega$ (see Theorem 2.3), $gK \mapsto \varphi(g)$, since for $\alpha \in \Omega$ and $gK \in G/K$, we have $\tau(\alpha^{gK}) = \alpha^{gK} = \alpha^{\varphi(g)} = \tau(\alpha)^{\psi(gK)}$.)

Orbits and stabilisers

We define orbits, stabilisers and fixed point sets for an action of G on Ω, which are fundamental to the study of actions.

Definition 2.16. Let G act on Ω.

(i) The **orbit** of $\alpha \in \Omega$ is $\alpha^G = \{\alpha^g : g \in G\} \subseteq \Omega$.

(ii) The **pointwise stabiliser** of $\Delta \subseteq \Omega$ is $G_{(\Delta)} = \{g \in G : \alpha^g = \alpha \text{ for all } \alpha \in \Delta\} \subseteq G$.

(iii) The **fixed point set** of $g \in G$ is $\mathrm{Fix}_\Omega(g) = \{\alpha \in \Omega : \alpha^g = \alpha\} \subseteq \Omega$, dually to the stabiliser.

In (ii) above, if $\Delta = \{\alpha\}$ then we write $G_\alpha = \{g \in G : \alpha^g = \alpha\} \subseteq G$ for the **(point) stabiliser** of $\alpha \in \Omega$. If $\Delta = \{\alpha_1, \ldots, \alpha_k\}$, then we may write $G_{(\Delta)} = G_{\alpha_1,\ldots,\alpha_k}$. For $\alpha \in \Delta$, it is often useful to note that $G_{(\Delta)} = (G_{(\Delta\setminus\alpha)})_\alpha$. The stabiliser of an element of Ω is a *subgroup* of G:

Proposition 2.17. *Let G act on Ω and $\alpha \in \Omega$. Then $G_\alpha \leq G$.*

Proof. We use the subgroup criterion. First $1 \in G_\alpha$, since $\alpha^1 = \alpha$. Let $g, h \in G_\alpha$; then

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

so $gh^{-1} \in G_\alpha$. The third equality follows from applying h^{-1} to the equality $\alpha^h = \alpha$. □

Since the intersection of subgroups is a subgroup and $G_{(\Delta)} = \bigcap_{\alpha\in\Delta} G_\alpha$, we get the following:

Corollary 2.18. *Let G act on Ω and $\Delta \subseteq \Omega$. Then $G_{(\Delta)} \leq G$.* □

Proposition 2.19. *Let G act on Ω. Then the kernel of the action is $G_{(\Omega)} = \bigcap_{\alpha\in\Omega} G_\alpha \trianglelefteq G$.*

Proof. Let K be the kernel, which contains the elements of G which map to Id_Ω under the action. Then $g \in K$ if and only if $\alpha^g = \alpha$ for all $\alpha \in \Omega$, so $K = G_{(\Omega)}$. The result then follows from Corollary 2.18. □

The orbits of G on Ω partition Ω: indeed, if we define a relation on Ω by saying $\alpha, \beta \in \Omega$ are related when some orbit contains both α and β, this is an equivalence relation, and the orbits are the equivalence classes.

Example 2.20. Let G, H be groups such that G acts on Ω and H acts on $\tilde{\Omega}$. Then $G \times H$ acts on $\Omega \times \tilde{\Omega}$ in a natural way: $(\alpha, \beta)^{(g,h)} = (\alpha^g, \beta^h)$ for $(\alpha, \beta) \in \Omega \times \tilde{\Omega}$ and $(g, h) \in G \times H$ (this is easy to verify).

For $(\alpha, \beta) \in \Omega \times \tilde{\Omega}$, we can see that its orbit is $(\alpha, \beta)^{G\times H} = \{(\alpha^g, \beta^h) : g \in G, h \in H\} = \alpha^G \times \beta^H$, and its stabiliser is

$$(G \times H)_{(\alpha,\beta)} = \{(g, h) \in G \times H : \alpha^g = \alpha, \beta^h = \beta\} = G_\alpha \times H_\beta.$$

Example 2.21. (a) Recall the right regular action $\mathcal{R}$ on G from Example 2.7, and let $\alpha \in G$. Then the orbit of α is $\alpha^G = \{\alpha^g = \alpha g : g \in G\} = G$. The stabiliser of α is $G_\alpha = \{g \in G : \alpha g = \alpha^g = \alpha\} = 1$. The fixed point set of $g \in G$ is $\mathrm{Fix}_G(g) = \{\alpha \in G : \alpha g = \alpha^g = \alpha\}$; this is all of G if $g = 1$, and empty otherwise. Note that if G is finite, we see that $|\alpha^G||G_\alpha| = |G||1| = |G|$.

(b) When $G \leq K$, we can extend $\mathcal{R}$ to a G-action $\mathcal{R}^K : G \to \mathrm{Sym}(K)$ on K, by $\alpha^g = \alpha g$ for $\alpha \in K$ and $g \in G$. Then the orbits are the left cosets αG of G in K, so by Lagrange's theorem, there are $|K : G|$ orbits, each with size $|G|$.

Example 2.22. Recall from Example 2.14 the action φ of D_8 on $D = \{d_1, d_2\}$, the set of diagonals of a square S. The orbit of d_1 is $d_1^{D_8} = \{d_1, d_2\} = D$ since $d_1^1 = d_1$ and $d_1^r = d_2$. The stabiliser of d_1 is $(D_8)_{d_1} = \{1, r^2, sr, sr^3\}$. From this, we see that $|d_1^{D_8}||(D_8)_{d_1}| = 2 \cdot 4 = 8 = |D_8|$. Note that the fixed point sets of $g = 1, r^2, sr, sr^3$ are all of D, but the fixed point sets of $g = r, r^3, s, sr^2$ are empty.

Since G_α is a subgroup of G, we can consider its (right) cosets. Let $G_\alpha\backslash G$ denote the set of its right cosets in G. From the previous examples, we see a pattern that for any $\alpha \in \Omega$, we have $|G| = |\alpha^G||G_\alpha|$, at least when G is finite. This is made precise for any group G, possibly infinite, by the *orbit-stabiliser theorem*, which gives a bijection of $G_\alpha\backslash G$ with the orbit of α, i.e. a bijective correspondence between (right) cosets of the stabiliser of α and elements in the orbit of α:

Theorem 2.23 (orbit-stabiliser (OST); Fact 1 in [3]). *Let G act on Ω and let $\alpha \in \Omega$. The map $G_\alpha\backslash G \to \alpha^G$ given by $G_\alpha g \mapsto \alpha^g$ is a bijection. So, the index of G_α in G is $|G : G_\alpha| = |\alpha^G|$, and $|G| = |\alpha^G||G_\alpha|$ by Lagrange's theorem.*

Proof. The map is well-defined, since if $G_\alpha g = G_\alpha h$, then $gh^{-1} \in G_\alpha$, so $\alpha^{gh^{-1}} = \alpha$; applying h results in $\alpha^g = \alpha^{gh^{-1}h} = \alpha^h$, as required. The map is injective: let $g, h \in G$ and suppose $\alpha^g = \alpha^h$. Then $\alpha^{gh^{-1}} = \alpha^1 = \alpha$, so $gh^{-1} \in G_\alpha$, so $G_\alpha g = G_\alpha h$. The map is surjective: let $\alpha^g \in \alpha^G$ where $g \in G$; clearly $G_\alpha g \mapsto \alpha^g$. So the map is a bijection. □

Note that G_α may not be a normal subgroup, so we may not be able to talk about quotient groups. But the intersection of stabilisers is normal in G by Proposition 2.19, as the kernel of the action.

Conjugacy, centralisers and normalisers

Another important action of G on $\Omega = G$ is *conjugation*. Recall that an **automorphism** of G is an isomorphism $G \to G$; the set of automorphisms form a group, $\mathrm{Aut}(G)$, under composition.

Example 2.24 (conjugation). For $\alpha \in G$, **conjugation** of α by $g \in G$ gives the element $\alpha^g := g^{-1}\alpha g$. This defines an action of G on $\Omega = G$: $\alpha^1 = 1^{-1}\alpha 1 = \alpha$ and $\alpha^{gh} = (gh)^{-1}\alpha gh = h^{-1}(g^{-1}\alpha g)h = (\alpha^g)^h$ for $\alpha, g, h \in G$.

The orbit of $\alpha \in G$ is the **conjugacy class** $\mathrm{Cl}_G(\alpha) := \{g^{-1}\alpha g : g \in G\}$. Elements in the same conjugacy class are said to be **conjugate** and have the same order, since for $g \in G$ the **inner automorphism** $G \to G$ given by $\alpha \mapsto g^{-1}\alpha g$ is an automorphism: the inverse map is clearly given by $\alpha \mapsto g\alpha g^{-1}$ (which is conjugation by g^{-1}), and we have $g^{-1}\alpha\beta g = (g^{-1}\alpha g)(g^{-1}\beta g)$ for $\alpha, \beta \in G$ (so it is an *endomorphism*). The set of inner automorphisms forms a group, $\mathrm{Inn}(G)$.

The stabiliser of $\alpha \in G$ is the **centraliser** of α: suppose $g \in G$ is such that $\alpha^g = g^{-1}\alpha g = \alpha$. Then $\alpha g = g\alpha$, so $G_\alpha = \{g \in G : \alpha g = g\alpha\} =: C_G(\alpha)$; this is the set of elements that commute with α. The OST then implies that $|\operatorname{Cl}_G(\alpha)| = |G|/|C_G(\alpha)|$ in the case that G is finite. (If G is *abelian*, then $C_G(\alpha) = G$, and it follows that G acts trivially on itself by conjugation.) The kernel of the action is the **centre** $Z(G) := \{g \in G : \alpha g = g\alpha \text{ for all } \alpha \in G\} \trianglelefteq G$.

We may also define conjugacy and associated notions for subgroups H of G; the discussion above then corresponds to the case that $H = 1 \leq G$.

Example 2.25. For a *subgroup* $H \leq G$, **conjugation** of H by $g \in G$ gives the subgroup $H^g = g^{-1}Hg = \{g^{-1}hg : h \in H\} \leq G$. This defines an action of G on the subgroups $\Omega = \{H : H \leq G\}$ of G.

Subgroups in the same orbit are said to be **conjugate (subgroups)** and are isomorphic: the inner automorphism described in Example 2.24 restricts to an isomorphism $H \to H^g$. However isomorphic subgroups need not be conjugate; if G is abelian, $H^G = \{H\}$ only, and in $G = \mathbb{Z}$ we know that $\mathbb{Z} \cong 2\mathbb{Z} \leq \mathbb{Z}$, for instance. In this context, the orbits are called **conjugacy classes (of subgroups)**.

The stabiliser of $H \leq G$ is the **normaliser** of H: suppose $g \in G$ is such that $H^g = g^{-1}Hg = H$. Then $Hg = gH$, so $G_H = \{g \in G : Hg = gH\} =: N_G(H)$; clearly $H \trianglelefteq N_G(H)$, and $N_G(H)$ is the largest subgroup of G with this property. The OST then implies $|G : N_G(H)|$ is the number of subgroups of G conjugate to H. The **centraliser** of H is $C_G(H) = \{g \in G : hg = gh \text{ for all } h \in H\} \subseteq N_G(H)$; we see that $C_G(G) = Z(G)$.

The notion of permutation isomorphism relates to conjugacy of subgroups in a special case.

Lemma 2.26. *Let $G, H \leq \operatorname{Sym}(\Omega)$ be permutation isomorphic via $\tau : \Omega \to \Omega$ and $\psi : G \to H$. Then G and H are conjugate subgroups.*

Proof. Let $\alpha \in \Omega$ and $g \in G$. Then $H = G^\tau$, where $\tau \in \operatorname{Sym}(\Omega)$: indeed, we have $\psi(g) = \tau^{-1}g\tau$ since

$$\tau(\alpha)^{\psi(g)} = \tau(\alpha^g) = \alpha^{g\tau} = \tau(\alpha)^{\tau^{-1}g\tau}.$$ fl

Recall that a **maximal subgroup** H of G is a subgroup $H < G$ such that $H < K \leq G$ implies $K = G$.

Lemma 2.27. *If $H < G$ is maximal, then H^g is maximal for all $g \in G$.*

Proof. Suppose for contradiction that H^g is not maximal; then there is $K \leq G$ with $H^g < K < G$. Clearly $K^{g^{-1}} < G$ (since $K \cong K^{g^{-1}}$ by Example 2.25), and moreover for $h \in H$ we have $h = g(g^{-1}hg)g^{-1} \in K^{g^{-1}}$ since $g^{-1}hg \in H^g < K$, so $H < K^{g^{-1}}$. This contradicts maximality of H. □

There is a useful result that relates the stabilisers of two elements in the same orbit: they are conjugate, thus isomorphic.

Proposition 2.28. *Let G act on Ω and let $g \in G$ and $\alpha \in \Omega$. Then $G_{\alpha^g} = (G_\alpha)^g$.*

Proof. If $h \in G_{\alpha^g}$, then $\alpha^{gh} = (\alpha^g)^h = \alpha^g$, so $\alpha^{ghg^{-1}} = \alpha$. Then $h = g^{-1}(ghg^{-1})g \in (G_\alpha)^g$, since we have $ghg^{-1} \in G_\alpha$. Conversely, if $h \in (G_\alpha)^g$, then $h = g^{-1}sg$ for some $s \in G_\alpha$, so $(\alpha^g)^h = (\alpha^g)^{g^{-1}sg} = \alpha^{sg} = \alpha^g$ since $\alpha^s = \alpha$. So $h \in G_{\alpha^g}$. □

Recall the condition for equality of right cosets: for $H \leq G$, $Hg = Hk$ if and only if $gk^{-1} \in H$. We consider one more special G-action.

Example 2.29 (right coset action). Let $H \leq G$. Then G acts on the **right coset space** $H\backslash G = \{H\alpha : \alpha \in G\}$ via right-multiplication: $(H\alpha)^g = H\alpha g$ for $\alpha, g \in G$. The orbit of $H\alpha$ is $(H\alpha)^G = \{(H\alpha)^g = H\alpha g : g \in G\} = H\backslash G$; there is only one orbit under the action. The stabiliser of $H\alpha$ is

$$G_{H\alpha} = \{g \in G : (H\alpha)^g = H\alpha g = H\alpha\} = \{g \in G : \alpha g \alpha^{-1} \in H\} = \alpha^{-1}H\alpha = H^\alpha.$$

From this, it follows that $\bigcap_{g\in G} H^g = \bigcap_{g\in G} G_{Hg} \trianglelefteq G$ by Proposition 2.19; this is called the **core** of H in G.

Transitivity and primitivity

Definition 2.30. An action of G on Ω is **transitive** if it has a single orbit, i.e. for any $\alpha, \beta \in \Omega$, there is $g \in G$ with $\alpha^g = \beta$, so that $\alpha^G = \Omega$. Otherwise, it is said to be **intransitive**.

An action is **n-transitive** if $|\Omega| \geq n$, and for any ordered lists $[\alpha_1, \ldots, \alpha_n]$ and $[\beta_1, \ldots, \beta_n]$ of *distinct points* in Ω, we have $[\beta_1, \ldots, \beta_n] = [\alpha_1^g, \ldots, \alpha_n^g]$ for some $g \in G$. Clearly n-transitivity implies $(n-1)$-transitivity for $n > 1$; 1-transitivity corresponds to transitivity.

Example 2.21 tells us that the right regular action is transitive. The action φ from Example 2.22 of D_8 on $D = \{d_1, d_2\}$, the set of diagonals of a square S, is transitive, since $d_1^{D_8} = D$.

Example 2.31. Consider the natural action of $\mathrm{Sym}(n)$ on the set $\Omega = [n]$. It is clearly transitive; for distinct $\alpha, \beta \in \Omega$, just consider $(\alpha, \beta) \in \mathrm{Sym}(n)$. In fact, it is n-transitive: for any ordered lists $[\alpha_1, \ldots, \alpha_n]$, $[\beta_1, \ldots, \beta_n]$ of distinct (thus all) elements of Ω, simply consider the permutation $g \in \mathrm{Sym}(n)$ such that $\alpha_i^g := \beta_i$.

Example 2.32. Consider the natural action of $\mathrm{Alt}(n)$ on the set $\Omega = [n]$. It is $(n-2)$-transitive: for any ordered lists $[\alpha_1, \ldots, \alpha_{n-2}]$, $[\beta_1, \ldots, \beta_{n-2}]$ of distinct elements of Ω with α_{n-1}, α_n and β_{n-1}, β_n the remaining elements of $[n]$, define the permutation $g \in \mathrm{Sym}(n)$ with $\alpha_i^g := \beta_i$ for $i = 1, \ldots, n$. If $g \in \mathrm{Alt}(n)$, we are done; else, g is an odd permutation, and consider the product $\tilde{g} = g(\beta_{n-1}, \beta_n) \in \mathrm{Alt}(n)$ with the transposition (β_{n-1}, β_n). Then $\tilde{g} \in \mathrm{Alt}(n)$ satisfies $\alpha_i^{\tilde{g}} := \beta_i$ for $i = 1, \ldots, n-2$.

An interesting observation is that for isomorphic permutation groups G, H, the group G may be transitive yet H may be intransitive. For example, $G = \mathrm{Alt}(3)$ is transitive, but is clearly isomorphic to the intransitive group $H = \{(), (1,2,3), (1,3,2)\} \leq \mathrm{Sym}(4)$, which has two orbits $\{1,2,3\}$ and $\{4\}$. Perhaps more surprisingly, the same can be said even if G and H have the same degree:

$$G = \{(), (1,2), (3,4), (1,2)(3,4)\} \quad \text{and} \quad H = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

are isomorphic as subgroups of $\mathrm{Sym}(4)$, yet G is intransitive while H is transitive, as shown in the following GAP code:

```
gap> G := Group([ (1,2), (3,4) ]);
Group([ (1,2), (3,4) ])
gap> IsTransitive( G );
false
gap> H := Group([ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]);
Group([ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ])
gap> IsTransitive( H );
true
gap> IsomorphismGroups( G, H );
[ (1,2), (3,4) ] -> [ (1,2)(3,4), (1,3)(2,4) ]
```

However, if we impose that $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\tilde{\Omega})$ are *permutation isomorphic* via $\tau : \Omega \to \tilde{\Omega}$ and $\psi : G \to H$, then transitivity is preserved. This is because if G is transitive, then for arbitrary $\tilde{\alpha}, \tilde{\beta} \in \tilde{\Omega}$ with $\tilde{\alpha} = \tau(\alpha)$ and $\tilde{\beta} = \tau(\beta)$ for some $\alpha, \beta \in \Omega$, there is $g \in G$ such that

$$\tilde{\beta} = \tau(\beta) = \tau(\alpha^g) = \tau(\alpha)^{\psi(g)} = \tilde{\alpha}^{\psi(g)},$$

so H is transitive. The converse direction follows since (τ^{-1}, ψ^{-1}) give a permutation isomorphism from H to G. From this, we conclude that the isomorphic groups $G, H \leq \mathrm{Sym}(4)$ as defined above are *not* permutation isomorphic; moreover, it suggests that for permutation groups, the stronger form of permutation isomorphism is needed to ensure that various properties are preserved.

Definition 2.33. An action of G on Ω is **regular** if it is transitive and $G_\alpha = 1$ for some element $\alpha \in \Omega$.

If φ is *regular* with $G_\alpha = 1$, then for $\beta \in \Omega$, $\beta = \alpha^g$ for some $g \in G$ by transitivity, and we have $G_\beta = 1^g = 1$ by

Proposition 2.28; the stabiliser of *any* element is trivial. Then by Proposition 2.19, any regular action is *faithful*. Moreover, to show that φ is not regular, it suffices to check that $G_\alpha \neq 1$ for some $\alpha \in \Omega$.

Indeed, the right regular action is regular, as seen in Example 2.21. By the OST, for a regular action, we must have $|G| = |\alpha^G||1| = |\Omega|$.

Example 2.34. The cyclic group $C_4 = \{1, r, r^2, r^3\}$ also acts on the vertices $V = \{v_1, v_2, v_3, v_4\}$ of a square S (labelled anticlockwise) by rotation: $r \mapsto (v_1, v_2, v_3, v_4)$. In this case, there is one orbit under the action (so it is transitive) and the stabiliser of each vertex is trivial, so it is regular, thus faithful. Indeed, we see that $|C_4| = |V|$.

It turns out that every regular action is equivalent to the right regular action:

Proposition 2.35. *G acts regularly on Ω via φ if and only if φ is equivalent to the right regular action $\mathcal{R}$ on G.*

Proof. Recall that the right regular action $\mathcal{R} : G \to \mathrm{Sym}(G)$. If G acts regularly, then fix $\alpha \in \Omega$ and define $\tau : \Omega \to G$ by the following: for $\beta \in \Omega$, by transitivity we have $\beta = \alpha^g$ for some $g \in G$; then set $\beta = \alpha^g \mapsto g$. This map is a bijection with well-defined inverse $\tau^{-1} : G \to \Omega$, $g \mapsto \alpha^g$; if $\beta = \alpha^g = \alpha^{\tilde{g}}$ for $\tilde{g} \in G$, then $\alpha^{g\tilde{g}^{-1}} = \alpha$, so $g\tilde{g}^{-1} = 1$ (since $G_\alpha = 1$ by regularity), i.e. $g = \tilde{g}$. Then for $\beta \in \Omega$, $\beta = \alpha^g$ for some $g \in G$, so for $h \in G$,

$$\tau(\beta^h) = \tau(\alpha^{gh}) = gh = \tau(\alpha^g)h = \tau(\beta)h = \tau(\beta)^h,$$

so φ is equivalent to $\mathcal{R}$ via τ.

Conversely, for $\alpha \in \Omega$, if φ is equivalent to $\mathcal{R}$ via $\tau : \Omega \to G$, then

$$G_\alpha = \{g \in G : \alpha^g = 1\} = \{g \in G : \tau(\alpha^g) = \tau(\alpha)\} = \{g \in G : \tau(\alpha)g = \tau(\alpha)^g = \tau(\alpha)\} = 1,$$

so φ is regular. (The second equality follows from τ being a bijection, and the third from equivalence of φ and $\mathcal{R}$.) □

Definition 2.36. If G acts on Ω, then a nonempty subset $\Delta \subseteq \Omega$ is a **block** under the action, if $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$ for all $g \in G$, where $\Delta^g := \{\alpha^g : \alpha \in \Delta\}$. The block is **nontrivial** if $|\Delta| > 1$ and $\Delta \neq \Omega$.

Clearly every singleton in Ω is a (trivial) block. Also, Ω is a block. Orbits of any action are clearly blocks since for $\alpha \in \Omega$, $(\alpha^G)^g = \{\alpha^{hg} : h \in G\} = \alpha^G$. We usually consider blocks only for transitive actions, i.e. actions with one orbit (as G acts on each orbit, as seen below).

If $\Delta \subseteq \Omega$ is a block, G may not act on Δ, as if $\Delta^g \cap \Delta = \emptyset$ for $g \in G$, then for $\alpha \in \Delta$, $\alpha^g \notin \Delta$. But the following lemma shows that there is a subgroup of G that acts on Δ.

Lemma 2.37. *If G acts on Ω and $\Delta \subseteq \Omega$, then*

(a) for $g, h \in G$, $\Delta^{gh} = (\Delta^g)^h$, and

*(b) the **setwise stabiliser** $G_\Delta := \{g \in G : \Delta^g = \Delta\} \leq G$ acts on Δ with kernel $G_{(\Delta)} \trianglelefteq G_\Delta$.*

The action $\varphi : G \to \mathrm{Sym}(\Omega)$ relates to the action $\tilde{\varphi} : G_\Delta \to \mathrm{Sym}(\Delta)$ by $\alpha^{\varphi(g)} = \alpha^{\tilde{\varphi}(g)} \in \Delta$ for $\alpha \in \Delta$ and $g \in G_\Delta$. (Since $\Delta \subseteq \Omega$, $\mathrm{Sym}(\Delta)$ embeds naturally into $\mathrm{Sym}(\Omega)$ via $g \mapsto \tilde{g} \in \mathrm{Sym}(\Omega)$, where $\alpha^{\tilde{g}} = \alpha^g$ for $\alpha \in \Delta$, else $\alpha^{\tilde{g}} = \alpha$.)

Proof. (a) We have $\beta \in \Delta^{gh}$ if and only if $\beta = \alpha^{gh}$ for some $\alpha \in \Delta$, if and only if $\beta = (\alpha^g)^h$ with $\alpha \in \Delta$ and $\alpha^g \in \Delta^g$, if and only if $\beta \in (\Delta^g)^h$.

(b) For $g, h \in G_\Delta$, we have $\Delta^{gh} = (\Delta^g)^h = \Delta^h = \Delta$, so $gh \in G_\Delta$. Similarly, we have $\Delta^{g^{-1}} = (\Delta^g)^{g^{-1}} = \Delta^1 = \Delta$, so $g^{-1} \in G_\Delta$. So $G_\Delta \leq G$, by the subgroup criterion. Then G_Δ acts on Δ since the associated action $\tilde{\varphi}$ is well-defined.

Note that that $G_{(\Delta)} \subseteq G_\Delta$ since if $\alpha^g = \alpha$ for all $\alpha \in \Delta$, then $\Delta^g = \Delta$. Then the kernel of the G_Δ-action on Δ is $\{g \in G_\Delta : \alpha^g = \alpha \text{ for all } \alpha \in \Delta\} = G_{(\Delta)}$, so $G_{(\Delta)} \trianglelefteq G_\Delta$. □

Remark 2.38. For G-actions (on Ω) and fixed $\alpha \in \Omega$, setting $\Delta = \alpha^G$ gives $G_\Delta = G$ (since $\Delta^g = (\alpha^G)^g = \alpha^G = \Delta$ for all $g \in G$), so G acts on α^G by Lemma 2.37(b). If the action is intransitive, then $\alpha^G \neq \Omega$, and G acts on a strict subset of Ω; the image of the restricted G-action embeds into the image of the original G-action.

Thus, when classifying permutation groups, it suffices to consider transitive groups. Suppose G acts on Ω via φ. Partition $\Omega = \bigsqcup_{i\in I} \Omega_i$, where each Ω_i is a G-orbit. Then for each $i \in I$, G acts transitively on Ω_i via $\varphi_i : G \to \mathrm{Sym}(\Omega_i)$, as in Remark 2.38. Conversely, suppose G acts transitively on Ω_i via φ_i for $i \in I$. Then, setting $\Omega = \bigsqcup_{i\in I} \Omega_i$ as the disjoint union, we may construct a G-action $\varphi : G \to \mathrm{Sym}(\Omega)$ by the following: for $\alpha \in \Omega$ and $g \in G$, we have $\alpha \in \Omega_i$ for unique $i \in I$, and then we set $\alpha^{\varphi(g)} = \alpha^{\varphi_i(g)} \in \Omega_i$. This constructs every intransitive G-action on Ω, and thus every intransitive group $G \leq \mathrm{Sym}(\Omega)$ where we take the natural action. We use this construction in Example 4.9.

Another important property of group actions is *primitivity*.

Definition 2.39. A transitive action of G on Ω is **primitive** if there are no nontrivial blocks under the action; otherwise it is **imprimitive**.

For a *transitive* action, the distinct *translates* Δ^g of a block Δ *partition* Ω (either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$); the set $\Sigma = \{\Delta^g : g \in G\}$ of these translates (which are blocks themselves) is a **block system** for G. So the condition of primitivity for a transitive action is equivalent to *not* preserving a nontrivial partition of Ω (otherwise we would have a nontrivial block). Clearly $|\Delta| = |\Delta^g|$, so all blocks in a block system have the same size; if $|\Omega|$ is finite, then $|\Delta|$ divides $|\Omega|$. So if the action of G on Ω is transitive and $|\Omega|$ is prime, then every block has size 1 or size $|\Omega|$ and is thus trivial, so the action is primitive. If a block system comprises nontrivial blocks, then it is also called a **system of imprimitivity**; the corresponding action is imprimitive.

If a transitive G-action on Ω has a block system $\Sigma = \{\Delta_0^g : g \in G\}$ for some block $\Delta_0 \subseteq \Omega$, then G acts transitively on Σ via $\hat{\varphi}$ in the expected way: for $\Delta \in \Sigma$, $\Delta^{\hat{\varphi}(g)} := \Delta^g$. This follows from the fact that $\Delta^1 = \Delta$ and $\Delta^{gh} = (\Delta^g)^h$ (which is Lemma 2.37(a)). In particular, this applies if Σ is a system of imprimitivity; if Σ is *maximal* (in the sense that Δ_0 is maximal with respect to inclusion: if $\tilde{\Delta}$ is a block such that $\Delta_0 \subsetneq \tilde{\Delta} \subseteq \Omega$ then $\tilde{\Delta} = \Omega$), then G acts primitively on Σ.

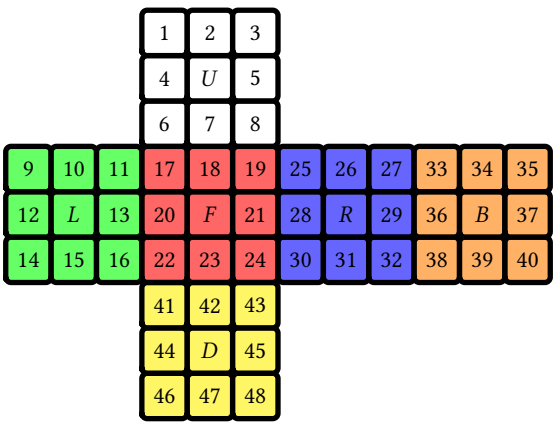
Lemma 2.40. *Let G act transitively on Ω and let Δ be a nontrivial block under the action. If the system of imprimitivity $\Sigma = \{\Delta^g : g \in G\}$ is maximal, then G acts primitively on Σ (under the induced action on blocks).*

Proof. First we prove that if $\Gamma = \{\Delta^s : s \in S_\Gamma\}$ is a block under the action on Σ, then $\Delta_\Gamma = \bigcup_{s\in S_\Gamma} \Delta^s$ is a block under the action on Ω. Observe that $\Delta_\Gamma^g = \bigcup_{t\in S_\Gamma} \Delta^{tg}$, so if $\Gamma^g = \Gamma$, then for $s \in S_\Gamma$, $\Delta^s = \Delta^{tg}$ for some $t \in S_\Gamma$, and $\Delta_\Gamma^g = \Delta_\Gamma$. If $\Gamma^g \cap \Gamma = \emptyset$, then $\Delta^s \cap \Delta^{tg} = \emptyset$ for all $s, t \in S_\Gamma$, so $\Delta_\Gamma^g \cap \Delta_\Gamma = \emptyset$; this proves Δ_Γ is a block.

If Σ is maximal, then suppose Γ is a nontrivial block under the action on Σ. Then Δ_Γ is a block under the action on Ω that properly contains Δ, and by maximality of Δ with respect to inclusion (of blocks), we have $\Delta_\Gamma = \Omega$, so that $\Gamma = \Sigma$. Thus there are no nontrivial blocks under the action on Σ, and G acts primitively on Σ. □

Analysing the kernel of this action on blocks tells us the elements of G that fix every Ω-block $\Delta \in \Sigma$ setwise. By a similar argument to Proposition 2.19, we see that it is the intersection of the *setwise stabilisers* G_Δ for $\Delta \in \Sigma$.

Example 2.41 (Rubik's group). This action on blocks is useful in analysing permutation groups such as the Rubik's group G of degree 48 and its action on the Rubik's cube, where we label each small cube (except the centres) by a number from 1 to 48, as below.



To mimic operations on the cube, we define $G = \langle U, L, F, R, B, D\rangle \leq \mathrm{Sym}(48)$ where

- $U = (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)$,
- $L = (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)$,
- $F = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)$,
- $R = (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)$,
- $B = (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)$, and
- $D = (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)$.

Then for $g \in G$, applying the operation g moves sticker i to the position of sticker i^g; this is the natural action. See appendix for GAP code related to implementation. Note that each generator of G above has order 4 (recall that the order of a permutation is the lcm of the cycle lengths), and by computing

$$RUR^{-1}U^{-1} = (1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)$$

and

$$RU = (1,3,38,43,11,35,27,32,30,17,9,33,48,24,6)(2,5,36,45,21,7,4)(8,25,19)(10,34,26,29,31,28,18),$$

we see that the commutator $RUR^{-1}U^{-1}$ and the operation RU have orders $\operatorname{lcm}(6,3,6,3) = 6$ and $\operatorname{lcm}(15,7,3,7) = 105$ respectively; this is the smallest number of times these operations must be applied to return to the initial state.

The following analysis on G is adapted from [1]. Firstly, GAP computes that $|G| = 43\,252\,003\,274\,489\,856\,000 \approx 4.3 \cdot 10^{19}$ Now, the Rubik's group has two orbits under its natural action:

$$1^G = \{1,6,40,27,8,35,16,41,32,25,48,3,11,24,46,33,43,17,30,14,19,9,22,38\}$$

and

$$2^G = \{2,5,12,7,36,10,47,4,28,45,34,13,29,44,20,42,26,21,37,15,31,18,23,39\},$$

representing corner and edge stickers respectively. So G acts transitively on the 24 corner stickers, and we get a homomorphism $G \to \operatorname{Sym}(1^G)$ with image of size 88 179 840; for instance, under this homomorphism,

$$F = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)$$
$$\mapsto (17,19,24,22)(6,25,43,16)(8,30,41,11) \in \operatorname{Sym}(1^G).$$

(Note that GAP relabels the elements of 1^G to $[24]$, when using `ActionHomomorphism` to get the action on the orbit.)

Then we may use GAP to check that the 3 stickers in each corner form a maximal block, and

$$\Sigma = \{\{1,35,9\},\{6,11,17\},\{40,46,14\},\{27,3,33\},\{8,25,19\},\{16,41,22\},\{32,48,38\},\{24,43,30\}\}$$

is a maximal system of imprimitivity that partitions 1^G. So by Lemma 2.40, G acts primitively on Σ (the 8 corners themselves) under the action on blocks, giving a homomorphism $G \to \operatorname{Sym}(\Sigma)$. For instance,

$$F = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)$$
$$\mapsto (\{6,11,17\},\{8,25,19\},\{24,43,30\},\{16,41,22\}) \in \operatorname{Sym}(\Sigma),$$

which matches our intuition on the diagram above. It can be shown that the image of this action is $\operatorname{Sym}(\Sigma) \cong \operatorname{Sym}(8)$ (i.e. the action is surjective), since it has order $40\,320 = 8!$; thus, we can permute the corners (ignoring *orientation*) in any way we want on a Rubik's cube. (We discuss this more in Example 5.22.)

The centre of G (see Example 2.24) is the subgroup of operations that commute with any other operation. In [1], GAP is used to show that the centre of G is

$$Z(G) = \langle (2,34)(4,10)(5,26)(7,18)(12,37)(13,20)(15,44)(21,28)(23,42)(29,36)(31,45)(39,47) \rangle,$$

generated by an operation that flips all 12 edges simultaneously, which has order 2; thus the centre contains only one nontrivial element.

By saying G^Ω is transitive, regular or primitive, we mean that the action of G on Ω is transitive, regular or primitive. When $G \leq \operatorname{Sym}(\Omega)$ is a permutation group, if we consider the natural action of G on Ω as defined in Example 2.13, we

simply say that G is **transitive**, **regular** or **primitive** (when the action is). Thus, by Lemma 2.40, if G acts transitively on Ω and Σ is a maximal system of imprimitivity, then the image of the action is a primitive (permutation) group.

Recall that from above, if $G \leq \mathrm{Sym}(\Omega)$ is regular, then its order is equal to its degree (i.e. $|G| = |\Omega|$). The following shows that the converse also holds for transitive permutation groups:

Proposition 2.42. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive. If the order of G equals its degree (i.e. $|G| = |\Omega|$), then G is regular.*

Proof. For $\alpha \in \Omega$, the orbit-stabiliser theorem implies $|G_\alpha||\alpha^G| = |G| = |\Omega|$. But G is transitive, so $\alpha^G = \Omega$, which gives $|G_\alpha| = 1$, thus $G_\alpha = 1$, and G is regular. □

Example 2.43. Consider the natural action of $\mathrm{Sym}(n)$ on the set $\Omega = [n]$. It is clearly primitive for $n = 1, 2$. Let $n \geq 3$ and $\Delta \subsetneq \Omega$ with $|\Delta| > 1$, say $\Delta = \{\alpha_1, \ldots, \alpha_d\}$ with $\beta \notin \Delta$. Then the transposition $g = (\alpha_1, \beta) \in \mathrm{Sym}(n)$ is such that $\Delta^g = \{\beta, \alpha_2, \ldots, \alpha_d\} \neq \Delta$ and $\Delta^g \cap \Delta \neq \emptyset$, so Δ is not a block under the action. So $\mathrm{Sym}(n)$ is primitive for any n.

Example 2.44. Consider again the example of D_8 acting transitively on the vertices $V = \{v_1, v_2, v_3, v_4\}$ of a square, labelled anticlockwise (see Example 2.14). It preserves one nontrivial block system: $\{\{v_1, v_3\}, \{v_2, v_4\}\}$, since any symmetry of the square leaves opposite vertices opposite. Hence, this action is imprimitive.

Proposition 2.45. *A 2-transitive action of G on Ω is primitive.*

Proof. Let $\Delta \subseteq \Omega$ be such that $|\Delta| > 1$ and $\Delta \neq \Omega$. Then take $[\alpha_1, \alpha_2]$ distinct points in Δ and $[\beta_1, \beta_2]$ with $\beta_1 = \alpha_1$ and $\beta_2 \in \Omega \setminus \Delta$. Since G^Ω is 2-transitive, there is $g \in G$ such that $[\beta_1, \beta_2] = [\alpha_1^g, \alpha_2^g]$. But $\beta_1, \beta_2 \in \Delta^g$, so $\Delta^g \neq \Delta$ and $\Delta^g \cap \Delta \neq \emptyset$, thus Δ is not a nontrivial block. So there are no nontrivial blocks under the action, and it is primitive. □

This gives an alternative proof that $\mathrm{Sym}(n)$ is primitive for $n \geq 2$, since it is n-transitive (thus 2-transitive). Moreover, it shows that $\mathrm{Alt}(n)$ is primitive for $n \geq 4$, since it is $(n-2)$-transitive (thus 2-transitive). The following result, which we state without proof, relates primitivity to stabilisers; it is Corollary 1.5A in [12].

Proposition 2.46. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive with $|\Omega| \geq 2$. Then G is primitive if and only if G_α is a maximal subgroup of G for all $\alpha \in \Omega$.*

Since stabilisers of a transitive group $G \leq \mathrm{Sym}(\Omega)$ are all conjugate by Proposition 2.28 (as there is only one orbit), G_α is a maximal subgroup of G for some $\alpha \in \Omega$ if and only if G_β is maximal for all $\beta \in \Omega$. (This follows from the conjugate of a maximal subgroup being maximal, Lemma 2.27.) Thus, one way to verify primitivity for G is to check transitivity (by computing an orbit), and then checking if some stabiliser G_α is a maximal subgroup.

Another corollary of this result is that a regular permutation group $G \leq \mathrm{Sym}(\Omega)$ is primitive if and only if $|G|$ is prime (for $\alpha \in \Omega$, $G_\alpha = 1$ is a maximal subgroup of G if and only if G is cyclic of prime order, if and only if $|G|$ is prime). Thus, $\mathrm{Alt}(3)$ is primitive, as it is transitive (consider $(1, 2, 3) \in \mathrm{Alt}(3)$) and regular by Proposition 2.42 since $|\mathrm{Alt}(3)| = 3!/2 = 3$. Trivially, $\mathrm{Alt}(1) = 1$ and $\mathrm{Alt}(2) = 1$ are also primitive, so we see that $\mathrm{Alt}(n)$ is primitive for all n.

We present one more result on transitivity and primitivity concerning the induced action of a normal subgroup:

Proposition 2.47 (Theorem 1.6A in [12]). *Let G act transitively on Ω via φ and $N \trianglelefteq G$. Then:*

(a) if Δ is an N-orbit and $g \in G$, then Δ^g is an N-orbit; moreover, these are all the N-orbits (for any given Δ);

(b) the N-orbits form a block system for G; and

(c) if G acts primitively on Ω, then N acts transitively on Ω, or N acts trivially on Ω (and $N \leq \mathrm{Ker}\,\varphi$).

Proof. (a) Write $\Delta = \alpha^N$ for some $\alpha \in \Omega$. Then for $g \in G$, $\Delta^g = \{\beta^g : \beta \in \Delta\} = \{\alpha^{ng} : n \in N\} = \{\alpha^{gg^{-1}ng} : n \in N\} = \{(\alpha^g)^k : k \in N\} = (\alpha^g)^N$ since $N \trianglelefteq G$.

Now suppose $\tilde{\Delta}$ is an N-orbit, so $\tilde{\Delta} = \tilde{\alpha}^N$ for some $\tilde{\alpha} \in \Omega$. Then since G^Ω is transitive, $\tilde{\alpha} = \alpha^g$ for some $g \in G$, so $\tilde{\Delta} = (\alpha^g)^N = \Delta^g$ from before.

(b) Let Δ be an N-orbit, thus a block for G, and set $\Sigma = \{\Delta^g : g \in G\}$ which is a block system. Since N is normal, Δ^g is an N-orbit by part (a), and by transitivity of G^Ω, Σ covers all of Ω and is precisely all N-orbits.

(c) Since G^Ω is primitive, every block is trivial, so using part (b), if Δ is an N-orbit, then $\Delta = \Omega$ (in which case N^Ω is transitive) or $|\Delta| = 1$ (from which every N-orbit has size 1, thus N acts trivially on Ω). □

If $G \leq \mathrm{Sym}(\Omega)$ is a primitive permutation group (which acts on $\mathrm{Sym}(\Omega)$ by inclusion), then for $N \trianglelefteq G$, if N acts trivially on $\mathrm{Sym}(\Omega)$ then the inclusion map must be trivial, thus $N = 1$. Thus if N is a nontrivial normal subgroup of a primitive group G, then N is transitive.

2.2 Bases and stabiliser chains

In this section, we assume that $G \leq \mathrm{Sym}(\Omega)$ is a (finite) permutation group, and that G acts on Ω naturally (as in Example 2.13). A base is a subset of Ω that G fixes pointwise. Since stabilisers are subgroups, we can take successive stabilisers to get a subgroup series. In 1970, Sims introduced in [27] the notion of stabiliser chains and strong generating sets (generating sets which respect the base and stabiliser chain structure), which develops these ideas. Some definitions are taken from [3].

Definition 2.48. Consider the sequence $B = [\beta_1, \ldots, \beta_r]$ of distinct elements of Ω. Let $G^0 := G$ and

$$G^i := G^{i-1}_{\beta_i} = G_{\beta_1,\ldots,\beta_i} = \{g \in G : \beta_1^g = \beta_1, \ldots, \beta_i^g = \beta_i\}$$

for $1 \leq i \leq r$; each $G^i \geq G^{i+1}$. If $G^r = G_{(B)} = 1$, i.e. 1 is the only element that fixes all $\beta_1, \ldots, \beta_r$, then B is a **base** of G of *size* r, and the *subgroup series* $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is the associated **stabiliser chain**. A **strong generating set** for G relative to the base B is $S \subseteq G$ such that $G^i = \langle S \cap G^i \rangle$ for each i; we call the pair (B, S) a **BSGS**.

It is clear that every $G \leq \mathrm{Sym}(\Omega)$ has a base, Ω itself. Furthermore, if $[\beta_1, \ldots, \beta_r]$ is a base for G, then $[\beta_i, \ldots, \beta_r]$ is a base for $G^i = G_{\beta_1,\ldots,\beta_{i-1}}$. A question that we address later is, can we find a small base? The reason why we consider G to be a permutation group is as follows. Let G be an arbitrary finite group that acts on Ω; for a "base" to exist, the action must be faithful. Suppose instead that the kernel K of the action is nontrivial; then there is $k \in G$ that fixes every element of Ω; if $B = [\beta_1, \ldots, \beta_r] \subset \Omega$, then $k \in G^r \neq 1$, so B is not a base for G. In the faithful case, we can embed G as a subgroup of $\mathrm{Sym}(\Omega)$ via the action, so G is isomorphic to a (finite) permutation group, and a base for G is a base for its image G^Ω.

Example 2.49. Recall that the dihedral group $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ of order 8 acts faithfully on $\Omega = [4]$ by $r \mapsto (1,2,3,4)$ and $s \mapsto (1,4)(2,3)$. By identifying D_8 with its image $G = D_8^\Omega \leq \mathrm{Sym}(4)$, observe that $B = [1,2]$ is a base for D_8 of size 2 since $(3,4) \notin G$, however $[2,4]$ is not a base for D_8 since $sr^3 \mapsto (1,3) \in G$ which leaves 2 and 4 fixed. Consider the base $B = [1,2]$ and let $G^0 = G$:

- Let $G^1 = G^0_1 = \{(), (2,4)\}$.
- Let $G^2 = G^1_2 = G_{1,2} = 1$.

The stabiliser chain is $G = G^0 > G^1 > G^2 = 1$. A strong generating set S for G relative to B of size 2 is $\{(1,2,3,4), (2,4)\}$; this can be seen easily.

In [15], it is noted that the usefulness of the concept of a BSGS is supported by the observations that a BSGS appears to be the most appropriate way to represent a group in many important permutation group algorithms, effective algorithms (such as the *Schreier-Sims algorithm*) exist for constructing BSGSs for groups, and algorithms used to construct subgroups and homomorphic images of permutation groups and BSGSs of these tend to inherit a BSGS from the original group. One elementary observation on BSGSs is the following:

Lemma 2.50. *If $[\beta_1, \ldots, \beta_r]$ is a base for G, then every $g \in G$ is uniquely determined by the base image $[\beta_1^g, \ldots, \beta_r^g] \subset \Omega$.*

Proof. Suppose $h \in G$ satisfies $\beta_1^h = \beta_1^g, \ldots, \beta_r^h = \beta_r^g$. Then $\beta_i^{hg^{-1}} = \beta_i = \beta_i^1$ for every i, so $hg^{-1} \in G_{\beta_1,\ldots,\beta_r} = G^r = 1$, since we have a base. Then $h = g$. □

One advantage of the approach of using base images to represent group elements is that for many interesting groups (as per [15]), the size of a base may be rather small compared to its degree. For instance, the dihedral group example above can be generalised to D_{2n}; then $[1,2]$ is still a base of size 2, yet the degree is n which may be arbitrarily large.

Definition 2.51. Let G be a group and $H \leq G$. Then $T \subseteq G$ is a **(right) transversal** of H if every right coset of H contains exactly one element of T. Moreover, we assume without loss of generality for this thesis that $1 \in T$ (it must contain some element of H).

A transversal is a set of coset representatives for H in G. From Lagrange's theorem (which says that $|G| = |G : H||H|$), we see that $|T| = |G : H|$; moreover, $G = \bigsqcup_{t \in T} Ht$ is a disjoint union of cosets given by transversal elements. We give the following corollary of the OST:

Corollary 2.52. *Let T be a (right) transversal of G_α in G. The map $T \to \alpha^G$ given by $t \mapsto \alpha^t$ is a bijection.*

Proof. The map $T \to G_\alpha \backslash G$ given by $t \mapsto G_\alpha t$ is clearly a bijection, since a transversal gives a set of distinct coset representatives of G_α in G. Simply compose it with the map $G_\alpha \backslash G \to \alpha^G$ given by $G_\alpha g \mapsto \alpha^g$, which is a bijection by the OST. □

Thus, for α^G, a choice of elements $t \in G$ with the α^t all distinct and $\{\alpha^t\}_{t \in T} = \alpha^G$ defines a transversal T of G_α in G. (For $\alpha \in \alpha^G$, choose $t = 1$.) Recall that a base $[\beta_1, \ldots, \beta_r]$ has the associated stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$. Throughout this thesis, let T_i denote a transversal of $G^i = G^{i-1}_{\beta_i} = G_{\beta_1, \ldots, \beta_i}$ in G^{i-1} for $i = 1, \ldots, r$. Then by Corollary 2.52, the following is immediate with $G = G^{i-1}$ and $\alpha = \beta_i$:

Lemma 2.53. *Let G act on Ω and $[\beta_1, \ldots, \beta_r]$ be a base for G. Then $T_1, \ldots, T_r$ with each $T_i \subseteq G^{i-1}$ are corresponding transversals of the stabiliser chain if and only if for $1 \leq i \leq r$ and $\alpha \in \beta_i^{G^{i-1}}$, there is a unique $t \in T_i$ with $\alpha = \beta_i^t$.* □

Example 2.54. Recall from Example 2.49 the base $B = [1, 2]$ for $G = D_8$ (identified as a subgroup of $\mathrm{Sym}(4)$) and let $G^0 = G$. Using Lemma 2.53 to find transversals of the stabiliser chain, we see:

- Let $G^1 = G^0_1 = \{(), (2,4)\}$; note that $1^{G^0} = [4]$ and we take $T_1 = \{(), (1,2,3,4), (1,3), (1,4,3,2)\}$.
- Let $G^2 = G^1_2 = G_{1,2} = 1$; note that $2^{G^1} = \{2, 4\}$ and we take $T_2 = \{(), (2,4)\}$.

Sizes of bases and the group

Is there a relationship between a BSGS and the size of the group? First consider a similar question in the case of generating sets. A group G with a *nonredundant generating set* $X = \{x_1, \ldots, x_r\}$ is such that $G = \langle X \rangle$ but $G \neq \langle x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r \rangle$ for any i. In fact, considering the subgroup series $1 = U_0 < U_1 < \cdots < U_r = G$ where $U_i := \langle x_1, \ldots, x_i \rangle$ (each of the inclusions are proper), we see that $|U_{i+1}| \geq 2|U_i|$ for each i, so that $|G| \geq 2^r$; the size of a generating set is at worst logarithmic in the size of G. However, as opposed to using generating sets, using bases and stabiliser chains allows us to easily test membership in a group.

Clearly, if B is a base of size r for a permutation group G of degree n, then $|G| \leq n^r$ by the unique representation of elements of G by base images in Lemma 2.50, since there are (at most) n options for the image of each element in B and r elements in B. However, we can identify a precise result on $|G|$ by using bases, stabiliser chains and transversals (recall that these are in bijective correspondence with particular orbits).

Proposition 2.55. *Let $[\beta_1, \ldots, \beta_r]$ be a base for G, and $T_1, \ldots, T_r$ the associated transversals of the stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$. Then by Lagrange's theorem, $|G| = |G^0 : G^1| \cdots |G^{r-1} : G^r| = |T_1| \cdots |T_r|$ (this is Fact 3 in [3]). Also, $|\beta_i^{G^{i-1}}| = |G^{i-1}|/|G^{i-1}_{\beta_i}| = |G^{i-1}|/|G^i| = |T_i|$ in the finite case by the OST.* □

However, if $G^i = G^{i-1}$ for some i, then every element of G^{i-1} fixes β_i and $T_i = \{1\}$, and β_i is in some sense "redundant" in the base. Moreover, as noted above, Ω itself is a base for G. This leads us to the following notion, defined in [3]:

Definition 2.56. A base $B = [\beta_1, \ldots, \beta_r]$ for G is **nonredundant** if the inclusions in the associated stabiliser chain are proper: $G = G^0 > G^1 > \cdots > G^r = 1$. The size of a **minimum base** (a base with minimal size) for G is the **minimal base size** $b(G)$; every minimum base is nonredundant.

Since each element in G is completely determined by its action on a base (Lemma 2.50), a small base is desirable, as it can lead to a reduction in the space required to store the group elements, as noted in [3]. It can be easily seen that if

$B = [\beta_1, \ldots, \beta_r]$ is a base for G, then any list $\hat{B} = [\beta_1, \ldots, \beta_r, \ldots, \beta_k]$ of distinct elements of Ω with $k \geq r$ is also a base for G (the trivial group 1 only has itself as subgroups); thus, to verify that $b(G) \geq r$, it suffices to show that there is no base of size $r-1$. Also, for the base $B = [\beta_1, \ldots, \beta_r]$ for G, any permutation $\tilde{B} = [\beta_{\sigma_1}, \ldots, \beta_{\sigma_r}]$ of this list is also a base for G, as only 1 fixes every element in both lists (which contain precisely the same elements). However, the stabiliser chains associated to each base are different, which give rise to different transversals.

Lemma 2.57 (Lemma 4.1 in [3]). *Let $G \leq \mathrm{Sym}(\Omega)$ have degree n, and let r be the size of a nonredundant base for G. Then $r \leq \log |G|$; moreover, $r \leq b(G) \log n$. (All logarithms are base-2.)*

Proof. Let $B = [\beta_1, \ldots, \beta_r]$ be a nonredundant base for G with stabiliser chain $G = G^0 > G^1 > \cdots > G^r = 1$. Then we have $|G^i : G^{i+1}| \geq 2$ for all i (all inclusions proper); combining with Proposition 2.55 we get $2^r \leq |G^0 : G^1| \cdots |G^{r-1} : G^r| = |G|$.

From the above observation, since G has a base of size $b(G)$, we have $|G| \leq n^{b(G)}$. So $2^r \leq |G| \leq n^{b(G)}$, yielding $r \leq b(G) \log n$. □

Lemma 2.58. *If $G \leq \mathrm{Sym}(\Omega)$ and $H \leq G$, then if B is a base for G, then it is a base for H. Thus, $b(H) \leq b(G)$.*

Proof. Let $B = [\beta_1, \ldots, \beta_r]$ be a base for G, so that $G_{(B)} = 1$. But $H_{(B)} = \{h \in H : \beta_1^h = \beta_1, \ldots, \beta_r^h = \beta_r\} \subseteq G_{(B)}$, so $H_{(B)} = 1$ and B is a base for H. Thus a minimum base for G is a base for H, and $b(H) \leq b(G)$. □

If $G \leq \mathrm{Sym}(\Omega)$ has degree n, then clearly $b(G) \leq n$. In fact, as the following example shows, we must have $b(G) \leq n-1$ (applying the above lemma to $G \leq \mathrm{Sym}(\Omega)$ with $|\Omega| = n$), with equality if and only if $G = \mathrm{Sym}(\Omega)$.

Example 2.59 (symmetric groups). Consider the symmetric group $\mathrm{Sym}(n)$, which acts naturally on $\Omega = [n]$. Clearly $B = [1, \ldots, n]$ is a base for $\mathrm{Sym}(n)$, since 1 is the only permutation that fixes every element of B. However, $\tilde{B} = [1, \ldots, n-1]$ is also a base for $\mathrm{Sym}(n)$; a permutation that fixes $\{1, \ldots, n-1\}$ must also fix n (as it is a bijection), thus it is the identity.

Now suppose we have an ordered list $\hat{B}$ of $n-2$ or fewer elements. Then say α, β are not in $\hat{B}$; then the transposition (α, β) fixes every element of $\hat{B}$, so $\hat{B}$ is not a base for $\mathrm{Sym}(n)$. It follows that a smallest base for $\mathrm{Sym}(n)$ comprises any set of $n-1$ elements: $b(\mathrm{Sym}(n)) = n-1$ (note that $|\mathrm{Sym}(n)| = n!$).

Note that if $G < \mathrm{Sym}(n)$, then $b(G) \leq n-2$. This follows from the following: suppose that every ordered list $B = [\beta_1, \ldots, \beta_{n-2}]$ of distinct elements of $[n]$ is not a base. Then there is $g \in G$ with $\beta_i^g = \beta_i$ for all $i = 1, \ldots, n-2$ but $g \neq 1$. Then suppose α_1, α_2 are the remaining elements of $[n]$; then $g = (\alpha_1, \alpha_2) \in G$. Since B was arbitrary, it follows that $\langle \{(\alpha_1, \alpha_2) : 1 \leq \alpha_1 < \alpha_2 \leq n\} \rangle = \mathrm{Sym}(n) \leq G$, so $G = \mathrm{Sym}(n)$. (The general case follows since $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(n)$ where $|\Omega| = n$; this can be made formal using permutation isomorphism as below in Lemma 2.63.)

Example 2.60 (alternating groups). Consider the alternating group $\mathrm{Alt}(n)$ for $n \geq 3$, which acts naturally on $\Omega = [n]$. Let $B = [\beta_1, \ldots, \beta_r]$ be distinct elements of Ω. If $r = n-2$ then B is a base for $\mathrm{Alt}(n)$: suppose $g \in \mathrm{Alt}(n)$ satisfies $\beta_i^g = \beta_i$ for all $i = 1, \ldots, n-2$. Let α_1, α_2 be the remaining elements of $[n]$; then since the transposition $(\alpha_1, \alpha_2) \notin \mathrm{Alt}(n)$, we must have $g = 1$, and B is a base.

Now if $r = n-3$ then let $\alpha_1, \alpha_2, \alpha_3$ be the remaining elements of $[n]$. Then $(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1, \alpha_3)(\alpha_2, \alpha_3) \in \mathrm{Alt}(n)$ fixes B pointwise, so B is not a base for $\mathrm{Alt}(n)$. Thus $b(\mathrm{Alt}(n)) = n-2$ (compare this with $|\mathrm{Alt}(n)| = n!/2$).

Example 2.61 (cyclic subgroups of $\mathrm{Sym}(n)$). Let $\sigma = (1, \ldots, n) \in \mathrm{Sym}(n)$; the group $G = \langle \sigma \rangle$ is a cyclic permutation subgroup of $\mathrm{Sym}(n)$ with $G \cong C_n$, the cyclic group of order n. Clearly the ordered list $B = [1]$ (or any single element of Ω) is a base for G, since

$$1^{\sigma^k} = \underbrace{((1^\sigma)^\cdots)^\sigma}_{k \text{ times}} = 1 + (k \bmod n) \neq 1$$

for $n \nmid k$ (in which case $\sigma^k \neq 1$). It follows that $b(G) = 1$ (note that $|G| = n$).

However, if we choose a different $\tau \in \mathrm{Sym}(n)$, we get another cyclic permutation group $\tilde{G} = \langle \tau \rangle \leq \mathrm{Sym}(n)$ (isomorphic to C_k where k is the order of τ) which may have a longer minimum base; see Remark 4.8 for such a construction.

For instance with $n = 10$, $\tau = (1,2)(3,4,5)(6,7,8,9,10) \in \mathrm{Sym}(10)$ with coprime cycle lengths 2, 3, 5, and $\tilde{G} = \langle \tau \rangle \leq \mathrm{Sym}(10)$, a minimum base is $\tilde{B} = [1, 3, 6]$. This is explained by the following.

One way to increase the length of a minimum base for $\tilde{G} = \langle \tau \rangle$ is to consider a partition of n where the parts are coprime (say ℓ of them are not 1). Construct τ with that cycle type; doing so ensures that any base has length at least ℓ, as $|\tilde{G}| = |\tilde{G}^0 : \tilde{G}^1| \cdots |\tilde{G}^{r-1} : \tilde{G}^r|$ (Proposition 2.55 with $\tilde{B} = [\tilde{\beta}_1, \ldots, \tilde{\beta}_r]$ a base) is a product of the ℓ coprime cycle lengths.

Now, the length $|\tilde{G}^{i-1} : \tilde{G}^i| = |\tilde{\beta}_i^{\tilde{G}^{i-1}}|$ of the orbit $\tilde{\beta}_i^{\tilde{G}^{i-1}}$ is either 1 (if $\tilde{\beta}_i \in |\tilde{\beta}_j^{\tilde{G}}|$ for some $j < i$) or equal to $|\tilde{\beta}_i^{\tilde{G}}|$ (since cycle lengths are coprime and the cyclic stabiliser $\tilde{G}^i$ is generated by the $|\tilde{\beta}_i^{\tilde{G}^{i-1}}|$th power of the generator of $\tilde{G}^{i-1}$), thus the terms of the product necessarily contain the ℓ coprime cycle lengths. In fact, this argument shows that $b(\tilde{G}) = \ell$ in this case, since choosing $\tilde{\beta}_1, \ldots, \tilde{\beta}_\ell$ from different cycles (of length at least 2) yields a base for $\tilde{G}$.

One practical result that helps us to classify subgroups of $\mathrm{Sym}(\Omega)$ by minimal base size is the observation that conjugate subgroups have the same minimal base size.

Proposition 2.62. *Let $G \leq \mathrm{Sym}(\Omega)$ and $\sigma \in \mathrm{Sym}(\Omega)$. If $B = [\beta_1, \ldots, \beta_r]$ is a base for G, then $B^\sigma := [\beta_1^\sigma, \ldots, \beta_r^\sigma]$ is a base of the conjugate subgroup $G^\sigma \leq \mathrm{Sym}(\Omega)$; these are all the bases of G^σ. Thus, $b(G) = b(G^\sigma)$.*

Proof. Let $k = \sigma^{-1} g \sigma \in g^\sigma$, with $g \in G$. Then for all $1 \leq i \leq r$,

$$(\beta_i^\sigma)^k = (\beta_i^\sigma)^{\sigma^{-1} g \sigma} = (\beta_i^g)^\sigma = \beta_i^\sigma$$

since $g \in G$ fixes β_i. So $B^\sigma := [\beta_1^\sigma, \ldots, \beta_r^\sigma]$ is a base of G^σ.

Every base of G^σ is of this form, since $G = (G^\sigma)^{\sigma^{-1}}$, so if $\tilde{B}$ is a base of G^σ, then the above implies $\tilde{B}^{\sigma^{-1}}$ is a base of G. The results follow from the observation that $(\tilde{B}^{\sigma^{-1}})^\sigma = \tilde{B}$. □

Thus, to understand $b(G)$ for $G \leq \mathrm{Sym}(\Omega)$, it suffices to consider conjugacy classes of subgroups, which we do later in this thesis. Another useful lemma is that bases behave well under permutation isomorphism.

Lemma 2.63. *If $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\tilde{\Omega})$ are permutation isomorphic via $\tau : \Omega \to \tilde{\Omega}$ and $\psi : G \to H$, then*

(a) for $\alpha \in \Omega$, we have $H_{\tau(\alpha)} = \psi[G_\alpha]$ (equivalently, G_α and $H_{\tau(\alpha)}$ are permutation isomorphic via τ and $\psi|_{G_\alpha}$),

(b) if $B = [\beta_1, \ldots, \beta_r]$ is a base for G, then $\tilde{B} = [\tau(\beta_1), \ldots, \tau(\beta_r)]$ is a base for H, and

(c) $b(G) = b(H)$.

Proof. (a) Note that

$$h = \psi(g) \in H_{\tau(\alpha)} \iff \tau(\alpha)^h = \tau(\alpha) \iff \tau(\alpha^g) = \tau(\alpha)^{\psi(g)} = \tau(\alpha) \iff \alpha^g = \alpha$$

since τ is a bijection, if and only if $g \in G_\alpha$, if and only if $h = \psi(g) \in \psi[G_\alpha]$. Since ψ is an isomorphism, it restricts to an isomorphism $\psi|_{G_\alpha}$, so G_α and $H_{\tau(\alpha)}$ are permutation isomorphic.

(b) We show that $H_{\tau(\beta_1),\ldots,\tau(\beta_r)} = \psi[G_{\beta_1,\ldots,\beta_r}]$ by induction on r: the result follows from part (a) if $r = 1$. If $r > 1$, then $H_{\tau(\beta_1),\ldots,\tau(\beta_r)} = (H_{\tau(\beta_1),\ldots,\tau(\beta_{r-1})})_{\tau(\beta_r)}$ and $G_{\beta_1,\ldots,\beta_r} = (G_{\beta_1,\ldots,\beta_{r-1}})_{\beta_r}$, so by part (a),

$$H_{\tau(\beta_1),\ldots,\tau(\beta_r)} = (H_{\tau(\beta_1),\ldots,\tau(\beta_{r-1})})_{\tau(\beta_r)} = \psi[(G_{\beta_1,\ldots,\beta_{r-1}})_{\beta_r}] = \psi[G_{\beta_1,\ldots,\beta_r}]$$

since $G_{\beta_1,\ldots,\beta_{r-1}}$ and $H_{\tau(\beta_1),\ldots,\tau(\beta_{r-1})}$ are permutation isomorphic by the inductive hypothesis.

Since $B = [\beta_1, \ldots, \beta_r]$ is a base for G, it follows that $G_{\beta_1,\ldots,\beta_r} = 1_G$, so $H_{\tau(\beta_1),\ldots,\tau(\beta_r)} = \psi[1_G] = 1_H$, and thus $\tilde{B} = [\tau(\beta_1), \ldots, \tau(\beta_r)]$ is a base for H.

(c) Follows immediately from part (b). □

Strong generating sets

Recall that a strong generating set S for a base $B = [\beta_1, \ldots, \beta_r]$ is a subset of G such that each $G^i \leq G^{i-1}$ is generated by $S \cap G^i$. Note that for $i \neq j$, we have $T_i \cap T_j = \{1\}$: if $i < j$, then $G^i \geq G^{j-1} \geq G^j$, and suppose $t_i \in T_j \subseteq G^{j-1} \leq G^i$ for some $t_i \in T_i$. Then $t_i \in G^i$, but T_i is a transversal of G^i in G^{i-1}, so $t_i = 1$ (since $1 \in T_i$). Then transversals (naïvely) give rise to a strong generating set:

Lemma 2.64. *Let $B = [\beta_1, \dots, \beta_r]$ be a base for G, and let the corresponding transversals of the stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ be $T_1, \dots, T_r$. Then*

(a) $S = \bigsqcup_i (T_i \setminus \{1\})$ generates G and moreover is a strong generating set for B; and

(b) for $g \in G^i$, we have a unique decomposition $g = t_r t_{r-1} \cdots t_{i+1}$ where each $t_k \in T_k$.

Proof. For $G^r = 1$, $S \cap G^r = \emptyset$ and $G^r = \langle \emptyset \rangle = \langle S \cap G^r \rangle$. Now since $[\beta_{i+1}, \dots, \beta_r]$ is a base for G^i with stabiliser chain $G^i \geq G^{i+1} \geq \cdots \geq G^r$ and transversals $T_i, \dots, T_r$ for $i \leq r$, we proceed by induction on i and suppose that $G^i = \langle S \cap G^i \rangle$. Then for $g \in G^{i-1}$, we have $g \in G^i t$ if and only if $g = \tilde{G} t_i$ for *unique* $t_i \in T_i$, and with $\tilde{G} = t_r t_{r-1} \cdots t_{i+1} \in G^i = \langle S \cap G^i \rangle$ uniquely with each $t_k \in T_k$ (by the inductive hypothesis). So $g = \tilde{G} t_i = t_r t_{r-1} \cdots t_i \in \langle (S \cap G^i) \cup (T_i \setminus \{1\}) \rangle = \langle S \cap G^{i-1} \rangle$ since $T_i \setminus \{1\} \subseteq G^{i-1}$ is disjoint from G^i. It follows that $G^{i-1} = \langle S \cap G^{i-1} \rangle$.

Taking $i = 0$, we recover that $G = \langle S \cap G \rangle = \langle S \rangle$, and that (B, S) is a BSGS for G. □

A consequence of part (b) is that for $g \in G$, we have a unique decomposition $g = t_r t_{r-1} \cdots t_1$ with each $t_i \in T_i$. Since the $(T_i \setminus \{1\})_i$ are disjoint for every $1 \leq i \leq r$, it follows that $|S| = \sum_i |T_i| - r$. However, S is not necessarily a *minimal* strong generating set, as seen in the following example.

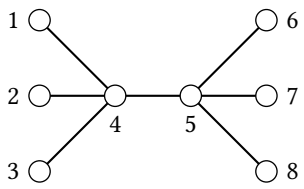
Example 2.65. Recall the base, stabiliser chain and transversals for $G = D_8$ (identified as a subgroup of $\mathrm{Sym}(4)$) in Example 2.54. A strong generating set S for G relative to B of size 4 is, by Lemma 2.64,

$$\{(1,2,3,4), (1,3), (1,4,3,2), (2,4)\};$$

this is different to the example earlier where $(1,4,3,2)$ and $(1,3)$ are removed. The problem of computing a better BSGS for G is dealt with by the Schreier-Sims algorithm, discussed below.

Lemma 2.64 allows us to easily show that a group G can have *nonredundant* bases and strong generating sets of different sizes. Also, we see the utility of Proposition 2.55 in determining the size of a permutation group without needing to know its full structure: below is an example with an automorphism group of a graph, but we can apply a similar process (perhaps using the Schreier-Sims algorithm, discussed below) to compute the order of the Rubik's group of symmetries of the Rubik's cube, which is a permutation group of degree 48 and discussed in Example 2.41.

Example 2.66. Let Γ be the following graph with vertex set $V = \{1, \dots, 8\}$:



The group $G = \mathrm{Aut}(\Gamma)$ of automorphisms of Γ (relabellings of Γ which preserve edges) acts naturally on $\Omega = V$, with the action of the automorphism $\sigma \in G$ on the vertex $v \in \Omega$ being v^σ. Then clearly $G \leq \mathrm{Sym}(8)$ is a permutation group of degree 8. Let $G^0 = \tilde{G}^0 = G = \mathrm{Aut}(\Gamma)$. We manually compute and consider two stabiliser chains for G (and find $|G|$):

- Let $G^1 = G^0_4$. Then $4^{G^0} = \{4, 5\}$, and take $T_1 = \{(), (1,6)(2,7)(3,8)(4,5)\}$.
  Let $G^2 = G^1_1 = G_{4,1}$. Then $1^{G^1} = \{1, 2, 3\}$, and take $T_1 = \{(), (1,2), (1,3)\}$.
  Let $G^3 = G^2_2 = G_{4,1,2}$. Then $2^{G^2} = \{2, 3\}$, and take $T_2 = \{(), (2,3)\}$.
  Let $G^4 = G^3_6 = G_{4,1,2,6}$. Then $6^{G^3} = \{6, 7, 8\}$, and take $T_3 = \{(), (6,7), (6,8)\}$.
  Let $G^5 = G^4_7 = G_{4,1,2,6,7} = 1$. Then $7^{G^4} = \{7, 8\}$, and take $T_4 = \{(), (7,8)\}$.

  But $G^5 = 1$, since the only automorphism that fixes 4, 1, 2, 6, and 7 is the identity. So we see that $B = [4, 1, 2, 6, 7]$ is a nonredundant base for G with stabiliser chain $G = G^0 > G^1 > G^2 > G^3 > G^4 > G^5 = 1$ and associated transversals $T_1, \dots, T_5$. A strong generating set S for G is $\{(1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8)\}$, with size 7. Moreover, from Proposition 2.55, we see that $|G| = |T_1| \cdots |T_5| = 2 \cdot 3 \cdot 2 \cdot 3 \cdot 2 = 72$, so there are 72 automorphisms (relabellings) of Γ.

- Let $\tilde{G}^1 = \tilde{G}^0_1$. Then $|1^{\tilde{G}^0}| = 6 = |\tilde{T}_1|$, since an automorphism sends 1 to any leaf.
  Let $\tilde{G}^2 = \tilde{G}^1_2 = G_{1,2}$. Then $|2^{\tilde{G}^1}| = 2 = |\tilde{T}_2|$, since when 1 is fixed, so are 4 and 5.
  Let $\tilde{G}^3 = \tilde{G}^2_6 = G_{1,2,6}$. Then $|6^{\tilde{G}^2}| = 3 = |\tilde{T}_3|$, since when 1 and 2 are fixed, 6 can map to 6, 7 or 8.
  Let $\tilde{G}^4 = \tilde{G}^3_7 = G_{1,2,6,7}$. Then $|7^{\tilde{G}^3}| = 2 = |\tilde{T}_4|$, since (similar to above) the image of 7 is 7 or 8.

  But $\tilde{G}^4 = 1$, since the only automorphism that fixes 1, 2, 6, and 7 is the identity. So we see that $\tilde{B} = [1, 2, 6, 7]$ is a nonredundant base for G with stabiliser chain $G = \tilde{G}^0 > \tilde{G}^1 > \tilde{G}^2 > \tilde{G}^3 > \tilde{G}^4 = 1$ and transversals $\tilde{T}_1, \ldots, \tilde{T}_4$. As before, we see that $|G| = |\tilde{T}_1| \cdots |\tilde{T}_4| = 6 \cdot 2 \cdot 3 \cdot 2 = 72$.

Note that any base B for G must contain at least two of $\{1, 2, 3\}$ and two of $\{6, 7, 8\}$, otherwise there is an automorphism $\sigma \neq 1_{\mathrm{Sym}(\Omega)}$ that fixes B but swaps two elements of $\{1, 2, 3\}$ or $\{6, 7, 8\}$ that are not in B. So $b(G) = 4$.

Also, note that while $\hat{B} = [1, 2, 6, 7, 4]$ is also a base for G as a permutation of the (nonredundant) base $B = [4, 1, 2, 6, 7]$, we see that $\hat{B}$ is *not* nonredundant since $\hat{G}^4 = G_{1,2,6,7} = 1 = G_{1,2,6,7,4} = \hat{G}^5$ from the second example.

Random elements and the constructive membership problem

In the above proof of Lemma 2.64, we found a *unique* decomposition of $g \in G$ as a product of transversal elements $t_r t_{r-1} \cdots t_1$ with each $t_i \in T_i$. This gives us a simple way of generating random elements in G, or simply enumerating all elements of G, assuming we have transversals of the stabiliser chain; these can be computed using the orbit-stabiliser algorithm.

Algorithm 2.67 (random element). *Let $B = [\beta_1, \ldots, \beta_r]$ be a base for $G \leq \mathrm{Sym}(\Omega)$ and $\mathcal{T} := [T_1, \ldots, T_r]$ be the corresponding transversals of the stabiliser chain. For each transversal T_i, choose $t_i \in T_i$ independently and uniformly at random, and return $g = t_r t_{r-1} \cdots t_1 \in G$ which is a random element in G.*

Note that this corresponds to a uniform distribution on G, since for fixed $\tilde{g} = \tilde{t}_r \tilde{t}_{r-1} \cdots \tilde{t}_1 \in G$, independence and uniqueness of the decomposition gives that the probability of randomly choosing $\tilde{g}$ is

$$\mathbb{P}(g = \tilde{g}) = \mathbb{P}(t_1 = \tilde{t}_1, \ldots, t_r = \tilde{t}_r) = \mathbb{P}(t_1 = \tilde{t}_1) \cdots \mathbb{P}(t_r = \tilde{t}_r) = \frac{1}{|T_1|} \cdots \frac{1}{|T_r|} = \frac{1}{|G|}.$$

Moreover, we can clearly generate an independent and identically distributed (uniform) random sample $g_1, \ldots, g_n$ from G by repeating this procedure. See the appendix for an implementation in GAP as the function `RandomElt`.

This is useful, since alternatives to getting a random element in a finitely generated large group $G = \langle x_1, \ldots, x_m \rangle$ may be to use a random product of generators and inverses of random length (a naïve approach that has no reason a priori to have favourable statistical properties), or possibly a more sophisticated approach as found in [9], which generates a list of random elements of G at the expense of independence and uniformity (which is only asymptotically true).

Example 2.68. Recall from Example 2.66 the graph Γ with vertex set $V = \{1, \ldots, 8\}$, the stabiliser chain $G = G^0 > G^1 > G^2 > G^3 > G^4 > G^5 = 1$ for $G = \mathrm{Aut}(\Gamma)$, and the strong generating set

$$S = \{(1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8)\}$$

for G. Using GAP, we may define G as the group generated by S:

```
G := Group([ (1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8) ]); # generators
B := [ 4, 1, 2, 6, 7];
SC := StabChain( G, B ); # stabiliser chain of G with respect to base B
```

The following GAP code assumes `G`, `B` and `SC` are defined as above. Let us run through Algorithm 2.67 to generate a random element of G. Below is GAP code with a modified `RandomElt` function that prints out the choices of $t_i \in T_i$ (and the intermediate calculations for constructing random $g \in G$; see appendix).

```
gap> RandomEltPrint( SC );
i = 1:  t_i = (1,6)(2,7)(3,8)(4,5)      g <- (1,6)(2,7)(3,8)(4,5)
i = 2:  t_i = (1,2)     g <- (1,7,2,6)(3,8)(4,5)
i = 3:  t_i = (2,3)     g <- (1,7,2,8,3,6)(4,5)
```

```
i = 4:  t_i = ()        g <- (1,7,2,8,3,6)(4,5)
i = 5:  t_i = (7,8)     g <- (1,7,3,6)(2,8)(4,5)
(1,7,3,6)(2,8)(4,5)
```

So here, the algorithm chooses $t_1 = (1,6)(2,7)(3,8)(4,5) \in T_1$, $t_2 = (1,2) \in T_2$, $t_3 = (2,3) \in T_3$, $t_4 = () \in T_4$, $t_5 = (7,8) \in T_5$, and returns $g = t_5 t_4 t_3 t_2 t_1 = (1,7,3,6)(2,8)(4,5) \in G$, a uniformly random automorphism of Γ.

Next we consider a naïve algorithm to test membership of $g \in \mathrm{Sym}(\Omega)$ in a permutation group $G \leq \mathrm{Sym}(\Omega)$ given a BSGS for G arising from transversals for the stabiliser chain:

Algorithm 2.69 (membership test). *Let $B = [\beta_1, \ldots, \beta_r]$ be a base for $G \leq \mathrm{Sym}(\Omega)$ and $\mathcal{T} := [T_1, \ldots, T_r]$ be the corresponding transversals of the stabiliser chain. For arbitrary $g \in \mathrm{Sym}(\Omega)$, to test if $g \in G$, we do the following:*

1: ***procedure*** MEMBERSHIP($G, \Omega, B, \mathcal{T}, g$) ▷ *Whether $g \in G$*
2: $h \leftarrow g$
3: ***for*** $i \leftarrow 1$ ***to*** r ***do*** ▷ *We go through each stabiliser G^{i-1}*
4: ***if*** $\beta_i^h = \beta_i^{t_i}$ *for some* $t_i \in T_i$ ***then*** $h \leftarrow h t_i^{-1}$ ▷ *$\beta_i^{h t_i^{-1}} = \beta_i$; here we set $h = g t_1^{-1} t_2^{-1} \cdots t_i^{-1}$*
5: ***else return*** `False`
6: ***if*** $h = 1$ ***then return*** `True`
7: ***else return*** `False`

Proof of correctness. This algorithm simultaneously deals with the cases that $g \in G$ and $g \notin G$. First, consider the case that $g \in G$. For each i, we find $t_i \in T_i$ with $h = g t_1^{-1} t_2^{-1} \cdots t_r^{-1} \in G^r = 1$ in line 6, so $g = t_r t_{r-1} \cdots t_1 \in G$, and we return `True`.

If $g \notin G$, suppose for a contradiction that we return `True`. Then $h = 1$ with $h = g t_1^{-1} \cdots t_r^{-1}$ and $t_1, \ldots, t_r \in G$, so $g = t_r t_{r-1} \cdots t_1 \in G$, which is a contradiction. □

See the appendix for an implementation in GAP as the function `Membership`.

Example 2.70. Recall from Example 2.66 the graph Γ with vertex set $V = \{1, \ldots, 8\}$, and the stabiliser chain $G = G^0 > G^1 > G^2 > G^3 > G^4 > G^5 = 1$ for $G = \mathrm{Aut}(\Gamma)$. The following GAP code assumes `G`, `B` and `SC` are defined as in Example 2.66. Let us run through Algorithm 2.69 to show that $(1,3,5,2)(7,8) \notin G$. Below is GAP code with a modified `Membership` function that prints out the values of h and t_i throughout the algorithm.

```
gap> Membership( SC, (1,3,5,2)(7,8) );
false
gap> MembershipPrint( SC, (1,3,5,2)(7,8) );
i = 1:  t_1 = (),       h <- (1,3,5,2)(7,8)
i = 2:  t_2 = (1,3),    h <- (2,3,5)(7,8)
i = 3:  t_3 = (2,3),    h <- (3,5)(7,8)
i = 4:  t_4 = (),       h <- (3,5)(7,8)
i = 5:  t_5 = (7,8),    h <- (3,5)
false
```

Recall that the base for G is $[4, 1, 2, 6, 7]$. Set $h = (1,3,5,2)(7,8)$ and suppose for contradiction that $h \in G$.

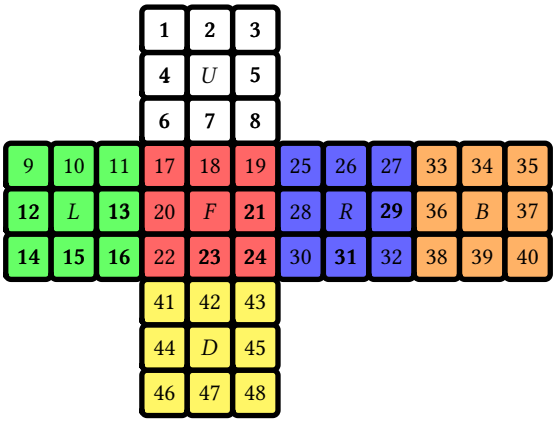
- For $i = 1$: $4^h = 4$ and we choose $t_1 = () \in T_1$. Then we redefine $h \leftarrow h t_1^{-1} = (1,3,5,2)(7,8) \in G^1$.
- For $i = 2$: $1^h = 2$ and we choose $t_2 = (1,3) \in T_2$. Then we redefine $h \leftarrow h t_2^{-1} = (2,3,5)(7,8) \in G^2$.
- For $i = 3$: $2^h = 3$ and we choose $t_3 = (2,3) \in T_3$. Then we redefine $h \leftarrow h t_3^{-1} = (3,5)(7,8) \in G^3$.
- For $i = 4$: $6^h = 6$ and we choose $t_4 = () \in T_4$. Then we redefine $h \leftarrow h t_4^{-1} = (3,5)(7,8) \in G^4$.
- For $i = 5$: $7^h = 8$ and we choose $t_5 = (7,8) \in T_5$. Then we redefine $h \leftarrow h t_5^{-1} = (3,5) \in G^5 = 1$.

This is clearly a contradiction, as $(3,5) \neq ()$. So $h \notin G$. (Note that if one of the base element images was not in the relevant orbit, we would stop the algorithm earlier and also conclude non-membership in G.)

Example 2.71. The above two algorithms (random element generation and membership testing) can also be applied to the Rubik's group G from Example 2.41, in which case we get a random move (or state) of the Rubik's cube, and the ability to test whether an arbitrary restickering of the cube can be solved. Using GAP, we may compute that a base of G of size 18 is

$$B = [1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21, 23, 24, 29, 31].$$

Recall that we represent the cube by the following diagram; the elements of the base B are bolded.

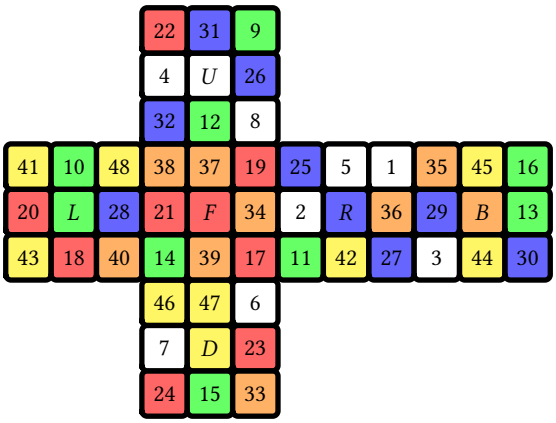


Thus, if we fix these 18 stickers, then the entire cube is fixed. The base B contains one sticker from each of 7 corners (except for the corner $\{32, 38, 48\}$) and 11 edges (except for the edge $\{39, 47\}$); if we fix these 7 corner and 11 edge stickers, then their respective corners and edges are also fixed, and the final corner and edge is necessarily in the correct position and orientation. So $b(G) \leq 18$. Thus, it is reasonable to ask if we can find a base of size less than 18.

Now, for instance, the randomly generated element (using GAP)

$$x = (1, 27, 32, 6, 43, 14, 22)(2, 28, 13, 37, 18, 15, 47, 42, 31)(3, 38, 17, 24, 46, 41, 9)(5, 26)$$
$$(7, 44, 39, 23, 45, 34, 21, 20, 12)(11, 30, 40, 16, 35, 33, 48)(29, 36) \in G$$

represents the following valid restickering of the Rubik's cube (for instance, $1^x = 27$ means that the sticker labelled 1 is moved to where the sticker labelled 27 was in the solved state).



In fact, one may verify that

$$x = LF^{-1}L^{-1}FUFU^{-1}F^2LFL^{-1}U^{-1}L^{-1}ULU^{-1}LUFU^{-1}F^{-1}L^{-2}ULF^{-1}LF(L^{-1}U)^2B^{-1}UBLUL^{-1}$$
$$F^{-1}L^{-1}FL^2UL^{-1}ULB^{-1}U^{-1}BLDF^2D^{-1}LF^{-1}UL^{-1}FU^{-1}LD^{-1}LBDU^{-2}B^{-1}R^{-1}BU^{-1}RF^{-1}UD^{-2},$$

that is, apply this move sequence to the solved state to get the state x in the above diagram, or equivalently, apply x^{-1} to a cube in this state to solve it (simply apply the inverses of each move in reverse). See the appendix for relevant GAP code (that also allows us to find a sequence of moves to solve a valid restickering, which is done implemented using permutation group theory and stabiliser chains).

We have not yet answered the question of how we *find* a BSGS for a permutation group G. One such way is the Schreier-Sims algorithm. However, to discuss this, we first discuss an algorithm for computing orbits, stabilisers and transversals.

The orbit-stabiliser and Schreier-Sims algorithms

To get the stabiliser chain for a base B, we must store information about the pointwise stabilisers of an elements in B. We can do this by finding a generating set for each stabiliser. Furthermore, it is useful to store transversals of the stabiliser chain for various purposes such as membership testing and random element generation; these can all be found by the orbit-stabiliser algorithm.

Algorithm 2.72 (orbit-stabiliser). *Suppose $G = \langle X \rangle$ is finitely generated by $X = [x_1, \dots, x_m]$ and acts on Ω. Let $\alpha \in \Omega$. Suppose further that the orbit α^G is finite. The following algorithm computes α^G, a generating set for G_α, and a right transversal T of G_α:*

(Denote the ith element of the ordered list L by $L[i]$, and the concatenation of lists L_1, L_2 by $L_1 \cup L_2$.)

1: ***procedure*** ORBITSTABILISER($G = \langle X \rangle, \Omega, \alpha$) ▷ *Computes the G-orbit and generating set of stabiliser (and its transversal) of α*
2: $\quad O \leftarrow [\alpha], T \leftarrow [1], S \leftarrow [\,], \mathcal{E} \leftarrow X \cup X^{-1} = [x_1, \dots, x_m, x_1^{-1}, \dots, x_m^{-1}], i \leftarrow 1$
3: $\quad$ ***while*** $i \le |O|$ ***do***
4: $\quad\quad o \leftarrow O[i]$ ▷ $o = O[i] = \alpha^{T[i]}$
5: $\quad\quad$ ***for*** $x \in \mathcal{E}$ ***do***
6: $\quad\quad\quad$ ***if*** $o^x \notin O$ ***then*** *append* o^x *to* O, $T[i]x$ *to* T ▷ $O[\ell+1] := o^x = \alpha^{T[i]x} = \alpha^{T[\ell+1]}$ *where* $\ell = |O|$
7: $\quad\quad\quad$ ***else if*** $o^x = O[j]$ *for some* j ***then*** *append* $T[i]xT[j]^{-1}$ *to* S ▷ $\alpha^{T[i]x} = o^x = \alpha^{T[j]}$ *so* $\alpha^{T[i]xT[j]^{-1}} = \alpha$
8: $\quad\quad i \leftarrow i + 1$
9: $\quad$ ***return*** O, T, S ▷ *The orbit is O, S generates the stabiliser, T is a transversal*

Then $O = \alpha^G$, $\langle S \rangle = G_\alpha$, and T is a transversal of G_α in G.

Next we show that the algorithm works (and terminates), but we omit the proof that $\langle S \rangle = G_\alpha$ for brevity (see Section 4.1 of [15] for proof). The key to this algorithm is that $O[i] = \alpha^{T[i]}$ for all i, from $O[1] = \alpha = \alpha^1 = \alpha^{T[1]}$ and the comment in line 6.

Proof. Observe that $T \subseteq G$ since we only append elements of the form $T[i]x$ to T whenever line 6 runs, where $T[i] \in T \subseteq G$ (since $T[1] = 1 \in G$ and then by induction on i) and $x \in \mathcal{E} \subseteq G$.

First we show that $O = \alpha^G$. Clearly $O \subseteq \alpha^G$: if $o \in O$ then $o = O[i]$ for some i, so $o = O[i] = \alpha^{T[i]}$ where $T[i] \in T \subseteq G$. To see that $\alpha^G \subseteq O$: take $\alpha^g \in \alpha^G$ where $g \in G$. Then $g = x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}$ with each $\varepsilon_{i_j} = \pm 1$ since $G = \langle X \rangle$ is finitely generated. We proceed by induction on k. If $k = 0$, then $g = 1$ and $\alpha^g = \alpha^1 = \alpha = O[1] \in O$. For the inductive step with $k \ge 1$, write

$$\alpha^g = \alpha^{x_{i_1}^{\varepsilon_1} \cdots x_{i_k}^{\varepsilon_k}} = \left(\alpha^{x_{i_1}^{\varepsilon_1} \cdots x_{i_{k-1}}^{\varepsilon_{k-1}}}\right)^{x_{i_k}^{\varepsilon_k}};$$

by the inductive hypothesis $\alpha^{x_{i_1}^{\varepsilon_1} \cdots x_{i_{k-1}}^{\varepsilon_{k-1}}} \in O$, say $\alpha^{x_{i_1}^{\varepsilon_1} \cdots x_{i_{k-1}}^{\varepsilon_{k-1}}} = O[\ell]$ for some ℓ. Then when $i = \ell$ (in line 3) and $x = x_{i_k}^{\varepsilon_k} \in \mathcal{E}$ (in line 5), we append $\alpha^g = o^{x_{i_k}^{\varepsilon_k}}$ to O. So indeed $O = \alpha^G$. Since α^G is finite, the algorithm terminates (see line 3).

By line 6, we see that at the end of the algorithm, T comprises elements $t \in G$ with α^t all distinct and $\{\alpha^t\}_{t \in T} = \alpha^G$. Then Corollary 2.52 implies T is a transversal of G_α in G. □

Now a subgroup of a finitely generated group need not be finitely generated; it is known that the free group on 2 generators has a subgroup isomorphic to a free group on a countably infinitely set of generators. However, the orbit-stabiliser algorithm proves that for any finitely generated group G acting on a set Ω, if an orbit α^G is finite, then the stabiliser G_α is finitely generated:

Corollary 2.73. *Let a finitely generated group $G = \langle X \rangle$ act on Ω and $\alpha \in G$. If α^G is finite, then G_α is finitely generated (by the output S of the orbit-stabiliser algorithm, which is finite with $|S| \leq 2|\alpha^G||X|$).* □

Now that we have established a way of computing orbits, stabilisers and transversals, we can look to a general form of computing a BSGS for a permutation group G. One such approach is the **Schreier-Sims algorithm**, if a partial base B and generating set S for G are known. (Often, we have the empty partial base $B = [\,]$, which we "extend" to find a base for G.)

Intuitively, a naïve version of the algorithm extends B to a base by considering generators $x \notin G_{\beta_1,\ldots,\beta_k}$ in S and appending points of Ω that are not fixed by x. We then use the orbit-stabiliser algorithm to compute and append *Schreier generators* for $G^i = G_{\beta_1,\ldots,\beta_i}$ to S, ignoring those that are equal to the identity $1 \in G$. The resulting (B, S) is a BSGS for G, and is an improvement over Lemma 2.64.

This algorithm was used by Sims to construct and prove existence of some of the theorised sporadic finite simple groups, such as Lyons' group (degree $n \approx 9 \cdot 10^6$) in 1973 [28]. It is implemented in many computational packages such as GAP to compute bases, and for large degree groups, a randomised variant is used to speed up computation since the number of Schreier generators to be processed becomes too large for the deterministic algorithm.

2.3 Elementary abelian groups

In chapter 4, we will need the notion of an elementary abelian p-group, which we then realise as a permutation group.

Definition 2.74. Let p be a prime. A **(finite) elementary abelian (p-)group** G is a finite abelian group such that the order of G is a power of p.

An equivalent definition is that G is a finite abelian group such that every nontrivial element has order p.

Recall that for groups G, H, their **direct product** is the group $G \times H$ with underlying set the Cartesian product $G \times H$ and group operation $(g, h)(a, b) = (ga, hb)$ for $g, a \in G$ and $h, b \in H$. When G and H are *abelian*, we may instead call it a **direct sum** and write $G \oplus H$; we sometimes use additive notation $(g, h) + (a, b) = (g + a, h + b)$ with identity 0, writing ng instead of g^n.

It turns out that the structure of a finite abelian group is quite simple. The following result is standard, and is often called the *fundamental theorem of finite abelian groups*; see Theorem 6.9 in [26] for a proof.

Theorem 2.75 (basis for finite abelian groups). *Every finite abelian group G is a direct sum of cyclic groups.*

Using this result, we may show that a finite elementary p-group must be a direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$.

Corollary 2.76. *If G is a finite elementary abelian p-group, then $G \cong (\mathbb{Z}/p\mathbb{Z})^k$ for some k. (In the literature, such $G \cong (\mathbb{Z}/p\mathbb{Z})^k$ is often denoted by p^k.)*

Proof. By the basis theorem (Theorem 2.75), write $G \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_k\mathbb{Z})$ with each $n_i > 1$. Let e_i be the element in $(\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/n_k\mathbb{Z})$ with a 1 in the ith entry and 0s elsewhere. Using the isomorphism, e_i has order p (since G is elementary abelian), so $p1 = 0$ in $\mathbb{Z}/n_i\mathbb{Z}$, so $n_i = p$ (as p is prime). Since $1 \leq i \leq k$ was arbitrary, the result follows. □

Example 2.77. Let p be prime and n, m be such that $mp \leq n$. Define the cycle $c_i = ((i-1)p + 1, \ldots, ip) \in \mathrm{Sym}(n)$ for $i = 1, \ldots, k$. Then we may construct a permutation group $G \leq \mathrm{Sym}(n)$ by

$$G = \langle c_1, \ldots, c_k \rangle = \langle (1, \ldots, p), (p+1, \ldots, 2p), \ldots, ((k-1)p + 1, \ldots, kp) \rangle;$$

note that each cycle c_i has order p, and moreover, the cycles commute: $c_i c_j = c_j c_i$ for all $i \neq j$, since they are disjoint. So, for arbitrary $1 \neq g = c_{i_1}^{\pm 1} \cdots c_{i_m}^{\pm 1} \in G$ (where $m \geq 1$), we have $g^\ell = c_{i_1}^{\pm \ell} \cdots c_{i_m}^{\pm \ell}$ for $\ell \in \mathbb{Z}$; in particular, $g^p = c_{i_1}^{\pm p} \cdots c_{i_m}^{\pm p} = 1$ and $g^\ell \neq 1$ for $1 \leq \ell \leq p - 1$. So g has order p, and for $h = c_{j_1}^{\pm 1} \cdots c_{j_s}^{\pm 1} \in G$ for some $s \in \mathbb{N}$,

$$gh = c_{i_1}^{\pm 1} \cdots c_{i_m}^{\pm 1} c_{j_1}^{\pm 1} \cdots c_{j_s}^{\pm 1} = c_{j_1}^{\pm 1} \cdots c_{j_s}^{\pm 1} c_{i_1}^{\pm 1} \cdots c_{i_m}^{\pm 1} = hg$$

since the cycles commute. Thus G is abelian, and G is an elementary abelian p-group that is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^k$.

A natural isomorphism $G \to (\mathbb{Z}/p\mathbb{Z})^k$ is given by $c_i \mapsto e_i$, where e_i is the element of $(\mathbb{Z}/p\mathbb{Z})^k$ with a 1 in the ith entry and 0s elsewhere. Note that here, we use multiplicative notation for G, as a permutation group.

Note that G is intransitive, as the orbits under the natural action are the elements of the cycles $c_1, \ldots, c_k$ and the singleton sets $\{kp+1\}, \ldots, \{n\}$.

However, elementary abelian permutation groups can be transitive, as shown in the following example.

Example 2.78. A transitive elementary abelian permutation group is

$$H = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\},$$

which is a permutation representation of the Klein 4-group $(\mathbb{Z}/2\mathbb{Z})^2$ (as every nontrivial element has order 2). However, it is not primitive: $\Sigma = \{\{1,2\},\{3,4\}\}$ is a block system, as shown by the below GAP code:

```
gap> H := Group([ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]);
Group([ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ])
gap> StructureDescription( H );
"C2 x C2"
gap> IsTransitive( H );
true
gap> IsPrimitive( H );
false
gap> Blocks( H, [ 1, 2, 3, 4 ] );
[ [ 1, 2 ], [ 3, 4 ] ]
```

Chapter 3

Preliminary concepts from complexity theory

Much of this chapter is adapted from [29].

The fundamental problem at the heart of **complexity theory** is, "what makes some problems computationally hard and others easy?" To do so, we generally need to analyse the running time of an *algorithm* that solves a problem. However, the exact running time is often complicated, so one form of estimation which considers large input sizes, called **asymptotic analysis**, considers only the dominating term in the expression. For example, the behaviour of the function $f : \mathbb{Z}^+ \to \mathbb{R}_{\geq 0}$ given by $n \mapsto \log(n) + 3n^4 + 5n + 1$ is largely dependent on the $3n^4$ term for large n, so f is *asymptotically at most* n^4 (if we ignore the coefficient). Formally, we say that $f = O(n^4)$:

Definition 3.1 (big-O notation). Let $f, g : \mathbb{N} \to \mathbb{R}_{\geq 0}$ (or defined on a subset of $\mathbb{N}$). Then f is **big-O** of g, written $f = O(g)$, if there are $c, N \in \mathbb{N}$ such that for $n \geq N$, $f(n) \leq cg(n)$. Then g is an **asymptotic upper bound** for f.

Sometimes, we use big-O notation with multiple variables. Suppose f, g are defined on some subset of $\mathbb{N}^k$. Then $f = O(g)$ if there are $c, N \in \mathbb{N}$ with $f(n_1, \ldots, n_k) \leq cg(n_1, \ldots, n_k)$ whenever $n_i \geq N$ for some i, i.e. when $\|(n_1, \ldots, n_k)\|_\infty \geq N$ (this is the sup norm).

It is perhaps more accurate to write $f \in O(g)$, since $O(g)$ is a class of functions that is dominated by g for large n. For instance, if $f = O(g)$, then $O(f) \subseteq O(g)$. Similarly, if $f = O(g)$ and $g = O(f)$, then $O(f) = O(g)$. Some reasonable arithmetic properties also hold for the big-O notation (note that $\max\{g, \tilde{g}\}$ is defined by $n \mapsto \max\{g(n), \tilde{g}(n)\}$):

- If $f = O(g)$ and $\tilde{f} = O(\tilde{g})$, then $f\tilde{f} = O(g\tilde{g})$ (i.e. $fO(g) = O(fg)$).
- If $f = O(g)$ and $\tilde{f} = O(\tilde{g})$, then $f + \tilde{f} = O(\max\{g, \tilde{g}\})$ (in practice, choose the larger of g and $\tilde{g}$ where n is large).
- If $f = O(g)$ and $\tilde{f} = O(g)$, then $f + \tilde{f} = O(g)$.
- If $f = O(g)$ and $\alpha > 0$, then $\alpha f = O(g)$ (i.e. $\alpha O(g) = O(\alpha g) = O(g)$).
- If $f(n) \to 0$ as $n \to \infty$, then $(1 \pm f)^{-1} = 1 + O(f)$.

We often also write that $f = h + O(g)$ to denote that $f - h = O(g)$. Some common classes of functions encountered in analysing runtime of algorithms, sorted by increasing growth speed, include constant time $O(1)$, logarithmic time $O(\log n)$, linear time $O(n)$, quasi-linear time $O(n \log n)$, quadratic time $O(n^2)$, polynomial time $O(n^k)$ for integer $k \geq 3$, exponential time $O(2^n)$, and factorial time $O(n!)$. A simple formula for the g in $f = O(g)$ is often desired, so "lower order terms" are usually ignored. Note that throughout this thesis, log denotes the base-2 logarithm.

Definition 3.2. Let $f, g : \mathbb{N} \to \mathbb{R}_{>0}$. Then f is **asymptotic** to g, written $f \sim g$, if $f(n)/g(n) \to 1$ as $n \to \infty$.

Asymptoticity is an equivalence relation. Note that if $g \sim \tilde{g}$, then clearly $fg \sim f\tilde{g}$; moreover, if $f = O(g)$, then $f = O(\tilde{g})$ (since if $f(n) \leq cg(n)$ for $n \geq N$, by taking $\epsilon = 1/2$ in "$\tilde{g}/g \to 1$" we get $f(n) \leq (2c)\tilde{g}(n)$ for large n).

A **greedy algorithm** is an algorithm that selects a locally optimal choice at each stage. On the other hand, a **brute force algorithm** is one that systematically enumerates all candidate solutions to find the best solution to the problem. A greedy algorithm is often much more efficient than a brute force algorithm, however, they do not always solve a given computational problem (optimally). The class of problems that greedy algorithms solve optimally is related to the combinatorial idea of a *matroid*, of which a generalisation, the *polymatroid*, is mentioned in [3].

Example 3.3 (membership test). Recall the membership test (Algorithm 2.69) which, given a permutation group $G \leq \mathrm{Sym}(\Omega)$, tests if $g \in G$, given a base $[\beta_1, \ldots, \beta_r]$ for G and associated transversals $T_1, \ldots, T_r$ of the stabiliser chain. The inner "for" loop runs at most $|T_i|$ times for each i, and within it, we just compute the image of β_i under h and t_i and may perform a product; we consider these constant time operations. The outer "for" loop runs at most r times. Thus the algorithm runs in $O(r \max_i |T_i|)$ time.

Example 3.4 (orbit-stabiliser algorithm). Recall the orbit-stabiliser algorithm (Algorithm 2.72) which computes, for finitely generated $G = \langle X \rangle$ acting on Ω and $\alpha \in \Omega$, the orbit α^G, a generating set for the stabiliser $G_\alpha = \langle S \rangle$, and a transversal T of G_α in G. It runs in $O(|\alpha^G|^2|X|)$ time, where we assume that appending to lists and calculations with the group action can be performed in constant $O(1)$ time. This is because the "while" loop (line 3) runs $|\alpha^G|$ times; within it, the "for" loop over $\mathcal{E}$ (line 5) runs $2|X|$ times; within this, in the worst case scenario we have $o^x \in \mathcal{O}$ (line 7) and we iterate through T ($O(|\alpha^G|)$ times by Corollary 2.52) to find j such that $o^x = \alpha^{T[j]}$.

3.1 Complexity classes

For the purposes of this thesis, a **Turing machine** M is a model of a general purpose computer, with unlimited and unrestricted memory. It computes on an infinite "tape" according to a deterministic rule (called a **transition function**) until it decides to produce an output, which is to either *accept* or *reject*; otherwise it will go on forever, never halting — we say that M *loops*. Importantly, a Turing machine can do everything that a real computer can do; thus, if a Turing machine cannot solve a problem in a certain framework, neither can a real computer.

A Turing machine M takes inputs, which are strings. A **string** is a finite sequence of symbols from an **alphabet**, which is a nonempty finite set of elements called *symbols*. A **language** L is a set of strings; if M accepts strings in L, then the language L is **recognised** by M. Two machines are **equivalent** if they recognise the same language.

A language L is **decidable** if there is a Turing machine M that recognises L and halts on all inputs; M is called a **decider** for L. Note that most languages are not Turing-recognisable, because the set of all Turing machines (up to equivalence) turns out to be countable, yet there are uncountably many languages, and each Turing machine can recognise a single language. (This is Corollary 4.18 in [29].)

A *computational problem* is a problem that can be solved by an algorithm. A **decision problem** is a problem that can be posed as a *yes-no* question for its input values, and every decision problem A corresponds with the membership problem of a language L. This can be answered in the following way: given a Turing machine M that recognises L, does M accept the input? We use *encodings* to translate between A and L. (Note that multiple problems can correspond to the same language and vice versa.) A language is decidable if and only if corresponding decision problems are decidable. Thus for our purposes, we will ignore languages and work at the level of problems.

A **nondeterministic Turing machine** is a Turing machine M for which at any point in the computation, M may proceed according to several possibilities; its computation can be modelled by an (infinite) tree. We can extend the above definitions in a straightforward way to nondeterministic Turing machines; the *time* for a decider, i.e. one that halts on all inputs, is defined in [29] as the time used by the longest computational branch. Since every nondeterministic Turing machine has an equivalent (deterministic) Turing machine (Theorem 3.16 in [29]), a problem is decidable if and only if some nondeterministic Turing machine halts on all valid inputs.

Definition 3.5. Let $t : \mathbb{N}^k \to \mathbb{R}_{\geq 0}$ be a function. The **(time) complexity class** $\mathrm{TIME}(t)$ is the collection of decision problems that are decidable by an $O(t)$-time (*deterministic*) Turing machine (one that halts in $O(t)$-time given an input string of size n). Similarly, $\mathrm{NTIME}(t)$ is the collection of decision problems that are decidable by an $O(t)$-time *nondeterministic* Turing machine.

Note that in practice, the inputs to algorithms are not strings; we first encode the inputs $X_1, \ldots, X_k$ into a single string $\langle X_1, \ldots, X_k \rangle$ of size $n = n(X_1, \ldots, X_k)$. Then a problem in $\mathrm{TIME}(t)$ is decided by a Turing machine that halts in $O(t) = O(t(n)) = O(t(n(X_1, \ldots, X_k)))$-time in the input size $n = n(X_1, \ldots, X_k)$.

In [29], Sipser notes that every $O(t)$-time nondeterministic Turing machine has an equivalent $2^{O(t)}$-time (deterministic) Turing machine. This is an at most *exponential* difference in time complexity of problems on deterministic and nondeterministic Turing machines; this is a large difference, as an exponential dominates any polynomial. But in some cases, alternative algorithms give rise to smaller differences in the complexity of problems.

The classes P and NP

Definition 3.6. **P** is the class of decision problems that are decidable in polynomial time (in the input size) on a (deterministic) Turing machine, i.e. $\mathrm{P} = \bigcup_p \mathrm{TIME}(p)$, where p ranges over all (multivariate) polynomials.

The class P is important because it roughly corresponds to the class of problems that are deemed realistically solvable on a computer. Even though a running time of $O(n^k)$ for large k is impractical for large inputs n, once a polynomial time algorithm has been found for a problem for the first time, that often indicates further reductions in complexity will follow. Moreover, it is invariant for all models of computation that are polynomially equivalent to the deterministic Turing machine, so it is not affected by particulars of the model being used; thus, a high-level description of an algorithm suffices.

Lemma 3.7. *$O(\max\{f, g\}) = O(f + g)$; by extension, $O(\max_{1 \leq i \leq k}\{f_i\}) = O(f_1 + \cdots + f_k)$. Thus, if there exist polynomials p_i such that $t_i = O(p_i)$ for $1 \leq i \leq k$, a problem decidable in $O(\max_{1 \leq i \leq k}\{t_i\})$-time is in* P.

Proof. For $n \in \mathbb{N}$, $\max\{f(n), g(n)\} \leq f(n) + g(n)$ since $f(n), g(n) \geq 0$, so $\max\{f, g\} = O(f + g)$. Conversely, $f(n) + g(n) \leq 2\max\{f(n), g(n)\}$, so $f + g = O(\max\{f, g\})$. Thus, $O(\max\{f, g\}) = O(f + g)$. The extended statement follows by induction on k.

Now if $t_i = O(p_i)$ for all i, then $O(\max_{1 \leq i \leq k}\{t_i\}) = O(t_1 + \cdots + t_k) = O(p_1 + \cdots + p_k)$; a problem decidable in this time is in $\mathrm{TIME}(p_1 + \cdots + p_k)$, thus in P (as $p_1 + \cdots + p_k$ is a polynomial). □

Example 3.8 (membership test). Recall the membership test algorithm (Algorithm 2.69) for $g \in G$ runs in $O(r \max_i |T_i|)$ time, where $G \leq \mathrm{Sym}(\Omega)$ has base $[\beta_1, \ldots, \beta_r]$ and associated transversals $T_1, \ldots, T_r$ of the stabiliser chain. By Lemma 3.7, $O(r \max_i |T_i|) = O(r(|T_1| + \cdots + |T_r|))$. Thus, the problem of membership in G is in the class P, since we consider the inputs of the problem to comprise $r, |T_1|, \ldots, |T_r|$ (among other things), which describe the structure or attributes of G.

Example 3.9 (orbit-stabiliser algorithm). Recall the orbit-stabiliser algorithm (Algorithm 2.72) for $\alpha \in \Omega$ runs in $O(|\alpha^G|^2|X|)$ time, where a finitely generated group $G = \langle X \rangle$ acts on Ω. Again, this is a polynomial time algorithm in the inputs, so the problem of computing the orbit and (a generating set for the) stabiliser of α and a transversal of G_α is in the class P.

Example 3.10 (Schreier-Sims algorithm). The Schreier-Sims algorithm extends a sequence $\tilde{B} \subseteq \Omega$ and generating set X to a BSGS (B, S) for $G = \langle X \rangle \leq \mathrm{Sym}(\Omega)$ (i.e. $\tilde{B}$ is extended to B and X is extended to S); this is a naïve description of the algorithm with inefficiencies. In [19], Knuth describes another version of the Schreier-Sims algorithm which improves the running time to $O(n^5 + rn^2)$ (which is certainly polynomial time) where r is the length of the base B and $n = |\Omega|$ is the degree of G.

Where P is the class of decision problems decidable in polynomial time on a deterministic Turing machine, NP is the analogous class for nondeterministic Turing machines.

Definition 3.11. **NP** is the class of decision problems that are decidable in polynomial time on a *nondeterministic* Turing machine, i.e. $\mathrm{NP} = \bigcup_p \mathrm{NTIME}(p)$ where p ranges over all polynomials. We often say a problem in NP is a **nondeterministic polynomial time** problem, or simply a **NP-problem**.

Clearly P ⊆ NP. An equivalent characterisation of NP, which is often more useful, is the class of decision problems with *polynomial time verifiers*. A **verifier** is an algorithm that uses additional information (called a *certificate*) to verify (but not necessarily find) a solution.

Example 3.12. Suppose $G \leq \mathrm{Sym}(n)$ acts on a set Ω. One way of seeing that the problem of finding a base for G is in NP is to observe that it has a polynomial time verifier. A certificate for G is a base $B = [\beta_1, \ldots, \beta_r]$ for G: a naïve approach is to use the orbit-stabiliser algorithm (Algorithm 2.72) to check that $G_{\beta_1,\ldots,\beta_r} = ((G_{\beta_1})\ldots)_{\beta_r} = 1$ in polynomial time. (In fact, it is in P, by Example 3.10.)

The class NP is important as it contains many problems of practical interest (for instance, the well-known knapsack, travelling salesman, and Hamiltonian path problems). Moreover, showing that a problem is in the class P is often much more difficult than showing it is NP, as we need to find a polynomial time (deterministic) algorithm for solving it. However, it is also difficult to argue that a problem in the class NP is *not* in the class P, as we must show that *no* algorithm that solves the problem can run in polynomial time. In fact, this problem is so hard that it is the famous P versus NP conjecture, which carries a US$1 million prize for a proof or disproof:

Conjecture 3.13 (P versus NP problem). P ≠ NP, *that is, there are problems that can be verified in polynomial time but cannot be solved in polynomial time.*

Reducibility and NP-completeness

The primary method for showing that problems are computationally unsolvable is **reducibility**. A **reduction** is a method of converting one problem A to another problem B such that a solution to B can be used to solve A. Reducibility says nothing about the solvability of A or B alone, but only the solvability of A given a solution to B. (Recall that solutions to decision problems can be in the affirmative or negative.)

If A is reducible to B, then solving A cannot be harder than solving B, since a solution to B gives a solution to A. So if B is decidable, then so is A. Equivalently, if A is undecidable and reducible to B, then B is undecidable.

Definition 3.14. A problem A is **polynomial time reducible** to a problem B if there is a **Karp reduction** of A to B, i.e. a function that is computable by a Turing machine in polynomial time such that a solution/non-solution to B yields a solution/non-solution to A.

Definition 3.15. A problem B is **NP-complete** if $B \in$ NP and every problem $A \in$ NP is polynomial time reducible to B.

The above discussion leads to the following result, which says that to answer the conjecture that P = NP in the affirmative, it suffices to find a NP-complete problem that is in the class P.

Theorem 3.16. *If a problem B is NP-complete and $B \in$ P, then* P = NP. □

Clearly, the non-resolution of the P versus NP conjecture implies that we do not currently know of any NP-complete problems that are in P; however, it is suspected that P ≠ NP, so it widely believed that such problems do not exist. Interestingly however, for reasons not well understood, [29] notes that most problems in NP can be shown to either be in P or be NP-complete. Additionally, NP-complete problems arise in many fields. A similar property to NP-completeness is NP-hardness, where we drop the condition that the problem itself is in NP (i.e. that it can be verified in polynomial time), or that it is even decidable:

Definition 3.17. A problem B is **NP-hard** if every problem $A \in$ NP is polynomial time reducible to B.

Thus a NP-hard problem is informally "at least as hard as any NP-problem"; they may not even be decidable. However, finding a polynomial time solution to a NP-hard problem would imply that P = NP.

One NP-complete problem that is relevant to this thesis is the problem of finding an exact cover by 3-sets (X3C), as this is used in [3] to show that the problem of finding a small bases for a group G is NP-hard:

Example 3.18 (X3C). Consider (Y, M) where Y is a finite set with $|Y| = 3q$ and M is a collection of 3-element subsets of Y. The yes-no *question*, as given in [13], is, "does M contain an exact cover for Y, i.e. a subcollection $M' \subseteq M$ such that each element of Y is in exactly one member of M'?" This exact 3-cover problem is NP-complete, as by the *Cook-Levin theorem* (see Theorem 7.37 in [29]), every problem in NP is reducible to SAT (the Boolean satisfiability problem), which is shown to be reducible to X3C (more precisely, the related "exact cover" problem where we drop the restriction to 3-sets) in [18].

In [13], Garey and Johnson note that the problem remains NP-complete if no element of Y occurs in more than three members of M, but it is solvable in polynomial time if no element of Y occurs in more than two members of M. (A related problem, the exact cover by 2-sets, is in the class P using graph matching techniques.)

Chapter 4

Blaha: computing minimum bases is NP-hard

In this chapter, we present a self-contained expansion and explanation of Blaha's paper [3], in particular its results and proofs, many of which are not explained or only done so very briefly. In [3], Blaha shows that the problem of finding a minimum base for a permutation group is NP-hard, even when restricted to cyclic or elementary abelian groups. He also finds a sharp bound for the size of a base given by a particular greedy algorithm, to determine whether it is a good approach for computing small bases.

Throughout this chapter, take $G \leq \mathrm{Sym}(n)$ to be a permutation group (this is without loss of generality, since of course if $|\Omega| = n$, then $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(n)$), and that $B = [\beta_1, \ldots, \beta_r]$ is a base for G with associated stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ (with $G^i = G^{i-1}_{\beta_i}$). Recall from Definition 2.56 that the size of a minimum base for G is denoted $b(G)$.

First, we define the **minimum base (MB) problem**: let $G \leq \mathrm{Sym}(n)$ given by generators and a positive integer $N \leq n$. The *question* is: "does there exist a base for G of size no more than N?"

Blaha proves in [3] that the minimum base problem is NP-hard since it is NP-complete, i.e. it is in NP, and that every problem in NP is polynomial time reducible to it. The first claim is straightforward to verify:

Lemma 4.1. *The MB problem is in NP, i.e. verifiable in polynomial time.*

Proof. Suppose a candidate base $B = [\beta_1, \ldots, \beta_r]$ for G is given. Simply check if $r \leq N$ (which can be performed in polynomial time with any reasonable implementation of an ordered list structure), then verify that B is indeed a base for G using a polynomial time algorithm (iteratively compute stabilisers using orbit-stabiliser algorithm). □

It remains to show that any problem in NP is polynomial time reducible to MB. Blaha describes a Karp reduction from exact cover by three-sets (X3C) to MB. In particular, showing that MB is NP-hard for G a cyclic group or elementary abelian group implies the NP-hardness of MB for arbitrary G; we analyse these cases in the subsequent sections.

We also describe a greedy algorithm (suggested in [5]) for finding a base for a permutation group G. (See the appendix for an implementation in GAP, which we use later on in this thesis.)

Algorithm 4.2 (Greedy base algorithm). *Let $G \leq \mathrm{Sym}(\Omega)$ be a permutation group that acts naturally on Ω. Construct a base $B = [\beta_1, \ldots, \beta_r]$ for G by repeatedly choosing $\beta_i \in \Omega$ from a largest orbit of G^{i-1} (where $G^0 = G$), then constructing $G^i = G^{i-1}_{\beta_i}$ until we reach $G^r = 1$. (Then $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$ is the associated stabiliser chain.)*

Since $|G^i| = |G^{i-1}|/|\beta_i^{G^{i-1}}|$ by the orbit-stabiliser theorem, this greedy algorithm chooses β_i that minimises $|G^i|$ at every stage. So it is reasonable to assume that the length r of the base B will be "small". However, does it construct a *minimum base*? Blaha shows in [3] that this is not the case.

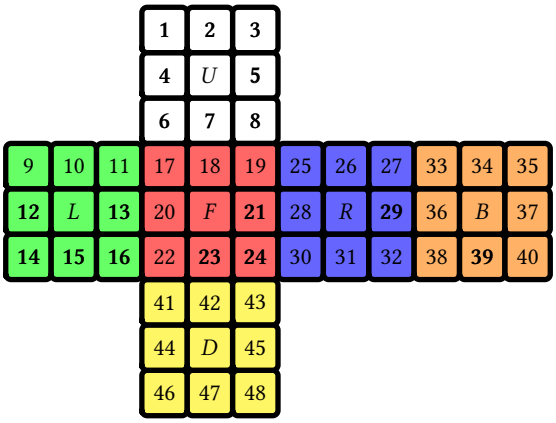
Note that the greedy base algorithm is in the class P. This follows from the fact that we may repeatedly use the orbit-stabiliser algorithm to compute orbits and stabilisers for each subsequent β_i found. The process yields a nonredundant base by Theorem 2.23, since we choose a largest orbit at each stage; if every G^{i-1}-orbit has size 1, then every stabiliser $G_\alpha^{i-1} = G^{i-1}$, and the intersection $\bigcap_{\alpha\in\Omega} G_\alpha^{i-1} = G^{i-1}$ is the kernel of the G^{i-1}-action (Proposition 2.19), thus $G^{i-1} = 1$ since the action is faithful. This also implies that the process necessarily terminates; in particular, $r \leq \log|G|$ by Lemma 2.57.

Before we continue with Blaha [3], we first apply the greedy base algorithm to the Rubik's group.

Example 4.3. Using the previous definition of the Rubik's group G from Example 2.41 and our implementation in GAP of the (randomised) greedy base algorithm as `GreedyBase`, we compute that

$$B = [1, 2, 4, 3, 5, 7, 6, 12, 8, 13, 14, 15, 21, 16, 23, 24, 29, 39]$$

is a base of length 18 for G. Below, we bold the stickers in B.



Similar to the example in Example 2.71, it also contains a sticker from each of 7 corners and 11 edges; the only difference is that the base computed by `BaseOfGroup` contains 31 instead of 39 (both edge stickers).

Using GAP, we verify that B is indeed a base, by seeing that $G_{(B)} = 1$. Also, we see that if we omit 39 from B, we get that the pointwise stabiliser is $\langle(31, 45)(39, 47)\rangle \neq 1$, so the resulting list is not a base for G. Thus, if we fix 7 corners and only 10 edges (including orientation), there is a valid nontrivial Rubik's cube move that interchanges only the two remaining edges. Similarly, if we omit 29 from B, we get that the pointwise stabiliser is $\langle(29, 36)(31, 45)\rangle \neq 1$, so the resulting list is not a base for G. Thus, if we fix 11 edges and only 6 corners (including orientation), there is a valid nontrivial Rubik's cube move that interchanges only the two remaining corners. (See the appendix for GAP code relating to this example.)

These observations show that $b(G) = 18$; this is an original result.

Theorem 4.4. *Let G be the Rubik's group. Then $b(G) = 18$.*

Proof. First, note that Example 4.3 shows that $b(G) \leq 18$. Now, it suffices to include one sticker per corner or edge in a base (as fixing the sticker fixes the entire corner or edge). Moreover, if we fix any 7 corners (and all edges), then the remaining corner is fixed too, including orientation, by symmetry and Example 4.3. Similarly, fixing any 11 edges (and all corners) fixes the remaining edge, including orientation.

If a "partial" base $\tilde{B}$ for G contains 17 stickers, with v vertex stickers and e edge stickers, then $v + e = 17$ with $v \leq 7$ and $e \leq 11$ from above. So $(v, e) \in \{(6, 11), (7, 10)\}$, but from Example 4.3 and by symmetry (there is nothing else special about the elements of the base B), we know that these cases do not lead to a trivial pointwise stabiliser for $\tilde{B}$. Thus $b(G) > 17$, and the result follows. □

4.1 The general case

NP-hardness of the minimum base problem for cyclic groups

First a preliminary lemma about a cyclic group.

Lemma 4.5 (Lemma 2.1 in [3]). *Given $G = \langle\sigma\rangle \leq \mathrm{Sym}(n)$ and a base $B = [\beta_1, \ldots, \beta_r]$, let $m_k = |\beta_k^G|$. Then for $1 \leq i \leq r$, we have $G^i = \langle\sigma^m\rangle$, where $m = \mathrm{lcm}(m_1, \ldots, m_i)$.*

Proof. Note that since $G = \langle\sigma\rangle$, the set $\beta_k^G = \{\beta_k^{\sigma^j} : j \in \mathbb{Z}\}$ comprises elements of the cycle in σ containing β_k. So $|\beta_k^G| = m_k$ divides j if and only if σ^j fixes β_k. Since $m_1, \ldots, m_i \mid m$, we have that σ^m fixes $\beta_1, \ldots, \beta_i$, so $\sigma^m \in G^i$, from which it follows that $\langle\sigma^m\rangle \subseteq G^i$.

Now suppose $\sigma^j \in G^i$, i.e. σ^j fixes $\beta_1, \ldots, \beta_i$. Then $m_1, \ldots, m_i \mid j$ from above, so $m = \mathrm{lcm}(m_1, \ldots, m_i) \mid j$, say $j = km$ with $k \in \mathbb{Z}$. Then $\sigma^j = \sigma^{km} = (\sigma^m)^k \in \langle\sigma^m\rangle$, so $G^i \subseteq \langle\sigma^m\rangle$. □

Recall that the *prime number theorem* gives that $p_n \sim n \log n$ for large n, where p_n is the nth prime number; we use this below. We aim to show that MB is NP-complete even for G a cyclic group, by providing a construction from [3] in the following. Then, we discuss the condition for the construction to yield a base for G, and by giving a Karp reduction to an NP-complete problem, conclude that the MB problem is NP-complete in this framework, following the proof in [3].

Let (Y, M) be an instance of X3C as described in Example 3.18, with $|Y| = 3q$ and $|M| = k$; suppose without loss of generality that the 3-sets in M cover Y (or else we clearly get a "no" for X3C). Let $P = \{p_1, p_2, \ldots, p_{3q}\}$ denote the first $3q$ primes, and let $f : Y \to P$ be a bijection. Then for each 3-set $m = \{x, y, z\} \in M$, define $s_m = f(x)f(y)f(z) \in \mathbb{N}$; the $\{s_m\}_{m\in M}$ are all distinct.

Now set $n = \sum_{m\in M} s_m \in \mathbb{N}$, and construct $\sigma \in \mathrm{Sym}(n)$ whose cycle decomposition comprises an s_m-cycle c_m for each $m \in M$ (k disjoint cycles in total, all different lengths). Consider an instance of MB with $G = \langle\sigma\rangle \leq \mathrm{Sym}(n)$ and $N = q$. (Note that indeed $N \leq n$: the elements of M cover Y, so there is $x \in m = \{x, y, z\} \in M$ with $f(x) = p_{3q} \geq 3q$. Then $s_m = f(x)f(y)f(z) \geq 3q$, so $n = \sum_{m\in M} s_m \geq 3q \geq q$.) This is a Karp reduction, since by the prime number theorem, $p_{3q} \sim 3q \log 3q \sim 3q \log q$, and so $s_m = O(p_{3q}^3) = O((q \log q)^3)$ for $m \in M$ and thus $n = O(k(q \log q)^3)$ (as $|M| = k$); this is certainly polynomial time in q, k (since $q \log q = O(q^2)$).

Now for $r \leq q$, let $B = [\beta_1, \ldots, \beta_r] \subseteq \{1, \ldots, n\}$ be such that each β_i is a point in the s_{m_i}-cycle c_{m_i} of σ, and define the stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r$ as usual (if B is not a base for G, then $G^r \neq 1$). Recall that the order of σ is $\mathrm{lcm}\{s_m\}_{m\in M} = p_1 p_2 \cdots p_{3q} = |G|$ since the $\{s_m\}_{m\in M}$ contain all primes in P (as M covers Y) and $G = \langle\sigma\rangle$ is cyclic. First note that B is a base for G if and only if $G^r = 1$. Let $s = \mathrm{lcm}(s_{m_1}, \ldots, s_{m_r})$, where we note that $s_{m_i} = |\beta_i^G|$ are the orbit sizes as $G = \langle\sigma\rangle$ is cyclic. We need a lemma:

Lemma 4.6. *Using the above construction, $B = [\beta_1, \ldots, \beta_r]$ is a base for $G = \langle\sigma\rangle$ if and only if $s = |G|$.*

Proof. ($\Longrightarrow$) By Lemma 4.5, if B is a base for G, then $1 = G^r$, and $G^r = \langle\sigma^s\rangle$, since $s = \mathrm{lcm}(s_{m_1}, \ldots, s_{m_r})$. Then s divides $|G|$ by $\{s_{m_1}, \ldots, s_{m_r}\} \subseteq \{s_m\}_{m\in M}$, and $|G|$ divides s by $\langle\sigma^s\rangle = 1$, so $s = |G|$.

($\Longleftarrow$) Since $G = \langle\sigma\rangle$, it follows that $|G| = \mathrm{lcm}\{s_m\}_{m\in M}$ is the order of σ. Suppose $\tau = \sigma^\ell$ fixes B pointwise; then $\beta_i^{\sigma^\ell} = \beta_i$ if and only if $s_{m_i} \mid \ell$ for all i (since β_i is in a s_{m_i}-cycle), so $s = \mathrm{lcm}(s_{m_1}, \ldots, s_{m_r}) \mid \ell$. But $s = |G|$ so $|G|$ divides ℓ, from which it follows that $\tau = \sigma^\ell = 1_{\mathrm{Sym}(n)}$, so that B is a base for G. □

Now, we are ready to prove the main result of this subsection, which is Theorem 3.1 in [3].

Theorem 4.7 (Blaha, 1992). *MB is NP-complete even for G a cyclic group.*

Proof. Consider the instance (Y, M) of X3C as described above. By Lemma 4.6, B is a base for G if and only if $s = |G|$.

Note that $s = |G| = p_1 \cdots p_{3q}$ if and only if $\ell = 3q$, where $s = \mathrm{lcm}(s_{m_1}, \ldots, s_{m_r})$ decomposes as a product of (exactly) ℓ primes. But $\ell \leq 3r$ (since each s_m is a product of three distinct primes) and so $\ell \leq 3r \leq 3q = \ell$ (since $r \leq q$) if and only if $s = |G|$; equivalently, $s = |G|$ if and only if $r = q$, from which it follows that the $s_{m_1}, \ldots, s_{m_r}$ are all relatively prime. But this occurs if and only if the $m_1, \ldots, m_r \in M$ are all disjoint. In summary, $B = [\beta_1, \ldots, \beta_r]$ is a base for G with $r \leq q$ if and

only if $r = q$ and the 3-sets $m_1, \ldots, m_r \in M$ form an exact cover of Y (answering the X3C problem). This is the desired Karp reduction from X3C to MB, and thus MB is NP-complete as X3C is known to be NP-complete (Example 3.18). □

Greedy base analysis for cyclic groups

Remark 4.8. Using the construction in Theorem 4.7, we can build cyclic groups for which the greedy base algorithm *fails* to find a minimum base. In fact, a similar construction of a cyclic group $G = \langle\sigma\rangle$ using a reduction from X2C (the exact 2-cover, defined analogously to X3C) to MB already causes it to fail.

For this, let $Y = \{a, b, c, d\}$ and $M = \{\{a, d\}, \{b, c\}, \{b, d\}\}$. Then let $f : Y \to \{2, 3, 5, 7\}$ be given by $a \mapsto 2$, $b \mapsto 3$, $c \mapsto 5$, $d \mapsto 7$. Then $n = \sum_{m\in M} s_m = 2 \cdot 7 + 3 \cdot 5 + 3 \cdot 7 = 50$ and we construct $\sigma \in \mathrm{Sym}(50)$ with cycle type $(21, 15, 14)$. (Note that the order of σ is $\mathrm{lcm}(21, 15, 14) = 210$.) This construction is found in [3].

Now we consider the greedy approach to finding a base. Set $G^0 = G$. The largest orbit of G^0 comprises elements of the 21-cycle $c_{\{b,d\}}$; pick β_1 in this. Then $G^1 = G^0_{\beta_1} = \langle\sigma^{21}\rangle$; σ^{21} comprises twenty-one 1-cycles (comprising elements of the 21-cycle $c_{\{b,d\}}$ in σ), three 5-cycles (comprising elements of the 15-cycle $c_{\{b,c\}}$ in σ), and seven 2-cycles (comprising elements of the 14-cycle $c_{\{a,d\}}$ in σ). A largest orbit of G^1 is one of the 5-cycles; pick β_2 in one of them. Then $G^2 = G^1_{\beta_2} = \langle\sigma^{105}\rangle$; σ^{105} comprises $(21 + 15)$ 1-cycles (comprising elements of the cycles $c_{\{b,d\}}$ and $c_{\{b,c\}}$ in σ) and seven 2-cycles (comprising elements of the cycle $c_{\{a,d\}}$ in σ). A largest orbit of G^2 is one of the 2-cycles; pick β_3 in one of them. Then $G^3 = G^2_{\beta_3} = 1$, so $B = [\beta_1, \beta_2, \beta_3]$ is a base for G of size 3, found via the greedy algorithm.

However, if we set $\tilde{G}^0 = G$, and choose $\tilde{\beta}_1$ from the 15-cycle $c_{\{b,c\}}$ in σ, then $\tilde{G}^1 = \tilde{G}^0_{\tilde{\beta}_1} = \langle\sigma^{15}\rangle$; σ^{15} has (15+14) 1-cycles and three 7-cycles (comprising elements of the 21-cycle $c_{\{b,d\}}$), so choosing $\tilde{\beta}_2$ from a 7-cycle results in $\tilde{B} = [\tilde{\beta}_1, \tilde{\beta}_2]$ being a base for G of size 2. This is a minimum base for G, since G does not act transitively on $\{1, \ldots, n\}$ (and thus we do not have a base of size 1).

In the above reduction of X3C to MB, as the problem size of X3C increases, the sizes of the orbits in the constructed group $G = \langle\sigma\rangle$ increase, since the primes involved are larger. The following section uses elementary abelian groups to show that even if the orbits are bounded, it is still not possible to solve the MB problem efficiently.

4.2 The case of bounded orbits

The following technical construction from [3] is repeatedly used in the following lemmas in this section. It closely resembles a construction given immediately after Remark 2.38.

Example 4.9. Suppose X is a finite set with $|X| = n$.

- Let $\{\sigma_x\}_{x\in X}$ be a fixed set of generators for the elementary abelian 2-group $(\mathbb{Z}/2\mathbb{Z})^n$ (this is necessarily a minimal generating set); each generator σ_x has order 2.
- For $Y \subseteq X$, define the subgroup $G(Y) = \langle\sigma_x \mid x \in Y\rangle$ (note that $(\mathbb{Z}/2\mathbb{Z})^n \cong G(X)$).
- Extend the right regular $G(Y)$-action $\mathcal{R} : G(Y) \to \mathrm{Sym}(G(Y))$ to the $G(X)$-action $\mathcal{R}_Y : G(X) \to \mathrm{Sym}(G(Y))$, in which $\{\sigma_x\}_{x\in X\setminus Y}$ act trivially (i.e. generators $\sigma_x \mapsto 1_{\mathrm{Sym}(G(Y))}$ for $x \in X \setminus Y$, then extend homomorphically). (So $\mathcal{R}_Y$ projects onto the right regular action on $G(Y)$ and the trivial action on $G(X \setminus Y)$, where $G(X) \cong G(Y) \times G(X \setminus Y)$.)
- Now suppose $\mathcal{C}$ is a collection of subsets of X, and let $\Omega_{\mathcal{C}} = \bigsqcup_{Y\in\mathcal{C}} G(Y)$ be the *disjoint* union of the *sets* $G(Y)$.
- Consider the induced action $\mathcal{R}_{\mathcal{C}} : G(X) \to \mathrm{Sym}(\Omega_{\mathcal{C}})$ (from the $\mathcal{R}_Y$ for $Y \in \mathcal{C}$), where for $\alpha \in \Omega_{\mathcal{C}}$, we have $\alpha \in G(Y)$ for precisely one $Y \in \mathcal{C}$; then set $\alpha^{\mathcal{R}_{\mathcal{C}}(\sigma)} = \alpha^{\mathcal{R}_Y(\sigma)} \in G(Y)$. (That is, for $\sigma \in G(X)$, we glue together the permutations $\mathcal{R}_Y(\sigma) : G(Y) \to G(Y)$ for $Y \in \mathcal{C}$ to get a permutation $\mathcal{R}_{\mathcal{C}}(\sigma) : \Omega_{\mathcal{C}} \to \Omega_{\mathcal{C}}$.) Each disjoint copy of $G(Y) \subseteq \Omega_{\mathcal{C}}$ is an *orbit* under $\mathcal{R}_{\mathcal{C}}$; thus $G(X)$ acts on each $G(Y)$ (Remark 2.38), precisely according to $\mathcal{R}_Y$.
- For $Z \subseteq X$, let $G_{\mathcal{C}}(Z) = \mathcal{R}_{\mathcal{C}}[G(Z)] \leq \mathrm{Sym}(\Omega_{\mathcal{C}})$ be the image of the $G(Z)$-action $\mathcal{R}_{\mathcal{C}}$, a permutation group. Then $G_{\mathcal{C}}(Z)$ acts on $\Omega_{\mathcal{C}}$ naturally. Note that $G_{\mathcal{C}}(Z) = \langle\mathcal{R}_{\mathcal{C}}(\sigma_x) \mid x \in Z\rangle$.

In this construction, we begin with a subgroup $G(Y)$ of $G(X)$ and extend its right regular action to $G(X)$ trivially to get $\mathcal{R}_Y$, which is transitive. Then for a collection $\mathcal{C}$ of subsets Y, this induces an action $\mathcal{R}_\mathcal{C}$ on the disjoint union $\Omega_\mathcal{C}$ of the $G(Y)$, with an element $\sigma \in G(X)$ acting on $\alpha \in G(Y) \subseteq \Omega_\mathcal{C}$ via $\mathcal{R}_Y$. The image of $G(Z)$ under this action is $G_\mathcal{C}(Z)$.

Note that for $Y, Z \subseteq X$, an element $\sigma \in G(Y)$ has, up to permutation of factors (since $G(Y)$ is abelian), a *unique* decomposition $\sigma = \sigma_{x_1} \cdots \sigma_{x_k}$ with each $x_i \in Y$ (distinct). Moreover, $G(Y) \cap G(Z) = G(Y \cap Z)$. (The reverse inclusion is trivial; the forward inclusion relies on the unique decomposition.)

Example 4.10. We illustrate the above construction by setting $n = 3$ and $X = [3]$. We use multiplicative notation for $(\mathbb{Z}/2\mathbb{Z})^3$ (i.e. we actually treat it as C_2^3).

- Note that $G(X) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle = \{1, \sigma_1, \sigma_2, \sigma_3, \sigma_1\sigma_2, \sigma_1\sigma_3, \sigma_2\sigma_3, \sigma_1\sigma_2\sigma_3\}$. Note that each $\sigma_i^2 = 1$ and $\sigma_i\sigma_j = \sigma_j\sigma_i$.
- If $Y = \{1, 3\}$, then $G(Y) = \langle \sigma_1, \sigma_3 \rangle = \{1, \sigma_1, \sigma_3, \sigma_1\sigma_3\} \leq G(X)$.
- The action $\mathcal{R}_Y$ is defined as such: for $\alpha \in G(Y)$ and say $\sigma = \sigma_1\sigma_2\sigma_3 = \sigma_2\sigma_1\sigma_3 \in G(X)$, we have
$$\alpha^{\mathcal{R}_Y(\sigma)} = \alpha^{\mathcal{R}_Y(\sigma_2)\mathcal{R}_Y(\sigma_1\sigma_3)} = (\alpha^{\mathcal{R}_Y(\sigma_2)})^{\mathcal{R}_Y(\sigma_1\sigma_3)} = \alpha^{\mathcal{R}(\sigma_1\sigma_3)} = \alpha\sigma_1\sigma_3.$$
It can be seen that $\mathcal{R}_Y$ acts regularly (like $\mathcal{R}$) for $G(Y)$, and trivially for $G(X \setminus Y) = \langle \sigma_2 \rangle = \{1, \sigma_2\}$. (Note that $G(X) \cong G(Y) \times G(X \setminus Y)$ via $\sigma_1 \mapsto (\sigma_1, 1)$, $\sigma_2 \mapsto (1, \sigma_2)$, $\sigma_3 \mapsto (\sigma_3, 1)$, then extending homomorphically.)
- Let $\mathcal{C} = \{\{1, 3\}, \{2\}, \{2, 3\}\}$. Then
$$\Omega_\mathcal{C} = \bigsqcup_{Y \in \mathcal{C}} G(Y) = G(\{1,3\}) \sqcup G(\{2\}) \sqcup G(\{2,3\}) = \{1, \sigma_1, \sigma_3, \sigma_1\sigma_3\} \sqcup \{1, \sigma_2\} \sqcup \{1, \sigma_2, \sigma_3, \sigma_2\sigma_3\}.$$
- For $\mathcal{R}_\mathcal{C}$ and $\sigma = \sigma_1\sigma_2\sigma_3 \in G(X)$, if say $\alpha = \sigma_2 \in G(\{2\}) \subseteq \Omega_\mathcal{C}$, then $\alpha^{\mathcal{R}_\mathcal{C}(\sigma)} = \sigma_2^{\mathcal{R}_{\{2\}}(\sigma)} = \sigma_2^{\mathcal{R}(\sigma_2)} = \sigma_2\sigma_2 = 1$. But if $\alpha = \sigma_2 \in G(\{2,3\}) \subseteq \Omega_\mathcal{C}$, then $\alpha^{\mathcal{R}_\mathcal{C}(\sigma)} = \sigma_2^{\mathcal{R}_{\{2,3\}}(\sigma)} = \sigma_2^{\mathcal{R}(\sigma_2\sigma_3)} = \sigma_2\sigma_2\sigma_3 = \sigma_3$.
- Now set $Z = \{1, 2\}$, so $G(Z) = \langle \sigma_1, \sigma_2 \rangle = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$. Then $G_\mathcal{C}(Z) = \mathcal{R}_\mathcal{C}[G(Z)]$ contains the permutations $\mathcal{R}_\mathcal{C}(\sigma)$ of $\Omega_\mathcal{C}$ where $\sigma \in G(Z)$. For example, for $\sigma = \sigma_2$ we get the permutation
$$\mathcal{R}_\mathcal{C}(\sigma_2) = \underbrace{(1, \sigma_2)}_{G(\{2\})}\ \underbrace{(1, \sigma_2)(\sigma_3, \sigma_2\sigma_3)}_{G(\{2,3\})} \in \mathrm{Sym}(\Omega_\mathcal{C});$$
note that on $G(\{1,3\}) \subseteq \Omega_\mathcal{C}$, $\mathcal{R}_\mathcal{C}(\sigma_2)$ acts trivially. As a permutation group, $G_\mathcal{C}(Z)$ acts naturally on $\Omega_\mathcal{C}$ and indeed $G_\mathcal{C}(Z) := \{\mathcal{R}_\mathcal{C}(\sigma) : \sigma \in G(Z)\} = \langle \mathcal{R}_\mathcal{C}(\sigma_1), \mathcal{R}_\mathcal{C}(\sigma_2) \rangle$: for $\sigma_1\sigma_2 \in G(Z)$, we have $\mathcal{R}_\mathcal{C}(\sigma_1\sigma_2) = \mathcal{R}_\mathcal{C}(\sigma_1)\mathcal{R}_\mathcal{C}(\sigma_2)$ since $\mathcal{R}_\mathcal{C}$ is an action (thus a homomorphism).

(a) Let us consider $Y = \{1, 3\} \in \mathcal{C}$ and $\alpha \in G(Y)$. Then with $Z = \{1, 2\}$ let us consider the stabiliser
$$G_\mathcal{C}(Z)_\alpha = \{\mathcal{R}_\mathcal{C}(\sigma) : \alpha^{\mathcal{R}_\mathcal{C}(\sigma)} = \alpha \text{ and } \sigma \in G(Z)\}.$$
For $\sigma \in G(Z) = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2\}$, if $\sigma \in G(Z \setminus Y) = G(\{2\})$, then $\mathcal{R}_\mathcal{C}(\sigma)$ acts trivially on $G(Y)$, so $\mathcal{R}_\mathcal{C}(\sigma) \in G_\mathcal{C}(Z)_\alpha$. Conversely, if $\sigma \notin G(\{2\}) = \{1, \sigma_2\}$ then $\sigma = \sigma_1$ or $\sigma = \sigma_1\sigma_2$; in the first case, $\alpha^{\mathcal{R}_\mathcal{C}(\sigma_1)} = \alpha\sigma_1 \neq \alpha$, and in the second case, $\alpha^{\mathcal{R}_\mathcal{C}(\sigma_1\sigma_2)} = \alpha\sigma_1 \neq \alpha$. So $G_\mathcal{C}(Z)_\alpha = G_\mathcal{C}(\{2\}) = G_\mathcal{C}(Z \setminus Y)$.

(b) If $W = Y \cap Z = \{1\}$, then $G(W) = \{1, \sigma_1\}$ and $|G(Y) : G(W)| = |G(Y)|/|G(W)| = 4/2 = 2$. Note that $G_\mathcal{C}(Z)$ acts on $G(Y) = \{1, \sigma_1, \sigma_3, \sigma_1\sigma_3\} \subseteq \Omega_\mathcal{C}$ since it is an orbit under $\mathcal{R}_\mathcal{C}$ (see Remark 2.38). The $G_\mathcal{C}(Z)$-orbits are
$$1^{G_\mathcal{C}(Z)} = \{1^{\mathcal{R}_\mathcal{C}(1)}, 1^{\mathcal{R}_\mathcal{C}(\sigma_1)}, 1^{\mathcal{R}_\mathcal{C}(\sigma_2)}, 1^{\mathcal{R}_\mathcal{C}(\sigma_1\sigma_2)}\} = \{1, \sigma_1, 1, \sigma_1\} = \{1, \sigma_1\} = \sigma_1^{G_\mathcal{C}(Z)}$$
and $\sigma_3^{G_\mathcal{C}(Z)} = \{\sigma_3, \sigma_1\sigma_3\} = (\sigma_1\sigma_3)^{G_\mathcal{C}(Z)}$. Thus there are $2 = |G(W)|$ orbits each of size $2 = |G(Y) : G(W)|$.

Lemma 4.11. *If $X = \bigcup_{Y \in \mathcal{C}} Y$, then $\mathcal{R}_\mathcal{C}$ is faithful.*

Proof. For now, fix $Y \in \mathcal{C}$; if $\mathcal{R}_Y(\sigma) = 1_{\mathrm{Sym}(G(Y))}$, then for $\alpha \in G(Y)$, we have $\alpha^{\mathcal{R}_Y(\sigma)} = \alpha$ if and only if $\sigma \in G(X \setminus Y)$, since $\mathcal{R}_Y(\sigma)$ acts regularly on $G(Y)$ and trivially on $G(X \setminus Y)$ (which have trivial intersection).

Now suppose $X = \bigcup_{Y \in \mathcal{C}} Y$ and that $\sigma \in G(X)$. If $\mathcal{R}_\mathcal{C}(\sigma) = 1_{\mathrm{Sym}(\Omega_\mathcal{C})}$, then $\mathcal{R}_Y(\sigma) = 1_{\mathrm{Sym}(G(Y))}$ for all $Y \in \mathcal{C}$. So $\sigma \in \bigcap_{Y \in \mathcal{C}} G(X \setminus Y) = G(\bigcap_{Y \in \mathcal{C}} X \setminus Y) = G(X \setminus \bigcup_{Y \in \mathcal{C}} Y) = G(X \setminus X) = G(\emptyset) = 1$, i.e. $\sigma = 1 \in G(X)$. This shows $\mathcal{R}_\mathcal{C}$ is faithful. □

In the subsequent lemmas, we use the restricted action of the permutation group $G_C(Z)$ on the block $G(Y) \subseteq \Omega_C$ for $Z \subseteq X$ as described above. The following generalises the observation in Example 4.10(a).

Lemma 4.12 (Lemma 2.2 in [3]). *Fix $Z \subseteq X$, a set $Y \in C$, and $\alpha \in G(Y)$. Then $G_C(Z)_\alpha = G_C(Z \setminus Y)$.*

Proof. Note that

$$G_C(Z)_\alpha = \{\sigma \in G_C(Z) : \alpha^\sigma = \alpha\} = \mathcal{R}_C[\{\sigma \in G(Z) : \alpha^{\mathcal{R}_C(\sigma)} = \alpha\}] = \mathcal{R}_C[G(Z \setminus Y)] = G_C(Z \setminus Y).$$

For the second last equality, the "$\supseteq$" is obvious since $G(Z \setminus Y)$ acts trivially on $\alpha \in G(Y)$. For "$\subseteq$", observe that for $\sigma \in G(Z)$, we can decompose $\sigma = \sigma_{Z\setminus Y}\sigma_{Z\cap Y}$ where $\sigma_{Z\setminus Y} \in G(Z \setminus Y)$ and $\sigma_{Z\cap Y} \in G(Z \cap Y)$. Then

$$\alpha = \alpha^{\mathcal{R}_C(\sigma)} = \alpha^{\mathcal{R}_Y(\sigma_{Z\setminus Y}\sigma_{Z\cap Y})} = \alpha^{\mathcal{R}_Y(\sigma_{Z\setminus Y})\mathcal{R}_Y(\sigma_{Z\cap Y})} = \alpha^{\mathcal{R}_Y(\sigma_{Z\cap Y})} = \alpha\sigma_{Z\cap Y},$$

so $\sigma_{Z\cap Y} = 1$ since $\sigma_{Z\setminus Y} \notin G(Y)$ acts trivially while $\sigma_{Z\cap Y} \in G(Y)$ acts regularly (on $G(Y)$), so that $\sigma = \sigma_{Z\setminus Y} \in G(Z \setminus Y)$.□

Now, a generalisation of the observation in Example 4.10(b):

Lemma 4.13 (Lemma 2.3 in [3]). *Let $W = Y \cap Z$ where $Z \subseteq X$ and $Y \in C$. Then the set $G(Y)$ has $|G(Y) : G(W)|$-many $G_C(Z)$-orbits each of size $|G(W)|$.*

Proof. Note that $G_C(Z)$ acts on $G(Y) \subseteq \Omega_C$ from above, since $G(Y)$ is an orbit under the action $\mathcal{R}_C$. Also recall that $G(Z) \cong G(Z \setminus Y) \times G(W)$ where $W = Y \cap Z$. Let $\alpha \in G(Y)$. Then using the $G_C(Z)$-action on $G(Y)$,

$$|\alpha^{G_C(Z)}| = \frac{|G_C(Z)|}{|G_C(Z)_\alpha|} = \frac{|\mathcal{R}_C[G(Z)]|}{|\mathcal{R}_C[G(Z \setminus Y)]|} = \frac{|\mathcal{R}_C[G(Z \setminus Y)] \times \mathcal{R}_C[G(W)]|}{|\mathcal{R}_C[G(Z \setminus Y)]|} = |\mathcal{R}_C[G(W)]| = |G(W)|.$$

The first equality is by the orbit-stabiliser theorem, the second by Lemma 4.12, the third since $\mathcal{R}_C$ is a homomorphism, and the last since $G(W)$ acts faithfully (in fact regularly) on $G(Y)$. So the $G_C(Z)$-orbits each have size $|G(W)|$. Also,

$$\begin{aligned}\alpha^{G_C(Z)} = \{\alpha^\sigma : \sigma \in G_C(Z)\} = \{\alpha^{\mathcal{R}_C(\sigma)} = \alpha^{\mathcal{R}_Y(\sigma)} : \sigma \in G(Z)\} \\ = \{\alpha^{\mathcal{R}_Y(\sigma_W)} = \alpha\sigma_W : \sigma = \underbrace{\sigma_{Z\setminus Y}}_{\in G(Z\setminus Y)}\underbrace{\sigma_W}_{\in G(W)} \in G(Z)\} = \alpha G(W)\end{aligned}$$

since $G(Z \setminus Y)$ acts trivially on $\alpha \in G(Y)$ under the action $\mathcal{R}_Y$. So the $G_C(Z)$-orbits are the left cosets of $G(W)$ in $G(Y)$; there are $|G(Y) : G(W)|$-many. □

NP-hardness of the minimum base problem for elementary abelian groups

The following is Theorem 3.2 in [3].

Theorem 4.14 (Blaha, 1992). *MB is NP-complete even for G an elementary abelian 2-group with orbits of size 8.*

Proof. Let (Y, M) be an instance of X3C as described in Example 3.18, with $|Y| = 3q$ and $|M| = k$; again suppose without loss of generality that the 3-sets in M cover Y. Now, using the notation in Example 4.9, define the group

$$G_M(Y) = \langle \mathcal{R}_M(\sigma_y) \mid y \in Y \rangle \leq \mathrm{Sym}(\Omega_M),$$

where M (c.f. C) is a collection of subsets of Y (c.f. X) and $\Omega_M = \bigsqcup_{m\in M} G(m)$. (Here, $G(Y) = (\mathbb{Z}/2\mathbb{Z})^{3q}$ and for a 3-set $m \in M$, $G(m) = \langle \sigma_y \mid y \in m \rangle \leq G(Y)$ has order $2^3 = 8$.)

Initialise an instance of MB with $G = G_M(Y)$ and $N = q$; G is indeed an elementary abelian 2-group, and the orbits of G have size $|G(m)| = 8$ (apply Lemma 4.13 with $Z \mapsto Y$ and $Y \mapsto m$). This is a Karp reduction from X3C to MB, since $|\Omega_M| = \sum_{m\in M} |G(m)| = 8|M| = 8k$ and G has $|Y| = 3q$ generators. For $r \leq q$, let $B = [\beta_1, \ldots, \beta_r]$ be a sequence of distinct points in Ω_M with $\beta_i \in G(m_i) \subseteq \Omega_M$; define the stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r$ as usual (if B is not a base for G, then $G^r \neq 1$). Let $Y_0 = Y$ and $Y_i = Y_{i-1} \setminus m_i = Y \setminus (m_1 \cup \cdots \cup m_i)$ for $1 \leq i \leq r$. By Lemma 4.12 and induction on i, $G^i = G_M(Y_i)$ for $1 \leq i \leq r$, since $G^0 = G = G_M(Y_0)$ and $G^i = G^{i-1}_{\beta_i} = G_M(Y_{i-1})_{\beta_i} = G_M(Y_{i-1} \setminus m_i)$ by induction with $\beta_i \in G(m_i)$.

Now B is a base for G if and only if $1 = G^r = G_M(Y_r)$, if and only if $Y_r = \emptyset$. Since each $m \in M$ is a 3-set and $|Y| = 3q$, $Y \setminus (m_1 \cup \cdots \cup m_r) = Y_r = \emptyset$ if and only if $r = q$ (since $r \leq q$) and the m_i are disjoint for $1 \leq i \leq r$. In summary,

$B = [\beta_1, \ldots, \beta_r]$ is a base for G with $r \leq q$ if and only if $r = q$ and the 3-sets $m_1, \ldots, m_r \in M$ form an exact cover of Y. This is the desired Karp reduction from X3C to MB. □

Remark 4.15. (a) Blaha notes in [3] that by replacing 2 with a fixed prime p, and 8 with p^3 in Theorem 4.14 (i.e. considering $(\mathbb{Z}/p\mathbb{Z})^n$ and an analogous construction), one can show that MB is NP-complete even for G an elementary abelian p-group with orbits of size p^3.

(b) If G is an elementary abelian p-group with orbits of size less than 8, then it can be shown that the minimum base problem is decidable in polynomial time. One approach by Blaha, mentioned in [3], uses Lovász's result in [22] that a maximum matching of a linear 2-polymatroid can be found in polynomial time.

4.3 Sharp bounds for sizes of bases

Even though the greedy base algorithm does not solve the minimum base problem, it is natural to ask whether it is a good heuristic for computing small bases. In [3], Blaha first gives a sharp bound of $O(b(G)\log n)$ for the size of a nonredundant base for $G \leq \mathrm{Sym}(n)$, then gives a sharp bound of $O(b(G)\log\log n)$ for the size of a greedy base (recall that log denotes the base-2 logarithm). From these, we conclude that a greedy base improves, in the worst-case, the size difference (to a minimum base) from a factor of $\log n$ to a factor of $\log\log n$ when compared to nonredundant bases.

A sharp bound for nonredundant bases

The difference in size between any two nonredundant bases for G is at most a factor of $\log n$, in particular from the size of an optimal (minimum) base. Recall from Lemma 2.57 that if $G \leq \mathrm{Sym}(n)$ and r is the size of a nonredundant base for G, then $r \leq b(G)\log n$.

Lemma 4.16 (Lemma 4.2 in [3]). *Fix $r \geq 1$; then for any $n \geq 8r^2$ there exists $G \leq \mathrm{Sym}(n)$ such that $b(G) = r$, and G has a nonredundant base of size at least $\frac{1}{3}b(G)\log n$.*

So, the $O(b(G)\log n)$ bound in Lemma 2.57 is *sharp* (i.e. cannot be improved upon), in the sense that for every large enough n there is a group $G \leq \mathrm{Sym}(n)$ for which the upper bound of $b(G)\log n$ for a nonredundant base is attained, up to a constant factor.

A sharp bound for greedy bases

When we consider greedy bases for G (as found by the greedy base algorithm), they are at most a factor of $\log\log n$ from the size of a minimum base, as opposed to a factor of $\log n$ for arbitrary nonredundant bases (as in Lemma 4.16).

Lemma 4.17 (Lemma 4.3 in [3]). *If $G \leq \mathrm{Sym}(n)$ has a base of size r, then there is a G-orbit of size at least $|G|^{1/r}$.*

Proof. Let $B = [\beta_1, \ldots, \beta_r]$ be a base for G with stabiliser chain $G = G^0 \geq G^1 \geq \cdots \geq G^r = 1$. Then Proposition 2.55 gives $|G| = |\beta_1^{G^0}| \cdots |\beta_r^{G^{r-1}}|$, so $|\beta_i^{G^{i-1}}| \geq |G|^{1/r}$ for some i. But $G^{i-1} \leq G$, so certainly $\beta_i^{G^{i-1}} \subseteq \beta_i^G$, giving that the size of the G-orbit of β_i is $|\beta_i^G| \geq |\beta_i^{G^{i-1}}| \geq |G|^{1/r}$. □

The following are Theorems 4.4 and 4.6 in [3], respectively.

Theorem 4.18 (Blaha, 1992). *If $G \leq \mathrm{Sym}(n)$, then a greedy base for G has size at most $\lceil b(G)\log\log n\rceil + b(G) = O(b(G)\log\log n)$.*

Theorem 4.19 (Blaha, 1992). *Fix $r \geq 2$; then for any $n \geq 2^{4r^2+7r+7}$ there is $G \leq \mathrm{Sym}(n)$ such that $b(G) = r$, and every greedy base for G has size at least $\frac{1}{5}b(G)\log\log n$.*

So, the $O(b(G)\log\log n)$ bound in Theorem 4.18 is also sharp. We conclude that greedy bases certainly offer a marked improvement over simply taking nonredundant bases for a permutation group.

Chapter 5

Classification results for permutation groups

The definitions and results in this section are primarily found in Rotman [26] and Dixon and Mortimer [12].

5.1 Classification of finite simple groups

Prime numbers are the "building blocks" of natural numbers, in the sense that a natural number has a unique factorisation as a product of prime numbers, by the fundamental theorem of arithmetic. Thus, to study number theory, it is often useful to study primes. A similar question arises for groups, in particular finite groups – is there a way to break down an arbitrary finite group into the simplest "building blocks"? The analogous object to prime numbers for groups is the notion of a simple group, which all finite groups can be decomposed into. (The inverse problem of reconstructing groups from simple groups is more difficult than for integers, and is referred to as the group extension problem.)

The classification of finite simple groups is one of the most famous problems in group theory, and its statement and proof was achieved by a collaboration of many group theorists across many decades and many volumes of work. In [30], Solomon notes that computational group theory has also been influential in the classification result: for instance, by 2001, computer algorithms were being created to identify permutation groups, linear groups and "black box" groups, and calculations of groups of order 2^{10} re-verified the fact that "most" finite groups are *nilpotent* groups of nilpotence class at most 2.

Recall that a **maximal normal subgroup** of a nontrivial group G is a normal subgroup $1 \neq N \lhd G$ such that $N \lhd M \trianglelefteq G$ implies $M = G$.

Definition 5.1. A group $G \neq 1$ is **simple** if it has no nontrivial normal subgroups.

For example, the cyclic groups C_p of prime order are simple by Lagrange's theorem; if $n = uv$ is not prime, then $C_n = \langle a \rangle$ is not simple since $1 \neq \langle a^u \rangle \lhd C_n$. Moreover, $\mathrm{Alt}(n)$ is simple for $n \geq 5$. Now, by the correspondence theorem (see Theorem 2.28 in [26]), $N \trianglelefteq G$ is a maximal normal subgroup of G if and only if G/N is simple. This is because a normal subgroup of G/N is of the form M/N with $N \trianglelefteq M \trianglelefteq G$, and $M = N$ (in which case $M/N \cong 1$) or $M = G$ (which implies simplicity of G/N) if and only if N is maximal in G.

Definition 5.2. Let N, Q be groups. A group G is an **extension** of N by Q if there is a normal subgroup $N \cong N^* \trianglelefteq G$ with $G/N^* \cong Q$; we write $G = N \,.\, Q$. (This is equivalent to saying that G factors over N with quotient Q.)

Here, we think of Q as the quotient after we factor out the "normal subgroup" N of G. For example, the direct product $G \times H$ is an extension of G by H and an extension of H by G; the subgroups $G \times 1$ and $1 \times H$ are normal in $G \times H$. Note that there may be nonisomorphic groups G that satisfy $G = N \,.\, Q$ for given groups N, Q. For example, set $N = Q = C_2$.

The groups $G = C_4 = \langle a \rangle$ and $\tilde{G} = C_2 \times C_2$ (where $C_2 = \langle b \rangle$) are nonisomorphic, yet $G/\langle a^2 \rangle \cong Q$ and $\tilde{G}/\langle (b,1) \rangle \cong Q$ with $\langle a^2 \rangle \cong N \cong \langle (b,1) \rangle$. Thus, there is, in general, no unique way to reconstruct groups from their factors, and this is part of the difficulty of the group extension problem.

This notation $G = N \,.\, Q$ is ATLAS notation, and is often used in finite group theory. Note that often a cyclic group C_n is simply written as n (e.g. $2 \,.\, \mathrm{Alt}(5) = \mathrm{Sym}(5)$), an elementary abelian p-group $(\mathbb{Z}/p\mathbb{Z})^d$ as p^d, and an unspecified group of order n as $[n]$.

Definition 5.3. A **composition series** is a finite subgroup series $G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = 1$ where each N_{i+1} is a *maximal* normal subgroup of N_i. The quotient groups N_i/N_{i+1} are the **composition factors**.

We say that two composition series $G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = 1$ and $G = \tilde{N}_0 \rhd \tilde{N}_1 \rhd \cdots \rhd \tilde{N}_{\tilde{r}} = 1$ of a group G are **equivalent** if there is a bijection between the multisets of composition factors such that corresponding composition factors are isomorphic.

Clearly, if $G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = 1$ is a composition series, then the composition factors N_i/N_{i+1} are simple, since the N_{i+1} are maximal in N_i. Moreover, if G is finite, then a composition series exists, since maximal subgroups exist (and the groups in the series decrease in size).

Example 5.4. Consider the cyclic group $C_{12} = \langle a \rangle$. Two composition series are $C_{12} \rhd \langle a^2 \rangle \rhd \langle a^4 \rangle \rhd 1$ and $C_{12} \rhd \langle a^2 \rangle \rhd \langle a^6 \rangle \rhd 1$. The composition factors of the first series are $C_{12}/\langle a^2 \rangle \cong C_2$, $\langle a^2 \rangle/\langle a^4 \rangle \cong C_2$ and $\langle a^4 \rangle/1 \cong C_3$, while the composition factors of the second series are $C_{12}/\langle a^2 \rangle \cong C_2$, $\langle a^2 \rangle/\langle a^6 \rangle \cong C_3$ and $\langle a^6 \rangle/1 \cong C_2$. Both composition series have the same length, 3, and the composition factors can be paired up, so the two series are equivalent.

The amazing fact is that for every group (possibly infinite) that has a composition series, every composition series is equivalent! This is the Jordan-Hölder theorem, which is proven as Theorem 5.12 in [26]:

Theorem 5.5 (Jordan-Hölder). *Any two composition series of a group G are equivalent.*

A fun corollary of this result is the fundamental theorem of arithmetic:

Corollary 5.6 (Fundamental theorem of arithmetic). *An integer $n \geq 2$ has a unique factorisation as a product of primes.*

Proof. We apply Theorem 5.5 to the group $C_n = \langle a \rangle$. First note that C_n has a composition series $C_n = N_0 \rhd N_1 \rhd \cdots \rhd N_r = 1$ with each N_i/N_{i+1} simple. Since all subgroups of C_n are cyclic, we have that each $N_i = \langle a^{n_i} \rangle$, and $N_i/N_{i+1} = \langle a^{n_i} \rangle/\langle a^{n_{i+1}} \rangle \cong C_{n_{i+1}/n_i}$ is simple, thus $n_{i+1}/n_i = p_{i+1}$ for some prime p_{i+1}. But then $1 = \langle a^n \rangle$ and $n_0 = 1$, so

$$n = n_r = (n_1/n_0)(n_2/n_1)\cdots(n_r/n_{r-1}) = p_1 p_2 \cdots p_r,$$

so n has a factorisation into primes.

Now, any product of primes p_i that equals n gives rise to a composition series: if $n = p_1 \cdots p_r$, then $G = \langle a \rangle \rhd \langle a^{p_1} \rangle \rhd \langle a^{p_1 p_2} \rangle \rhd \cdots \rhd \langle a^{p_1 \cdots p_r} \rangle = 1$ is a composition series (since the quotient groups have prime order p_i, thus simple). Then by Jordan-Hölder, any two composition series are equivalent, so the composition factors of the two series are isomorphic after permutation, and it follows that the primes in the resulting factorisations are the same up to rearrangement. □

Another consequence of the Jordan-Hölder theorem is that if G is a group with composition series $G = N_0 \rhd N_1 \rhd \cdots \rhd N_r = 1$ and composition factors $N_{i-1}/N_i = Q_i$, then $N_{i-1} = N_i \,.\, Q_i$ and thus

$$G = N_0 = N_1 \,.\, Q_1 = \cdots = ((\cdots(N_r \,.\, Q_r) \,.\, \cdots) \,.\, Q_2) \,.\, Q_1 = ((\cdots(Q_r \,.\, Q_{r-1}) \,.\, \cdots) \,.\, Q_2) \,.\, Q_1 = Q_r \,.\, \cdots \,.\, Q_1,$$

with the composition factors Q_i determined uniquely by G. Thus if we knew all finite simple groups, and we could solve the extension problem, then we could classify all finite groups.

Now, the extension problem asks one to "determine" all groups G such that $G/N \cong Q$ for given N, Q. One such approach is that we may construct a multiplication table for any such G; [26] notes that Schreier solved the problem in this sense. However, if we require that the isomorphism classes of G can be characterised, [26] notes that no solution is known. On the other hand, the classification of finite simple groups is complete, and the following may be found in [31]:

Theorem 5.7 (Classification of finite simple groups). *Every finite simple group is isomorphic to one of the following:*

(a) a cyclic group C_p of prime order p,

(b) an alternating group $\mathrm{Alt}(n)$ of degree $n \geq 5$,

*(c) a simple group of **Lie type** (including variants of infinite families of "classical" matrix groups, such as PSL), or*

*(d) one of 26 **sporadic simple groups**.*

The first three families are infinite families of groups, but the classification result shows that there are precisely 26 exceptions to the classification of finite simple groups into cyclic, alternating, and groups of Lie type. The existence of sporadic groups have often been theorised before their discovery, and the construction of the *Janko group* J_1 by Janko in 1965 (see [17]) was viewed as a surprise in the mathematical community, and launched the modern theory of sporadic groups, 90 years after the discovery of the last *Mathieu group* (another sporadic group). (Janko taught at Monash University in 1962, and joined the Australian National University in 1964 as a professor.) As shown in [21], the Janko group J_1 can be realised as a primitive permutation group of degree 266.

The projective special linear groups PSL are defined as follows. Given a finite field $\mathbb{F}_q$ (where q is a prime power), recall that the **special linear group** $\mathrm{SL}(n, q)$ is the set of $n \times n$ matrices over $\mathbb{F}_q$ with determinant 1. Recall that the centre $Z(G) \trianglelefteq G$ of a group G is the set of elements that commute with every element of G; the centre of $\mathrm{SL}(n, q)$ turns out to be scalar multiples of the identity matrix. Then the **projective special linear group** $\mathrm{PSL}(n, q)$ is the quotient $\mathrm{SL}(n, q)/Z(\mathrm{SL}(n, q))$ and is simple unless $n = 2$ and $q \in \{2, 3\}$, falling into category (c) of the above classification.

5.2 Semidirect products and wreath products

Semidirect products

Recall again that for groups G, N, their **direct product** is the group $G \times N$ with underlying set the Cartesian product $G \times N$ and group operation $(g, n)(h, m) = (gh, nm)$ for $g, h \in G$ and $n, m \in H$. Now, in some scenarios, the underlying set of a group is naturally the Cartesian product $G \times N$, but the group operation is not the direct product. For example, the underlying set of the dihedral group $D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ is naturally $C_2 \times C_n = \{1, s\} \times \{1, r, \ldots, r^{n-1}\}$ via the map $(s^a, r^b) \mapsto s^a r^b \in D_{2n}$. If G acts on N while respecting the group structure on N, we can define a more general type of product on the set $G \times N$, called the *semidirect product*, that turns it into a group.

Definition 5.8. Let G, N be groups and suppose G acts on N via a homomorphism $\varphi : G \to \mathrm{Aut}(N)$. The **semidirect product** of G and N (with respect to φ), denoted $G \ltimes_\varphi N$ (or simply $G \ltimes N$ if clear from context), is a group with underlying set the Cartesian product $G \times N$ and group operation $(g, n)(h, m) = (gh, n^h m)$ for $g, h \in G$ and $n, m \in N$.

We omit the proof that $G \ltimes N$ is a group, but observe that $|G \ltimes N| = |G||N|$, and for $g \in G$ and $n, m \in N$, we have $(nm)^g = n^g m^g$ and $(n^{-1})^g = (n^g)^{-1}$ since $\varphi(g) \in \mathrm{Aut}(N)$. Moreover, the identity in $G \ltimes N$ is $(1, 1)$, and inverses are given by $(g, n)^{-1} = (g^{-1}, (n^{-1})^{g^{-1}}) = (g^{-1}, (n^{g^{-1}})^{-1})$. Note that some sources (such as [12]) alternatively define the semidirect product as $N \rtimes G$ (with underlying set $N \times G$) with group operation $(n, g)(m, h) = (nm^{g^{-1}}, gh)$.

The semidirect product $G \ltimes N$ has a subgroup $G^* = \{(g, 1) : g \in G\} \cong G$ and a normal subgroup $N^* = \{(1, n) : n \in N\} \cong N$, since $(g, m)^{-1}(1, n)(g, m) = (g^{-1}, (m^{-1})^{g^{-1}})(g, n^g m) = (1, m^{-1} n^g m) \in N^*$ for $g \in G$ and $n, m \in N$. Note that when φ is the trivial map (i.e. $g \mapsto 1_{\mathrm{Aut}(N)}$ for all $g \in G$), we recover the direct product, since $n^h = n$ for all $n \in N$ and $h \in G$.

Example 5.9. The dihedral group $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$ of symmetries of a square can be realised as a semidirect product $C_2 \ltimes C_4$, where $C_2 = \{1, s\}$ acts on $C_4 = \{1, r, r^2, r^3\}$ by $1 \mapsto ()$ and $s \mapsto (r, r^3)$ (inversion). The isomorphism $C_2 \ltimes C_4 \to D_8$ is then simply $(g, h) \mapsto gh \in D_8$ (for $g \in C_2$ and $h \in C_4$). An interpretation of this is: to compose two symmetries $s^a r^b$ and $s^u r^v$ in D_8, the reflection components compose directly (to yield s^{a+u}), but the rotation component may be affected (yielding the direct composition $(r^b)^{s^u} r^v = r^{b+v}$ if $s^u = 1$, or r^{-b+v} otherwise).

We can verify that this is consistent with our permutation representation $r \sim (1,2,3,4)$ and $s \sim (1,4)(2,3)$ for D_8 in Example 2.14. Note that in $C_2 \ltimes C_4$, $(s,1)(1,r) = (s1, 1^1 r) = (s,r)$ and $(1,r)(s,1) = (1s, r^s 1) = (s, r^3)$. In the permutation representation, $sr = (2,4)$ and $(r,s) = (1,3) = sr^3$, which is compatible with the isomorphism $C_2 \ltimes C_4 \to D_8$ above.

This generalises to the dihedral group D_{2n}, which is isomorphic to the semidirect product $C_2 \ltimes C_n$ where $C_2 = \{1, s\}$ acts on $C_n = \{1, r, \dots, r^{n-1}\}$ by $1 \mapsto ()$ and $s \mapsto (r^a \mapsto r^{-a})$ (inversion). The isomorphism $C_2 \ltimes C_n \to D_{2n}$ is $(g,h) \mapsto gh \in D_{2n}$; D_{2n} thus has a normal subgroup isomorphic to C_n (which is the group of rotations).

Semidirect products are related to the notion of a split extension.

Definition 5.10. If G is a group and Q, N are subgroups with $N \trianglelefteq G$, $G = QN$ and $Q \cap N = 1$, then G is a **split extension** of N by Q, and write $G = N : Q$. We say that G **splits** over N. (Recall that $QN = \{qn : q \in Q, n \in N\}$.)

Lemma 5.11. *If $G = N : Q$ for $N, Q \leq G$, then $G \cong Q \ltimes_\varphi N$ where $\varphi : Q \to \mathrm{Aut}(N)$ is the conjugation action given by $n^g = g^{-1}ng$ for $n \in N$ and $g \in Q$.*

Note that the order of the factors are reversed in $N : Q$ compared to $Q \ltimes N$. This follows from the fact that the semidirect product is alternatively defined as $N \rtimes Q$, as seen earlier. We now prove the above lemma:

Proof. Consider the map $\psi : Q \ltimes_\varphi N \to N : Q$ with $(g,n) \mapsto gn$. Note that an element of $N : Q = QN$ can be uniquely expressed as gn with $g \in Q$ and $n \in N$: suppose $gn = hm$ for $g, h \in Q$ and $n, m \in N$. Then $Q \ni h^{-1}g = mn^{-1} \in N$, so $h = g$ and $m = n$ since $Q \cap N = 1$. Thus ψ is clearly a bijection.

Now for $(g,n), (h,m) \in Q \ltimes_\varphi N$,

$$\psi((g,n)(h,m)) = \psi((gh, n^h m)) = ghn^h m = gh(h^{-1}nh)m = (gn)(hm) = \psi((g,n))\psi((h,m)),$$

so ψ is a homomorphism, thus an isomorphism. □

The proof of this lemma also allows us to see that the *split extension* $N : Q$ is indeed an *extension* of N by Q (see Definition 5.2), since $N \trianglelefteq G$ with $G/N \cong Q$ via the homomorphism $\varphi : G \to Q$ where $qn \mapsto q$. Well-definition follows from the unique decomposition of elements in $G = N : Q = QN$ in the proof above; indeed $\varphi((gn)(hm)) = \varphi(gh(h^{-1}nh)m) = gh = \varphi(gn)\varphi(hm)$ for $gn, hm \in QN$ since $h^{-1}nh \in N \trianglelefteq G$; finally φ is clearly surjective and its kernel is clearly N, so the result follows from the first isomorphism theorem.

Now, Example 5.9 shows that the semidirect product construction $G \ltimes_\varphi N$ may lead to nonisomorphic groups with different choice of φ, so as with general extensions, split extensions are not unique. Suppose $D_8 \cong C_2 \ltimes_\varphi C_4$, so that $D_8 = C_4 \,.\, C_2$. However, the direct product $C_2 \times C_4$ is also a split extension (semidirect product) that is not isomorphic to D_8 (one is abelian, the other is not).

Wreath products

A special type of semidirect product, called the wreath product, plays an important role in the study of primitive and imprimitive permutation groups.

Definition 5.12. Let G be a group and X a set. Then G^X is the **group of functions** $X \to G$, which is a group under pointwise multiplication: for $\omega, \eta \in G^X$ and $x \in X$, $\omega\eta(x) = \omega(x)\eta(x) \in G$.

The proof that G^X forms a group is straightforward; the identity is 1, defined by $x \mapsto 1 \in G$; the inverse is defined pointwise. Note that in this context, G^X does not denote the image of G under an action on X.

Definition 5.13. Given groups G and H and suppose G acts on $\Omega \neq \emptyset$. Then the **wreath product** $H \wr_\Omega G$ of H by G is the semidirect product $G \ltimes H^\Omega$ where G acts on H^Ω, with $\omega^g \in H^\Omega$ given by $\alpha \mapsto \omega(\alpha^{g^{-1}})$ for $\omega \in H^\Omega$ and $g \in G$.

The **base group** of the wreath product $H \wr_\Omega G = G \ltimes H^\Omega$ is the subgroup $\{(1,\omega) : \omega \in H^\Omega\} \cong H^\Omega$.

Note that for $\omega \in H^\Omega$, $\alpha \in \Omega$ and $g, h \in G$, $\omega^{gh}(\alpha) = \omega(\alpha^{h^{-1}g^{-1}}) = \omega^g(\alpha^{h^{-1}}) = (\omega^g)^h(\alpha)$, so $\omega^{gh} = (\omega^g)^h$. Moreover, $\omega^1(\alpha) = \omega(\alpha^1) = \omega(\alpha)$, so $\omega^1 = \omega$; together, these imply that this is indeed a G-action. If φ is the G-action on H^Ω in this

definition, then indeed $\varphi : G \to \mathrm{Aut}(H^\Omega)$, so that we have a semidirect product: for $\omega, \eta \in H^\Omega$, $\alpha \in \Omega$ and $g \in G$,

$$\omega^g \eta^g(\alpha) = \omega^g(\alpha)\eta^g(\alpha) = \omega(\alpha^{g^{-1}})\eta(\alpha^{g^{-1}}) = \omega\eta(\alpha^{g^{-1}}) = (\omega\eta)^g(\alpha),$$

so $(\omega\eta)^g = \omega^g\eta^g$, as required. Note that $|H \wr_\Omega G| = |H|^{|\Omega|}|G|$.

In the case that $\Omega = [n]$, we may identify the base group of the wreath product $H \wr_\Omega G$ with the direct product H^n (via the isomorphism $H^\Omega \to H^n$ where $(\omega : \Omega \to H) \mapsto (\omega(1), \ldots, \omega(n))$), so that $H \wr_\Omega G = G \ltimes H^n$. The action of G on H^n corresponds to permuting components: $g \in G$ acts on $(\omega_1, \ldots, \omega_n) \in H^n$ by permuting components according to g, with $(\omega_1, \ldots, \omega_n)^g = (\omega_{1_g}, \ldots, \omega_{n_g})$ where $i_g = i^{g^{-1}}$. Then an element of $H \wr_\Omega G$ is $(g, \omega_1, \ldots, \omega_n)$ with $g \in G$ and each $\omega_i \in H$, and the product in $H \wr_\Omega G$ is given by

$$(g, \omega_1, \ldots, \omega_n)(h, \eta_1, \ldots, \eta_n) = (gh, \omega_{1_h}\eta_1, \ldots, \omega_{n_h}\eta_n)$$

where each $i_h = i^{h^{-1}}$. If we further have $G = \mathrm{Sym}(n)$ which acts naturally on $[n]$, then we write $H \wr \mathrm{Sym}(n)$ instead of $H \wr_\Omega \mathrm{Sym}(n)$. In the trivial case that $G = \mathrm{Sym}(1) = 1$, the wreath product $H \wr \mathrm{Sym}(1) = \mathrm{Sym}(1) \ltimes H \cong H$.

We discuss two important actions of the wreath product. The imprimitive action is natural and relates to imprimitive groups, while the product action is important in the classification of finite primitive groups. The imprimitive action helps us to understand the wreath product, e.g. that $\mathrm{Sym}(2) \wr \mathrm{Sym}(2) \cong D_8$, which we discuss in Example 5.17 below.

Definition 5.14. Suppose G acts on Ω and H acts on Γ. Let $W = H \wr_\Omega G$; the **imprimitive action** of W on $\Omega \times \Gamma$ is given by the following: for $(g, \omega) \in W = G \ltimes H^\Omega$ and $(\alpha, \gamma) \in \Omega \times \Gamma$ we define

$$(\alpha, \gamma)^{(g,\omega)} = (\alpha^g, \gamma^{\omega(\alpha^g)}).$$

This is indeed an action: for $(\alpha, \gamma) \in \Omega \times \Gamma$ and $(g, \omega), (h, \eta) \in W$,

$$((\alpha, \gamma)^{(g,\omega)})^{(h,\eta)} = (\alpha^g, \gamma^{\omega(\alpha^g)})^{(h,\eta)} = (\alpha^{gh}, \gamma^{\omega(\alpha^g)\eta(\alpha^{gh})}) = (\alpha^{gh}, \gamma^{\omega^h\eta(\alpha^{gh})}) = (\alpha, \gamma)^{(gh,\omega^h\eta)} = (\alpha, \gamma)^{(g,\omega)(h,\eta)}$$

since $\omega^h\eta(\alpha^{gh}) = \omega^h(\alpha^{gh})\eta(\alpha^{gh}) = \omega(\alpha^g)\eta(\alpha^{gh})$. Also, $(\alpha, \gamma)^{(1,1)} = (\alpha^1, \gamma^{1(\alpha^1)}) = (\alpha, \gamma^{1_H}) = (\alpha, \gamma)$.

In the case that $\Omega = [n]$, using the identification $H^\Omega \to H^n$ from above, the imprimitive action corresponds to $(i, \gamma)^{(g,\omega_1,\ldots,\omega_n)} = (i^g, \gamma^{\omega_i g})$ for $(i, \gamma) \in \Omega \times \Gamma$, $g \in G$ and $(\omega_1, \ldots, \omega_n) \in H^n$.

Proposition 5.15. *Suppose G acts on Ω via φ_G and H acts on Γ via φ_H. Let $\hat{\varphi}$ be the imprimitive action of $W = H \wr_\Omega G$ on $\Omega \times \Gamma$. Then $\mathrm{Ker}\,\hat{\varphi} = \mathrm{Ker}\,\varphi_G \times \{\omega \in H^\Omega : \omega[\Omega] \subseteq \mathrm{Ker}\,\varphi_H\}$. Thus, the imprimitive action $\hat{\varphi}$ of $W = H \wr_\Omega G$ on $\Omega \times \Gamma$ is faithful if and only if the G-action φ and H-action $\tilde{\varphi}$ are both faithful.*

Proof. Note that

$$\begin{aligned}
\mathrm{Ker}\,\hat{\varphi} &= \{(g, \omega) \in W : (\alpha^g, \gamma^{\omega(\alpha^g)}) = (\alpha, \gamma)^{(g,\omega)} = (\alpha, \gamma) \text{ for all } (\alpha, \gamma) \in \Omega \times \Gamma\} \\
&= \{(g, \omega) \in W : g \in G_\alpha \text{ for all } \alpha \in \Omega \text{ and } \omega(\alpha) \in H_\gamma \text{ for all } (\alpha, \gamma) \in \Omega \times \Gamma\} \\
&= \{(g, \omega) \in W : g \in \mathrm{Ker}\,\varphi_G \text{ and } \omega(\alpha) \in \mathrm{Ker}\,\varphi_H \text{ for all } \alpha \in \Omega\} \\
&= \mathrm{Ker}\,\varphi_G \times \{\omega \in H^\Omega : \omega[\Omega] \subseteq \mathrm{Ker}\,\varphi_H\}.
\end{aligned}$$

Then if φ_G, φ_H are faithful (i.e. $\mathrm{Ker}\,\varphi_G = 1_G$ and $\mathrm{Ker}\,\varphi_H = 1_H$), then $\omega[\Omega] \subseteq 1_H$ if and only if $\omega = 1 \in H^\Omega$, so $\mathrm{Ker}\,\hat{\varphi} = 1_G \times 1_{H^\Omega} = 1_W$, and the imprimitive action is faithful. Conversely, if the imprimitive action is faithful, then $\mathrm{Ker}\,\varphi_G = 1_G$ and $\{\omega \in H^\Omega : \omega[\Omega] \subseteq \mathrm{Ker}\,\varphi_H\} = 1_{H^\Omega}$, so $\mathrm{Ker}\,\varphi_H = 1_H$ (consider a constant map in H^Ω) and the result follows. □

Now, the image $W^{\Omega\times\Gamma}$ of the imprimitive action is a subgroup of $\mathrm{Sym}(\Omega \times \Gamma)$. So, if $G \leq \mathrm{Sym}(\Omega)$ and $H \leq \mathrm{Sym}(\Gamma)$ have the natural action (which is faithful), then W embeds as a subgroup of $\mathrm{Sym}(\Omega \times \Gamma)$.

Lemma 5.16. *Suppose G acts transitively on Ω and H acts primitively on Γ, with $|\Omega|, |\Gamma| > 1$. Then the imprimitive action of $W = H \wr_\Omega G$ on $\Omega \times \Gamma$ is imprimitive with $\Sigma = \{\{\alpha\} \times \Gamma : \alpha \in \Omega\}$ a system of imprimitivity.*

Proof. The action is transitive: for $(\alpha, \gamma), (\tilde{\alpha}, \tilde{\gamma}) \in \Omega \times \Delta$, we have $\tilde{\alpha} = \alpha^g$ for some $g \in G$, and $\tilde{\gamma} = \gamma^h$ for some $h \in H$. Then let $\omega \in H^\Omega$ be the constant map $\beta \mapsto h$; then $(\alpha, \gamma)^{(g,\omega)} = (\alpha^g, \gamma^{\omega(\alpha^g)}) = (\tilde{\alpha}, \gamma^h) = (\tilde{\alpha}, \tilde{\gamma})$.

Now each $\Delta = \{\alpha\} \times \Gamma$ is a block for $\alpha \in \Omega$ with $|\Delta| = |\Gamma|$; it is nontrivial as long as $|\Omega|, |\Gamma| > 1$ so that $|\Delta| > 1$ and $\Delta \neq \Omega \times \Gamma$. We verify that it is a block: for any $(g, \omega) \in W$,

$$\Delta^{(g,\omega)} = \{(\alpha, \gamma)^{(g,\omega)} : \gamma \in \Gamma\} = \{(\alpha^g, \gamma^{\omega(\alpha^g)}) : \gamma \in \Gamma\} = \{\alpha^g\} \times \Gamma^{\omega(\alpha^g)}$$

with $\Gamma^{\omega(\alpha^g)} = \Gamma$ or $\Gamma^{\omega(\alpha^g)} \cap \Gamma = \emptyset$ by primitivity of H^Γ. In the first case, and assuming $\alpha^g = \alpha$, then $\Delta^{(g,\omega)} = \{\alpha\} \times \Gamma = \Delta$; otherwise, $\Gamma^{\omega(\alpha^g)} \cap \Gamma = \emptyset$ or $\alpha^g \neq \alpha$, in which case $\Delta^{(g,\omega)} \cap \Delta = \emptyset$. So $W^{\Omega\times\Gamma}$ is imprimitive as long as $|\Omega|, |\Gamma| > 1$. □

If $G \leq \mathrm{Sym}(n)$ and $H \leq \mathrm{Sym}(m)$, consider the wreath product $W = H \wr_{[n]} G = G \ltimes H^n$. Note that H acts on the ordered list $[1, \ldots, m]$; let the ith copy of H act on $X_i = [(i-1)m+1, \ldots, im]$ (in the natural way). Let $X = \bigcup_{1\leq i\leq n} X_i = [1, \ldots, mn]$. Since G acts on $\{1, \ldots, n\}$, we now let G act on $\{X_1, \ldots, X_n\}$ by permutation. This allows us to consider W as a subgroup of $\mathrm{Sym}(X) = \mathrm{Sym}(mn)$ instead of $\mathrm{Sym}([n] \times [m])$ (using the map $[n] \times [m] \to [mn]$ where $(i, j) \mapsto (i-1)m + j$). In particular, the X_i form blocks and we have a block system $\Sigma = [X_1, \ldots, X_n]$; the imprimitive action of $(g, \omega_1, \ldots, \omega_n) \in W$ corresponds to permuting within each block X_i by $\omega_i \in H \leq \mathrm{Sym}(m)$, then permuting the blocks in Σ by $g \in G \leq \mathrm{Sym}(n)$.

Example 5.17. Let $G = H = \mathrm{Sym}(2)$ and consider the wreath product $W = H \wr G = \mathrm{Sym}(2) \wr \mathrm{Sym}(2)$. Since $H = \mathrm{Sym}(2)$ is primitive (Example 2.43) and $G = \mathrm{Sym}(2)$ is transitive, Lemma 5.16 shows that W acts imprimitively on $\Omega = \{1, 2\} \times \{1, 2\}$ with nontrivial block system $\Sigma = \{\{1\} \times \{1, 2\}, \{2\} \times \{1, 2\}\}$.

Now relabel Ω using $\tau : \Omega \to [4]$, where $(1, 1) \mapsto 1$, $(1, 2) \mapsto 3$, $(2, 1) \mapsto 2$, and $(2, 2) \mapsto 4$. Then W acts imprimitively on $[4]$ in the following way: for $(g, \omega_1, \omega_2) \in W$ for $g, \omega_1, \omega_2 \in \mathrm{Sym}(2)$, if $\tau((m, n)) = i$ for $m, n \in [2]$, then we set

$$i^{(g,\omega_1,\omega_2)} = \tau((m, n)^{(g,\omega_1,\omega_2)}) = \tau((m^g, n^{\omega_{m^g}})).$$

For example, $1^{((1,2),(1,2),())} = \tau((1, 1)^{((1,2),(1,2),())}) = \tau((1^{(1,2)}, 1^{()})) = \tau((2, 1)) = 2$ but $1^{((1,2),(),(1,2))} = \tau((1^{(1,2)}, 1^{(1,2)})) = \tau((2, 2)) = 4$. Since both actions are faithful, the imprimitive action is faithful and embeds into $\mathrm{Sym}(4)$. Calculation shows the following (see appendix for GAP code):

$w \in W$	1^w	2^w	3^w	4^w	$\psi(w) \in \mathrm{Sym}(4)$	$\tilde{\psi}(w) \in D_8$
$((), (), ())$	1	2	3	4	$()$	1
$((), (), (1, 2))$	1	4	3	2	$(2, 4)$	sr
$((), (1, 2), ())$	3	2	1	4	$(1, 3)$	sr^3
$((), (1, 2), (1, 2))$	3	4	1	2	$(1, 3)(2, 4)$	r^2
$((1, 2), (), ())$	2	1	4	3	$(1, 2)(3, 4)$	sr^2
$((1, 2), (), (1, 2))$	4	1	2	3	$(1, 4, 3, 2)$	r^3
$((1, 2), (1, 2), ())$	2	3	4	1	$(1, 2, 3, 4)$	r
$((1, 2), (1, 2), (1, 2))$	4	3	2	1	$(1, 4)(2, 3)$	s

The column with ψ denotes an embedding $\psi : W \to \mathrm{Sym}(4)$, and the column with $\tilde{\psi}$ denotes an isomorphism $\tilde{\psi} : W \to D_8$, the dihedral group comprising symmetries of a square (see Example 2.14; recall the embedding $D_8 = \langle r, s\rangle \to \mathrm{Sym}(4)$ via $r \mapsto (1, 2, 3, 4)$ and $s \mapsto (1, 4)(2, 3)$).

The corresponding system of imprimitivity is $\Sigma = [[1, 3], [2, 4]]$ (where we impose an ordering); for $w = (g, \omega_1, \omega_2) \in W$, we permute the first block $[1, 3]$ according to ω_1 and the second block $[2, 4]$ according to ω_2, then permute the blocks according to g, and consider the resulting permutation. (For example, $((1, 2), (1, 2), ()) \in W$ corresponds to starting with $\Sigma = [[1, 3], [2, 4]]$, then permuting $[1, 3]$ according to $\omega_1 = (1, 2)$ and $[2, 4]$ according to $\omega_2 = ()$ to get $[3, 1]$ and $[2, 4]$ respectively, then permuting blocks according to $g = (1, 2)$ to get $[[2, 4], [3, 1]]$; the resulting permutation is $(1, 2, 3, 4)$.)

Using generators, we have that $W = \langle(1, 2)\rangle \ltimes (\langle(1, 2)\rangle \times \langle(1, 2)\rangle)$. Note that $\langle(1, 2)\rangle \times \langle(1, 2)\rangle \cong \langle(1, 3), (2, 4)\rangle \leq \mathrm{Sym}(4)$; the group $\langle(1, 2)\rangle$ acts on $\langle(1, 2)\rangle \times \langle(1, 2)\rangle$ by permuting components, so if we apply the relabelling τ we may see that $\langle(1, 2)\rangle \ltimes (\langle(1, 2)\rangle \times \langle(1, 2)\rangle)$ is permutation isomorphic to $\langle(1, 2)(3, 4)\rangle \ltimes \langle(1, 3), (2, 4)\rangle$ where $\langle(1, 2)(3, 4)\rangle$ acts naturally on $\langle(1, 3), (2, 4)\rangle$. (Note that $(1, 2)(3, 4)$ acts naturally on the elements in $\Sigma = [[1, 3], [2, 4]]$ in the same way that $(1, 2)$ permutes the blocks themselves.) So (omitting some details) we get an isomorphism

$$\mathrm{Sym}(2) \wr \mathrm{Sym}(2) = \langle(1, 2)\rangle \ltimes (\langle(1, 2)\rangle \times \langle(1, 2)\rangle) \cong \langle(1, 2)(3, 4)\rangle \ltimes \langle(1, 3), (2, 4)\rangle$$
$$\cong \langle(1, 2)(3, 4), (1, 3), (2, 4)\rangle \cong \langle sr^2, sr, sr^3\rangle = D_8.$$

Definition 5.18. Suppose G acts on Ω and H acts on Γ. Let $W = H \wr_\Omega G$; the **product action** of W on $\Gamma^\Omega = \{\phi \mid \phi :$

$\Omega \to \Gamma\}$ is given by the following: for $(g, \omega) \in W = G \ltimes H^\Omega$ and $\phi \in \Gamma^\Omega$ we define $\phi^{(g,\omega)} \in \Gamma^\Omega$ by

$$\alpha \mapsto \phi(\alpha^{g^{-1}})^{\omega(\alpha)}.$$

The product action is indeed a W-action. First note that for $\phi \in \Gamma^\Omega$ and $\alpha \in \Omega$, $\phi^{(1,1)}(\alpha) = \phi(\alpha^1)^{1(\alpha)} = \phi(\alpha)$, so $\phi^{(1,1)} = \phi$. Then for $(g, \omega), (h, \eta) \in W$ and $\alpha \in \Omega$,

$$(\phi^{(g,\omega)})^{(h,\eta)}(\alpha) = \phi^{(g,\omega)}(\alpha^{h^{-1}})^{\eta(\alpha)} = \phi(\alpha^{h^{-1}g^{-1}})^{\omega(\alpha^{h^{-1}})\eta(\alpha)} = \phi(\alpha^{h^{-1}g^{-1}})^{\omega^h\eta(\alpha)} = \phi^{(gh,\omega^h\eta)}(\alpha),$$

so $(\phi^{(g,\omega)})^{(h,\eta)} = \phi^{(gh,\omega^h\eta)}$. The degree of the product action of W is $|\Gamma|^{|\Omega|}$.

In the case that $\Omega = [n]$, we may identify Γ^Ω with Γ^n via $(\phi : \Omega \to \Gamma) \mapsto (\phi(1), \dots, \phi(n)) \in \Gamma^n$. Then the product action corresponds to $(\phi_1, \dots, \phi_n)^{(g,\omega_1,\dots,\omega_n)} = (\phi_{1g}^{\omega_1}, \dots, \phi_{ng}^{\omega_n})$ for $(\phi_1, \dots, \phi_n) \in \Gamma^n$, $g \in G$ and $(\omega_1, \dots, \omega_n) \in H^n$, where each $i_g = i^{g^{-1}}$. Thus, we permute the components of $(\phi_1, \dots, \phi_n)$ according to g, then apply the permutations ω_i to each component.

Example 5.19. Let $k \le m$ and define an action of $\mathrm{Sym}(m)$ on $\binom{[m]}{k}$, the k-element subsets of $[m]$, by the following: for $\sigma \in \mathrm{Sym}(m)$ and $\{i_1, \dots, i_k\} \subseteq [m]$, let

$$\{i_1, \dots, i_k\}^\sigma = \{i_1^\sigma, \dots, i_k^\sigma\}.$$

This is an action: for $\{i_1, \dots, i_k\} \subseteq [m]$ and $\sigma, \tau \in \mathrm{Sym}(m)$, $\{i_1, \dots, i_k\}^1 = \{i_1^1, \dots, i_k^1\} = \{i_1, \dots, i_k\}$ and

$$\{i_1, \dots, i_k\}^{\sigma\tau} = \{i_1^{\sigma\tau}, \dots, i_k^{\sigma\tau}\} = \{i_1^\sigma, \dots, i_k^\sigma\}^\tau = (\{i_1, \dots, i_k\}^\sigma)^\tau.$$

The degree of the action is $\binom{m}{k}$.

Now consider the wreath product $\mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ with the product action, where the action of $H = \mathrm{Sym}(m)$ is the above action on k-element subsets $\Gamma = \binom{[m]}{k}$ of $[m]$, and the action of $G = \mathrm{Sym}(r)$ is the natural action on $\Omega = [r]$. Here, the product action of the wreath product has degree $|\binom{[m]}{k}|^{|[r]|} = \binom{m}{k}^r$; this example is important for the definition of a large base permutation group. (Note that $|\mathrm{Sym}(m) \wr \mathrm{Sym}(r)| = (m!)^r r!$.)

For example, if $m = 3$, $r = 4$ and $k = 2$, with $g = (1, 2, 4) \in G$ and $(\omega_1, \omega_2, \omega_3, \omega_4) = ((), (1, 2), (1, 2, 3), (2, 3)) \in H^4$, we have (using the identification for $\Omega = [r]$) that

$$\underbrace{\{1,2\}}_{\phi_1}, \underbrace{\{2,3\}}_{\phi_2}, \underbrace{\{1,2\}}_{\phi_3}, \underbrace{\{1,3\}}_{\phi_4})^{((1,2,4),(),(1,2),(1,2,3),(2,3))} = (\underbrace{\{1,3\}^{()}}_{\phi_4}, \underbrace{\{1,2\}^{(1,2)}}_{\phi_1}, \underbrace{\{1,2\}^{(1,2,3)}}_{\phi_3}, \underbrace{\{2,3\}^{(2,3)}}_{\phi_2})$$

$$= (\{1^{()}, 3^{()}\}, \{1^{(1,2)}, 2^{(1,2)}\}, \{1^{(1,3,2)}, 2^{(1,3,2)}\}, \{2^{(2,3)}, 3^{(2,3)}\}) = (\{1,3\}, \{2,1\}, \{3,1\}, \{3,2\}) \in \Gamma^4.$$

The following result gives a simple criterion for the product action of a wreath group to be primitive; see Lemma 2.7A in [12] for a proof.

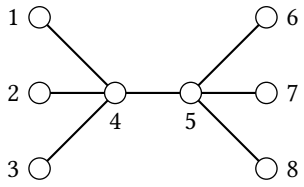
Proposition 5.20. *If nontrivial groups G and H act on Ω and Γ, then the wreath product $W = H \wr_\Omega G$ is primitive in the product action on Γ^Ω if and only if*

(i) H acts primitively but not regularly on Γ, and

(ii) Ω is finite and G acts transitively on Ω.

We conclude with two applications of wreath products to the automorphism group of the graph Γ from Example 2.66 and Rubik's group $G \le \mathrm{Sym}(48)$ from Example 2.41.

Example 5.21. Consider the graph Γ from Example 2.66, shown below.



Recall that Γ has automorphism group

$$\mathrm{Aut}(\Gamma) = \langle (1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8) \rangle.$$

Using GAP, we perform the following computations:

```
gap> G := Group([ (1,6)(2,7)(3,8)(4,5),(1,2),(1,3),(2,3),(6,7),(6,8),(7,8) ]); # generators
Group([ (1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8) ])
gap> StructureDescription( G ); # G is (S3 x S3) : C2, i.e. C2 \ltimes S_3^2 = Sym(3) \wr C2
"(S3 x S3) : C2"
gap> W := WreathProduct( SymmetricGroup(3), Group([ (1,2) ]) );
Group([ (1,2,3), (1,2), (4,5,6), (4,5), (1,4)(2,5)(3,6) ])
gap> IsomorphismGroups( G, W ); # verify it is wreath product
[ (1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8) ] -> [ (1,3), (1,6)(2,5)
    (3,4), (1,4)(2,6)(3,5),
  (1,5)(2,4)(3,6), (1,4)(2,5)(3,6), (1,5)(2,6)(3,4), (1,6)(2,4)(3,5) ]
```

Thus, we see that $\mathrm{Aut}(\Gamma) \cong \mathrm{Sym}(2) \ltimes \mathrm{Sym}(3)^2 = \mathrm{Sym}(3) \wr \mathrm{Sym}(2)$. (This is not a permutation isomorphism, since $\mathrm{Sym}(3) \wr C_2$ has degree 6; it is instead the transitive action of $\mathrm{Aut}(\Gamma)$ on the leaf vertices $\{1,2,3,6,7,8\}$.) Thus, we may permute the two "sides" of the graph (representing the $\mathrm{Sym}(2)$ in $\mathrm{Sym}(3) \wr \mathrm{Sym}(2)$), and within each "side", freely permute the leaf vertices in $\{1,2,3\}$ or $\{6,7,8\}$ (representing the $\mathrm{Sym}(3)$ in $\mathrm{Sym}(3) \wr \mathrm{Sym}(2)$).

Example 5.22. Recall that from Example 2.41, the Rubik's group G acts transitively on the corner stickers 1^G via φ, and primitively on the corners Σ of the Rubik's cube under the action on blocks. Let $\tilde{G}$ denote the image of the transitive G-action on 1^G; it is a permutation group of degree 24 with order $|\tilde{G}| = 88\,179\,840 = 8! \cdot 3^7$, and represents possible Rubik's cube moves if we ignore edge stickers. Then we have a surjective homomorphism $G/\ker\varphi \cong \tilde{G} \to \mathrm{Sym}(\Sigma)$, which is a primitive action (compare this with the quotient action from Example 2.15).

In [1], it is noted that the kernel of this action is isomorphic to the elementary abelian group 3^7. In fact, $\tilde{G} \cong \mathrm{Sym}(8) \ltimes 3^7$, and moreover, $\tilde{G}$ is a subgroup of the wreath product $C_3 \wr \mathrm{Sym}(8) \cong \mathrm{Sym}(8) \ltimes 3^8$ (with the imprimitive action of degree $8 \cdot 3 = 24$) of index 3; this shows we do not have complete freedom in turning the 8 corners — if we turn one corner clockwise, we must turn another anticlockwise [1].

Similarly, it can be shown that G acts transitively on edge stickers 2^G via $\hat{\varphi}$ and primitively on the edges (which are maximal blocks) [1]. The transitive action on edge stickers yields a homomorphism into a group $\hat{G}$ of order $980\,995\,276\,800 = 12! \cdot 2^{11} \approx 9.8 \cdot 10^{11}$ that is permutation isomorphic to $\mathrm{Sym}(11) \ltimes 2^{11}$ which is a subgroup of $C_2 \wr \mathrm{Sym}(12)$. So if an edge is flipped, then another edge is flipped. Also, we can see that G is a *subdirect product* of its transitive constituents $\tilde{G}$ and $\hat{G}$ (see Cameron [6]), thus a subgroup of $\tilde{G} \times \hat{G}$, which is a group of order $2|G|$; the index 2 of G in this direct product shows that we cannot operate on corners and edges completely independently — if we swap a pair of corners, we must swap a pair of edges, and vice versa [1].

5.3 Matrix groups and affine groups

Affine transformations and the affine general linear group

The notion of an affine group is important for the later discussion and results in this thesis. The following results may be found primarily in [12].

Definition 5.23. Let K be a field and V be a vector space over K. Let $\mathrm{GL}(V)$ be the **general linear group** over V, comprising invertible linear maps $V \to V$; note that $\mathrm{GL}(V) \leq \mathrm{Sym}(V)$, so $\mathrm{GL}(V)$ acts naturally on V. When V is finite dimensional, $V \cong K^d$ for some integer d, and thus it suffices to consider the general linear group $\mathrm{GL}(K^d)$.

Invertible linear maps $K^d \to K^d$ (or equivalently $V \to V$ given a choice of basis) may be represented by invertible $d \times d$ matrices in $M_d(K)$, which form the **general linear group** $\mathrm{GL}_d(K)$ **over** K **of degree** d which is isomorphic to

$\mathrm{GL}(K^d)$ (and thus $\mathrm{GL}(V)$). Alternatively, $\mathrm{GL}_d(K) = \{a \in M_d(K) : \det(a) \neq 0\}$. Note that $\mathrm{GL}_d(K)$ acts on K^d by matrix multiplication: for $a \in \mathrm{GL}_d(K)$ and $u \in K^d$ a row vector, we have $u^a = ua$.

When $K = \mathbb{F}_q$ is a finite field, we often write $\mathrm{GL}_d(q) = \mathrm{GL}_d(\mathbb{F}_q)$.

The following definition comes from representation theory; see Example 2.8 for the definition of a representation.

Definition 5.24. Let $G \leq \mathrm{GL}_d(K)$ for some field K. A G-**invariant subspace** of K^d is a subspace $W \leq K^d$ such that $wa \in W$ for all $w \in W$ and $a \in G$. Note that 0 and K^d are always G-invariant; these are the *trivial invariant subspaces*.

The subgroup $G \leq \mathrm{GL}_d(K)$ is **irreducible** if there are no nontrivial G-invariant subspaces (of K^d). (In other words, the *setwise stabilisers* $G_W = \{a \in G : w^a = wa \in W \text{ for all } w \in W\} \neq G$ for $0 < W < K^d$.)

In the language of representation theory, we take $V = K^d$ in the above definition so that $\mathrm{GL}(V) \cong \mathrm{GL}_d(K)$, and the representation $\rho : G \to \mathrm{GL}(V)$ is simply the inclusion map; we identify ρ with G, and irreducibility of G corresponds with irreducibility of ρ.

Definition 5.25. Let K be a field and $d \geq 1$. For an invertible matrix $a \in \mathrm{GL}_d(K)$ and a row vector $v \in K^d$, the corresponding **affine transformation** $t_{a,v} : K^d \to K^d$ is given by $u \mapsto ua + v$ (where we think of $u \in K^d$ as a row vector).

Definition 5.26. The set of invertible affine transformations of K^d forms a group under composition, called the **affine general linear group** of dimension $d \geq 1$ over K, and denoted by $\mathrm{AGL}_d(K) = \{t_{a,v} : a \in \mathrm{GL}_d(K), v \in K^d\}$.

When $K = \mathbb{F}_q$ is a finite field, we often write $\mathrm{AGL}_d(q) = \mathrm{AGL}_d(\mathbb{F}_q)$. (Note that for a d-dimensional vector space V over K, we may similarly define $\mathrm{AGL}(V) = \{t_{a,v} : a \in \mathrm{GL}(V), v \in V\}$ where $t_{a,v} : K \to K$ is given by $u \mapsto u^a + v$.)

The following lemma proves that $\mathrm{AGL}_d(K)$ is indeed a group. In particular, it is a 2-transitive subgroup of $\mathrm{Sym}(K^d)$, the group of *all* bijections $K^d \to K^d$. This shows $\mathrm{AGL}_d(K)$ is a primitive permutation group that acts naturally on K^d (Proposition 2.45); if $K = \mathbb{F}_q$ is finite, $\mathrm{AGL}_d(q)$ has degree q^d. The group $\mathrm{AGL}_d(K)$ is of interest as it respects the affine structure on K^d.

Lemma 5.27. *Let K be a field. The group $\mathrm{AGL}_d(K)$ is a 2-transitive subgroup of $\mathrm{Sym}(K^d)$. In particular, it has identity $1_{\mathrm{AGL}_d(K)} = t_{1,0}$, product $t_{a,v}t_{b,w} = t_{ab,vb+w}$, and inverses $t_{a,v}^{-1} = t_{a^{-1},-va^{-1}}$, for $t_{a,v}, t_{b,w} \in \mathrm{AGL}_d(K)$.*

Proof. First, we show that $\mathrm{AGL}_d(K) \leq \mathrm{Sym}(K^d)$. Indeed, each $t_{a,v} \in \mathrm{AGL}_d(K)$ is a bijection with inverse $t_{a,v}^{-1} = t_{a^{-1},-va^{-1}}$ with $a^{-1} \in \mathrm{GL}_d(K)$ and $-va^{-1} \in K^d$: for $u \in K^d$,

$$(u^{t_{a,v}})^{t_{a^{-1},-va^{-1}}} = (ua+v)^{t_{a^{-1},-va^{-1}}} = (ua+v)a^{-1} - va^{-1} = u$$

and similarly $(u^{t_{a^{-1},-va^{-1}}})^{t_{a,v}} = u$. So $\mathrm{AGL}_d(K) \subseteq \mathrm{Sym}(K^d)$ (and is clearly non-empty, since the identity matrix $1 \in \mathrm{GL}_d(K)$ and $0 \in K^d$). This also shows $\mathrm{AGL}_d(K)$ is closed under inversion, since $t_{a,v}^{-1} = t_{a^{-1},-va^{-1}} \in \mathrm{AGL}_d(K)$.

Now suppose $a, b \in \mathrm{GL}_d(K)$ and $v, w \in K^d$; then the composition

$$t_{a,v}t_{b,w} = t_{ab,vb+w} \in \mathrm{AGL}_d(K)$$

since $ab \in \mathrm{GL}_d(K)$, $vb + w \in K^d$, and for $u \in K^d$,

$$(u^{t_{a,v}})^{t_{b,w}} = (ua+v)b + w = uab + (vb+w) = u^{t_{ab,vb+w}}.$$

So indeed $\mathrm{AGL}_d(K) \leq \mathrm{Sym}(K^d)$; in particular, $\mathrm{AGL}_d(K)$ is a group under composition.

Next we show $\mathrm{AGL}_d(K)$ is 2-transitive. Here, $\mathrm{Sym}(K^d)$ acts naturally on $\Omega = K^d$; since $\mathrm{AGL}_d(K) \leq \mathrm{Sym}(K^d)$, we take the natural action on K^d. Clearly $|\Omega| \geq 2$ (since K is a field and $d \geq 1$). Suppose $[\alpha_1, \alpha_2]$ and $[\beta_1, \beta_2]$ are lists of distinct points in K^d; then extend $a_1 = \alpha_1 - \alpha_2 \neq 0$ and $b_1 = \beta_1 - \beta_2 \neq 0$ to bases $\{a_1, \ldots, a_d\}$ and $\{b_1, \ldots, b_d\}$ of K^d. Let b, c be matrices (in $\mathrm{GL}_d(K)$ by construction) with rows $a_1, \ldots, a_d$ and $b_1, \ldots, b_d$ respectively.

Note that $c = a^{-1}b \in \mathrm{GL}_d(K)$ if and only if $b = ac$, if and only if $b_i = a_i c$ for all $1 \leq i \leq d$. Then $\beta_1 - \beta_2 = b_1 = a_1 c = (\alpha_1 - \alpha_2)c$, which holds if and only if $\beta_1 - \alpha_1 c = \beta_2 - \alpha_2 c$. Let $v = \beta_1 - \alpha_1 c = \beta_2 - \alpha_2 c \in K^d$, so that $[\beta_1, \beta_2] = [\alpha_1 c + v, \alpha_2 c + v] = [\alpha_1^{t_{c,v}}, \alpha_2^{t_{c,v}}]$ with $t_{c,v} \in \mathrm{AGL}_d(K)$. So $\mathrm{AGL}_d(K)$ is 2-transitive. □

From this lemma, we see that affine groups arise as semidirect products of general linear groups over the underlying vector space. In particular, $|\mathrm{AGL}_d(K)| = |\mathrm{GL}_d(K)||K|^d$; if $K = \mathbb{F}_q$ is a finite field (with $|\mathbb{F}_q| = q$ a prime power), it can be shown that $|\mathrm{AGL}_d(q)| = q^d(q^d-1)(q^d-q)\cdots(q^d-q^{d-1})$ (here, the degree of the permutation group $\mathrm{AGL}_d(q)$ is q^d). The case that $q = 2$ is of particular interest, due to a question in [23] which we investigate.

Affine group structure

Proposition 5.28. *The group $\mathrm{AGL}_d(K)$ is isomorphic to the semidirect product $\mathrm{GL}_d(K) \ltimes_\varphi K^d$ via the action φ determined by $v^a = va \in K^d$ for $v \in K^d$ (viewed as a row vector) and $a \in \mathrm{GL}_d(K)$. (So $\mathrm{AGL}_d(K)$ has a subgroup isomorphic to $\mathrm{GL}_d(K)$ and a normal subgroup isomorphic to K^d.)*

Proof. This follows directly from the isomorphism $t_{a,v} \mapsto (a,v) \in \mathrm{GL}_d(K) \ltimes_\varphi K^d$, since $t_{a,v}t_{b,w} = t_{ab,vb+w}$ in $\mathrm{AGL}_d(K)$ (from Lemma 5.27) while $(a,v)(b,w) = (ab, v^b + w) = (ab, vb+w)$ in $\mathrm{GL}_d(K) \ltimes_\varphi K^d$ (by Definition 5.8). □

Proposition 5.29. *(a) The group $\mathrm{AGL}_d(K) \le \mathrm{Sym}(K^d)$ is permutation isomorphic to the subgroup*

$$G^* = \left\{ \begin{pmatrix} a & 0 \\ v & 1_K \end{pmatrix} : a \in \mathrm{GL}_d(K), v \in K^d \right\} \le \mathrm{GL}_{d+1}(K) \le \mathrm{Sym}(\Delta),$$

where $\Delta = K^d \times \{1\} \subseteq K^{d+1}$ is a block under the right-multiplication action of G^* on K^{d+1}, and

(b) $b(\mathrm{AGL}_d(K)) = d+1$, except that $b(\mathrm{AGL}_1(2)) = 1$ (where $d = 1$ and $K = \mathbb{F}_2$).

Proof. (a) The isomorphism $\psi : \mathrm{AGL}_d(K) \to G^*$ is given by

$$t_{a,v} \mapsto \begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix};$$

it is clearly bijective, and indeed $G^* \subseteq \mathrm{GL}_{d+1}(K)$: the rows $a_i \in K^d$ of $a \in \mathrm{GL}_d(K)$ form a basis for K^d, so the $\begin{pmatrix} a_i & 0 \end{pmatrix} \in K^{d+1}$ (viewed as a row vector) are linearly independent for $i = 1, \ldots, d$. In particular, adding $\begin{pmatrix} v & 1 \end{pmatrix} \in K^{d+1}$ to this collection clearly preserves linear independence, and thus forms a basis for K^{d+1}.

Recall from Lemma 5.27 that, for $t_{a,v}, t_{b,w} \in \mathrm{AGL}_d(K)$,

$$t_{a,v}t_{b,w} = t_{ab,vb+w}$$

in $\mathrm{AGL}_d(K)$. This translates to

$$\begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix}\begin{pmatrix} b & 0 \\ w & 1 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ vb+w & 1 \end{pmatrix},$$

in G^*. Thus ψ is a homomorphism (and the image G^* is a subgroup of $\mathrm{GL}_{d+1}(K)$).

Note that $G^* \le \mathrm{GL}_{d+1}(K)$ acts on K^{d+1} by matrix right-multiplication. In particular, Δ is a block under this action: for $\begin{pmatrix} u & 1 \end{pmatrix} \in \Delta$ (viewed as a row vector, with $u \in K^d$), $a \in \mathrm{GL}_d(K)$ and $v \in K^d$, we have $ua + v \in K^d$, so

$$\begin{pmatrix} u & 1 \end{pmatrix}^{\left(\begin{smallmatrix} a & 0 \\ v & 1 \end{smallmatrix}\right)} = \begin{pmatrix} u & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix} = \begin{pmatrix} ua+v & 1 \end{pmatrix} \in \Delta.$$

Then $G^* = G^*_\Delta$, and Lemma 2.37(b) implies G^* acts on Δ.

Define $\tau : K^d \to \Delta$ by $u \mapsto \begin{pmatrix} u & 1 \end{pmatrix} \in K^{d+1}$ (clearly a bijection). Then for $u \in K^d$ and $t_{a,v} \in \mathrm{AGL}_d(K)$, we have

$$\tau(u^{t_{a,v}}) = \tau(ua+v) = \begin{pmatrix} ua+v & 1 \end{pmatrix} = \begin{pmatrix} u & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix} = \tau(u)\begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix} = \tau(u)^{\left(\begin{smallmatrix} a & 0 \\ v & 1 \end{smallmatrix}\right)} = \tau(u)^{\psi(t_{a,v})},$$

so $\mathrm{AGL}_d(K)$ and G^* are permutation isomorphic via τ and ψ.

(b) Note that $B = [e_1, \ldots, e_{d+1}]$ is a base for G^*, where $e_1, \ldots, e_{d+1}$ are the standard basis vectors for K^{d+1}. This follows from the fact that for $a \in \mathrm{GL}_d(K)$ and $v \in K^d$,

$$e_i^{\left(\begin{smallmatrix} a & 0 \\ v & 1 \end{smallmatrix}\right)} = e_i\begin{pmatrix} a & 0 \\ v & 1 \end{pmatrix} = e_i$$

for all i if and only if the ith row of the matrix is e_i for all i, so the matrix is the identity (and $a = 1, v = 0$). (In fact, any basis for K^{d+1} forms a base for G^*.) So $b(\mathrm{AGL}_d(K)) = b(G^*) \le d+1$ (using Lemma 2.63(c)). If $d = 1$ and $K = \mathbb{F}_2$, note that $[0]$ is a base for $\mathrm{AGL}_1(2)$, since if $0^{t_{a,v}} = 0$ then $v = 0a + v = 0$ and $a = 1$ (since $K^* = 1$).

Now suppose $B = [u_1, \dots, u_d] \subseteq K^d$ are all distinct. Then for $k \leq d$ and with $G = \mathrm{AGL}_d(K)$, we have $G_{u_1,\dots,u_d} \leq G_{u_1,\dots,u_k}$, so if $G_{u_1,\dots,u_d} \neq 1$, then $[u_1, \dots, u_k]$ is certainly not a base for G. Now we claim that B is not a base for G. If $d = 1$ and $K \neq \mathbb{F}_2$, then if $u_1 = 0$, then there is $1 \neq a \in K^*$ such that $0^{t_{a,0}} = 0a + 0 = 0$, so B is not a base for G. If $u_1 \neq 0$, then set $u_1 \neq v \in K^*$ (such v exists) and $a = u_1^{-1}(u_1 - v) \in K^*$, then $u_1^{t_{a,v}} = u_1 a + v = u_1 u_1^{-1}(u_1 - v) + v = u_1$, and B is not a base for G.

Now suppose $d \geq 2$. If $\{u_1, \dots, u_d\}$ are linearly independent (and form a basis for K^d), let $b \in \mathrm{GL}_d(K)$ be the matrix with rows u_i, and let c be the matrix with rows $u_i - v$, where $v = u_1 - u_2 \neq 0$. Since $\mathrm{Span}_K\{u_1 - v, u_2 - v\} = \mathrm{Span}_K\{u_2, 2u_2 - u_1\} = \mathrm{Span}_K\{u_1, u_2\}$, it follows that

$$\mathrm{Span}_K\{u_1 - v, u_2 - v, \dots, u_d - v\} = \mathrm{Span}_K\{u_1, u_2, u_3 - v, \dots, u_d - v\} = \mathrm{Span}_K\{u_1, u_2, \dots, u_d\} = K^d,$$

so $\{u_1 - v, u_2 - v, \dots, u_d - v\}$ is linearly independent, and thus $c \in \mathrm{GL}_d(K)$. Now set $a = b^{-1}c \in \mathrm{GL}_d(K)$ (recall $v = u_1 - u_2 \neq 0$); then $t_{a,v} \neq \mathrm{Id}_{K^d}$ satisfies

$$u_i^{t_{a,v}} = u_i a + v = u_i b^{-1} c + v = e_i c + v = (u_i - v) + v = u_i$$

for $i = 1, \dots, d$ (where e_i is the ith standard basis vector in K^d), and B is not a base for G.

If $\{u_1, \dots, u_d\}$ are linearly dependent, let $U = \mathrm{Span}_K\{u_1, \dots, u_d\}$ and write $K^d = U \oplus W$ for some nontrivial subspace $W \leq K^d$. Set $v = 0$ and take $a \in \mathrm{GL}(K^d)$ such that $a|_U = \mathrm{Id}_U$ and $a|_W \neq \mathrm{Id}_W$. Then $u_i^{t_{a,v}} = u_i a + v = u_i$ for $i = 1, \dots, d$, so that $t_{a,v} \in G_{(B)}$, but $w^{t_{a,v}} = wa + v = wa \neq w$ for some $w \in W$, so $t_{a,v} \neq \mathrm{Id}_{K^d}$. Thus B is not a base for G.

From these two cases, we get that $b(\mathrm{AGL}_d(K)) > d$. So $b(\mathrm{AGL}_d(K)) = d + 1$, as claimed. □

Finally, we look at a few important subgroups of the affine group, which we consider again later. This next result expands upon Proposition 5.28.

Proposition 5.30. *(a) The general linear group* $\mathrm{GL}_d(K) \cong \mathrm{GL}(K^d) = \{t_{a,0} : a \in \mathrm{GL}_d(K)\} \leq \mathrm{AGL}_d(K)$ *acts transitively on the nonzero vectors in* $K^d \setminus \{0\}$.

(b) The ***translation subgroup*** $T = \{t_{1,v} : v \in K^d\} \trianglelefteq \mathrm{AGL}_d(K)$ *is a minimal normal subgroup of* $\mathrm{AGL}_d(K)$. *Moreover,* $T \cong K^d$ *and* $\mathrm{AGL}_d(K)/T \cong \mathrm{GL}_d(K)$.

(c) The group $\mathrm{AGL}_d(K)$ *splits over the translation subgroup* T, *and* $\mathrm{AGL}_d(K) = \mathrm{GL}(K^d)T$ *is the product of subgroups.*

Proof. (a) Clearly $\mathrm{GL}(K^d)$ is a subgroup of $\mathrm{AGL}_d(K)$ by the subgroup criterion, since $t_{a,0}t_{b,0} = t_{ab,0}$ and $t_{a,0}^{-1} = t_{a^{-1},0} \in \mathrm{GL}(K^d)$ for $a, b \in \mathrm{GL}_d(K)$. It acts on $K^d \setminus \{0\}$, since for $a \in \mathrm{GL}_d(K)$, $ua = 0$ for $u \in K^d$ if and only if $u = 0$. For $v, w \in K^d \setminus \{0\}$, extend v and w to two ordered bases of K^d; then setting $a \in \mathrm{GL}_d(K)$ to be the change-of-basis matrix from the basis containing v to the basis containing w, we have $v^a = va = w$. So $\mathrm{GL}_d(K)$ acts transitively on $K^d \setminus \{0\}$.

(b) Firstly, the map $\psi : \mathrm{AGL}_d(K) \to \mathrm{GL}_d(K)$ given by $t_{a,v} \mapsto a$ is a surjective homomorphism: for $t_{a,v}, t_{b,w} \in \mathrm{AGL}_d(K)$, $\psi(t_{a,v}t_{b,w}) = \psi(t_{ab,vb+w}) = ab = \psi(t_{a,v})\psi(t_{b,w})$. The kernel of ψ is T, since $t_{a,v} \mapsto 1$ if and only if $a = 1$, if and only if $t_{a,v} = t_{1,v} \in T$. Thus T is a normal subgroup of $\mathrm{AGL}_d(K)$ and $\mathrm{AGL}_d(K)/T \cong \mathrm{GL}_d(K)$ by the first isomorphism theorem. The claim that $T \cong K^d$ is obvious (consider the map $t_{1,v} \mapsto v$).

We now show T is minimal. Suppose $1 \neq N \trianglelefteq \mathrm{AGL}_d(K)$ is a proper subgroup of $T \cong K^d$; we identify N with the corresponding subgroup of K^d (identify $t_{1,v} \sim (1, v) \sim v$). Then for $0 \neq v \in N$ there is $a \in \mathrm{GL}_d(K)$ such that $va \notin N$ (by transitivity of $\mathrm{GL}_d(K)$ on $K^d \setminus \{0\}$ from part (a)), contradicting normality of N. (This is because if N were normal then $(a, w)^{-1}(1, v)(a, w) = (1, va) \sim va \in N$ for all $w \in K^d$.) So no such N exists, and T is minimal.

(c) We know that $T \trianglelefteq \mathrm{AGL}_d(K)$ (part (b)) and $\mathrm{GL}(K^d) \cap T = 1$; it remains to observe that for $t_{a,v} \in \mathrm{AGL}_d(K)$ we have $t_{a,v} = t_{a1,0\cdot 1+v} = t_{a,0}t_{1,v}$ so indeed $\mathrm{AGL}_d(K) = \mathrm{GL}(K^d)T$. □

Symplectic and orthogonal groups

Another important matrix group that we briefly discuss is the symplectic group. The following may be found in section 7.7 of [12]. Let K be a field and consider K^d, where $d = 2m$ is even. Let

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad f = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = e - e^\top,$$

be $d \times d$ block matrices, where 0 and 1 denote the $m \times m$ zero and identity matrices.

Definition 5.31. For $d \geq 2$ even, the **symplectic group** of dimension d over K is $\mathrm{Sp}_d(K) = \{a \in \mathrm{GL}_d(K) : afa^\top = f\} \leq \mathrm{GL}_d(K)$, with the induced action on K^d.

It can be shown that if $K = \mathbb{F}_q$ is a finite field, then writing $\mathrm{Sp}_d(q)$ instead of $\mathrm{Sp}_d(\mathbb{F}_q)$, we have

$$|\mathrm{Sp}_d(q)| = q^{m^2}(q^2-1)(q^4-1)\cdots(q^d-1),$$

where $d = 2m$ (there is a typo on page 245 of [12]). Moreover, the quotient of $\mathrm{Sp}_d(q)$ by its centre gives a finite simple group of Lie type, as described in the classification theorem (Theorem 5.7). We are primarily interested in the case that $K = \mathbb{F}_2$ for the next chapter, where $f = e + e^\top$.

Recall that an orthogonal matrix satisfies $a^\top a = 1$. The set of such matrices (over any field K) forms a group.

Definition 5.32. For any $d \geq 1$, the **(general) orthogonal group** of dimension d over K is $\mathrm{GO}_d(K) = \{a \in \mathrm{GL}_d(K) : a^\top a = 1\} \leq \mathrm{GL}_d(K)$, with the induced action on K^d.

For $K = \mathbb{F}_q$, again write $\mathrm{GO}_d(q)$ instead of $\mathrm{GO}_d(\mathbb{F}_q)$. In the case that $d = 2m$ is even and $q = 2^k$, it can be shown that

$$|\mathrm{GO}_{d+1}(2^k)| = 2^{km^2}(2^{2k}-1)(2^{4k}-1)\cdots(2^{dk}-1).$$

Note that this is equal to $|\mathrm{Sp}_d(2^k)|$. This is no coincidence; in the special case of $q = 2^k$, symplectic groups are related to orthogonal groups. A proof of this next theorem can be found as Theorem 11.9 in Taylor [32].

Theorem 5.33. *For even d, the symplectic group $\mathrm{Sp}_d(2^k)$ is isomorphic to the orthogonal group $\mathrm{GO}_{d+1}(2^k)$.*

5.4 Primitive permutation groups and the O'Nan-Scott theorem

Cameron notes in [6] that intransitive groups are *subdirect products* of their transitive constituents. (A subdirect product is a subgroup H of a direct product $\prod_i G_i$ such that the ith projection $\pi_i : \prod_i G_i \to G_i$ satisfies $\pi_i[H] = G_i$.) A transitive but imprimitive group is contained in the iterated wreath product of its primitive components. Thus, many questions about permutation groups can be reduced to questions about primitive groups. The O'Nan-Scott theorem classifies primitive permutation groups. In particular, [12] notes that combined with the classification of finite simple groups (Theorem 5.7), the O'Nan-Scott theorem is a powerful tool that has helped to answer long-standing problems about permutation groups.

Computationally, in [16], Hulpke presents a recursive way to classify all transitive groups of degree n (up to conjugacy) using the transitive groups of all degrees dividing n and the primitive groups of degree n. Recall from earlier that given transitive groups acting on $\{\Omega_i\}$, we may also study intransitive groups by acting on the disjoint union of the Ω_i. So in a number of senses, primitive groups are a building block for arbitrary permutation groups.

The socle

The following results may be found primarily in [12]. Recall that a **minimal normal subgroup** of a nontrivial group G is a normal subgroup $1 \neq N \trianglelefteq G$ such that $M \lhd N$ with $M \trianglelefteq G$ implies $M = 1$. We define the *socle* of a group, which is important because the O'Nan-Scott theorem characterises finite primitive groups by the structure of their socles.

Definition 5.34. Let G be a group. The **socle** $\mathrm{Soc}(G)$ is the subgroup generated by the set of all minimal normal subgroups of G. If G has no minimal normal subgroups, we use the convention of defining $\mathrm{Soc}(G) = 1$.

Every nontrivial *finite* group G has at least one minimal normal subgroup. (Consider a maximal chain $G = N_0 \rhd N_1 \rhd N_2 \rhd \cdots$ of normal subgroups of G; then $|G| = |N_0| > |N_1| > |N_2| > \cdots$ is a strictly decreasing sequence of positive integers, thus the chain must have finite length, say $G = N_0 \rhd N_1 \rhd N_2 \rhd \cdots \rhd N_{k-1} \rhd N_k = 1$. Then N_{k-1} is a minimal normal subgroup.) Thus, such G has a nontrivial socle. However, this may not be the case for infinite groups: for example, $\mathrm{Soc}(\mathbb{Z}) = 0$, since any nontrivial normal subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for integer $n \geq 1$; then $0 \lhd 2n\mathbb{Z} \lhd n\mathbb{Z}$, and $n\mathbb{Z}$ is thus not minimal.

Example 5.35. Consider $G = \mathbb{Z}/12\mathbb{Z}$, which is abelian; thus every subgroup is normal. By the correspondence theorem (see Theorem 2.28 in [26]), subgroups of $\mathbb{Z}/12\mathbb{Z}$ are precisely of the form $S/12\mathbb{Z}$ where $12\mathbb{Z} \leq S \leq \mathbb{Z}$, so $S \in \{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 6\mathbb{Z}, 12\mathbb{Z}\}$. The group $12\mathbb{Z}/12\mathbb{Z}$ is trivial; the correspondence theorem also gives $\mathbb{Z}/12\mathbb{Z} > 2\mathbb{Z}/12\mathbb{Z} > 4\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z} > 2\mathbb{Z}/12\mathbb{Z} > 6\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z} > 3\mathbb{Z}/12\mathbb{Z} > 6\mathbb{Z}/12\mathbb{Z}$, from which it follows that the minimal normal subgroups of G are $4\mathbb{Z}/12\mathbb{Z}$ and $6\mathbb{Z}/12\mathbb{Z}$.

Thus the socle of G is $\langle 4\mathbb{Z}/12\mathbb{Z}, 6\mathbb{Z}/12\mathbb{Z}\rangle = \langle 4 + 12\mathbb{Z}, 6 + 12\mathbb{Z}\rangle = \langle 2 + 12\mathbb{Z}\rangle = 2\mathbb{Z}/12\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})$.

Lemma 5.36. *The socle* $\mathrm{Soc}(G)$ *is normal in* G*. (In particular, the socle is* ***characteristic****:* $\psi[\mathrm{Soc}(G)] = \mathrm{Soc}(G)$ *for all* $\psi \in \mathrm{Aut}(G)$*.)*

Proof. We consider the case that $\mathrm{Soc}(G) \neq 1$. For a minimal normal subgroup $N \trianglelefteq G$, $\psi[N]$ is minimal normal, since $\psi[N] \trianglelefteq G$ (as $\psi \in \mathrm{Aut}(G)$) and if $M \trianglelefteq G$ satisfies $M \lhd \psi[N]$, then $\psi^{-1}[M] \lhd N$, so $\psi^{-1}[M] = 1$ by minimality, and thus $M = 1$. Moreover, for N, M minimal normal subgroups, $\psi[N] = \psi[M] \implies N = M$, by applying ψ^{-1}. From this, it is clear that $\psi[\mathrm{Soc}(G)] = \mathrm{Soc}(G)$ for all $\psi \in \mathrm{Aut}(G)$, as elements of $\mathrm{Soc}(G)$ are products of elements of minimal normal subgroups (which are permuted amongst themselves by ψ).

Since $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, it follows that $\mathrm{Soc}(G)^g = \mathrm{Soc}(G)$ for all $g \in G$, so $\mathrm{Soc}(G) \trianglelefteq G$. □

If $G \leq \mathrm{Sym}(\Omega)$ is a finite nontrivial permutation group, then we reasoned above that $\mathrm{Soc}(G) \trianglelefteq G$ is nontrivial. Then by Proposition 2.47(c), if G is transitive, it follows that $\mathrm{Soc}(G)$ is a transitive group.

Next, we look at the structure of the socle of a group. First, we give some properties of products of (minimal) normal subgroups.

Lemma 5.37. *Let* $M, N \trianglelefteq G$*. Then:*

(a) The product $MN = \langle M, N\rangle \trianglelefteq G$

(b) If $M \cap N = 1$*, then* $MN \cong M \times N$*.*

(c) If M *is minimal, then* $M \cap N = 1$ *or* $M \leq N$*. In particular, if* M, N *are distinct minimal normal subgroups, then* $M \cap N = 1$ *and* $\langle M, N\rangle = MN$*.*

Proof. (a) Note that $\langle M, N\rangle$ is the smallest subgroup of G containing M, N and $M, N \leq MN$, so certainly $\langle M, N\rangle \leq MN$. However, for $mn \in MN$, we have $m \in M \leq \langle M, N\rangle$ and $n \in N \leq \langle M, N\rangle$, so $mn \in \langle M, N\rangle$. (Showing $MN \trianglelefteq G$ is routine.)

(b) Note that there is a natural isomorphism $MN \to M \times N$ given by $mn \mapsto (m, n)$, which is well-defined since $M \cap N = 1$ (so every element of MN is uniquely mn for $m \in M$ and $n \in N$).

(c) If M is minimal, then $M \cap N \trianglelefteq M$. By minimality, $M \cap N = 1$ or $M \cap N = M$ (which implies $M \leq N$). If N is also minimal (and $M \neq N$), then the case that $M \leq N$ is impossible, as this would contradict minimality or $M \neq N$, so $M \cap N = 1$. □

Since the product of normal subgroups of G is a normal subgroup and $\langle M, N\rangle = MN$, it follows that in the case that G is finite and nontrivial, the socle is the product of the minimal normal subgroups (providing an alternative proof that $\mathrm{Soc}(G) \trianglelefteq G$ in the finite case). Then we may conclude the following:

Proposition 5.38. *If* $G \neq 1$ *is finite, then* $\mathrm{Soc}(G) \cong N_1 \times \cdots \times N_m$ *for some minimal normal subgroups* $N_1, \ldots, N_m$ *of* G*.*

Proof. Since G is finite, we may find a collection of $\{N_1, \ldots, N_m\}$ of minimal normal subgroups of G that is maximal with respect to the property $S = \langle N_1, \ldots, N_m\rangle \cong N_1 \times \cdots \times N_m$. Then $\mathrm{Soc}(G) = S$, since S contains all minimal normal

subgroups of G: suppose not, then there is a minimal normal subgroup N that is not contained in $\langle N_1, \dots, N_m \rangle$. But then $\langle N_1, \dots, N_m \rangle \cap N = 1$ by Lemma 5.37(c), so $\langle N_1, \dots, N_m, N \rangle \cong N_1 \times \cdots \times N_m \times N$, contradicting the choice of $\{N_1, \dots, N_m\}$. □

Proposition 5.39. *The socle of* $\mathrm{AGL}_d(K)$ *is the translation subgroup* $T \cong K^d$.

Proof. Let $S = \mathrm{Soc}(\mathrm{AGL}_d(K))$. From Proposition 5.30(b), we know that T is a minimal normal subgroup of $\mathrm{AGL}_d(K)$, so $T \leq S$. Now suppose for a contradiction that $T < S$. Then there is $s \in S \setminus T$ that is in some other minimal normal subgroup N of $\mathrm{AGL}_d(K)$; by Lemma 5.37(c), $T \cap N = 1$.

Now identifying T with K^d (via $t_{1,v} \sim v$; write $v^{-1} \sim t_{1,v}^{-1} = t_{1,-v}$ and $1 \sim t_{1,0}$), there is $v \in K^d$ with $w = v^{-1}v^s \neq 1$. (This is because $v^{-1}v^s = 1$ if and only if $v^s = s^{-1}vs = v$; with $s = (a, w)$, where $a \in \mathrm{GL}_d(K)$ and $w \in K^d$, this occurs if and only if $v = s^{-1}vs = (a, w)^{-1}(1, v)(a, w) = (1, va) = va$ for some $a \in \mathrm{GL}_d(K)$. However, $s = (a, w) \notin T$, so $a \neq 1$ and therefore such a with $va \neq v$ exists.) But then $w = v^{-1}v^s \in T \trianglelefteq \mathrm{AGL}_d(K)$ and $w = v^{-1}s^{-1}vs = (s^{-1})^v s \in N \trianglelefteq \mathrm{AGL}_d(K)$, so $w = 1$ (since $T \cap N = 1$), a contradiction. So $T = S$. □

By Theorem 4.3A in [12], every minimal subgroup N of finite $G \neq 1$ is (isomorphic to) a direct product $N = T_1 \times \cdots \times T_k$ of simple normal subgroups of K that are conjugate in G. Thus, every minimal normal subgroup of G is elementary abelian, or its centre is trivial (as the centre of a nonabelian simple group is an abelian normal subgroup, thus trivial); moreover, $\mathrm{Soc}(G)$ is a direct product of simple groups.

Now, recall that Proposition 2.47(c) implies a nontrivial normal subgroup of a primitive group is transitive. This restricts the possibilities for minimal normal subgroups of a finite primitive group, and we get the following characterisation of their socles (Corollary 4.3B in [12]).

Theorem 5.40. *If* $G \leq \mathrm{Sym}(\Omega)$ *is a finite primitive group, then* $\mathrm{Soc}(G)$ *is a direct product of isomorphic simple groups.*

Note that this behaviour is seen in Proposition 5.39 for finite $K = \mathbb{F}_{p^k}$ (with p prime), since $\mathrm{AGL}_d(p^k)$ is primitive, and $(\mathbb{F}_{p^k}, +) \cong (\mathbb{F}_p^k, +)$ with $(\mathbb{F}_p, +)$ simple. Moreover, Example 5.35 does not violate this characterisation, since when $\mathbb{Z}/12\mathbb{Z}$ takes the (transitive) right regular action (addition), $\{\{0, 2, 4, 6, 8, 10, 12\}, \{1, 3, 5, 7, 9, 11\}\}$ is a nontrivial block system, and is thus an imprimitive action.

The O'Nan-Scott theorem

Finally, we present the O'Nan-Scott theorem. Chapter 4 of Dixon and Mortimer ([12]) is dedicated to its proof and consequences.

Theorem 5.41 (O'Nan-Scott). *Let* G *be a finite primitive group of degree* n*, and let* $H = \mathrm{Soc}(G)$*. Then either*

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

(b) H *is isomorphic to a direct product* 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* $d \mid m$ *and primitive group* U *with* $\mathrm{Soc}(U) \cong T^d$*, we have that* 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*; or*

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

To conclude this chapter, we make a few comments on the O'Nan-Scott theorem. Suppose that $G \leq \mathrm{Sym}(\Omega)$ has degree n. Then the socle, as a subgroup of G, also acts on Ω. In case (a) of the O'Nan-Scott theorem, if $H = \mathrm{Soc}(G)$ is isomorphic to an elementary abelian p-group and $|H| = p^m = n = |\Omega|$, then since $H \trianglelefteq G$ is transitive, H is automatically regular by Proposition 2.42.

Moreover, computer algebra systems such as GAP have functions that classify primitive permutation groups into their O'Nan-Scott types, as described in the O'Nan-Scott theorem. (In GAP, this is implemented as `ONanScottType`.)

Using the O'Nan-Scott theorem and classification of finite simple groups, the primitive permutation groups of degree less than 1000 were partially classified by Dixon and Mortimer in 1988 (see [11]), with the affine case completed in 2003 by Roney-Dougal and Unger (see [25]). Those of degree less than 2500 were classified by Roney-Dougal in 2005 (see [24]), and those of degree less than 4096 were classified by Coutts, Quick, and Roney-Dougal in 2011 (see [10]), using the same techniques.

Chapter 6

Results on minimum bases for primitive groups

6.1 Results for non-large base primitive permutation groups

Suppose we have a finite primitive permutation group G of degree n. What can we say about $|G|$? (This problem attracted a lot of attention in the 19th century, as noted in [23].) Of course, $|G| \leq n!$, and in the case that $G = \mathrm{Sym}(n)$ which is primitive, we have equality. In the case that $G = \mathrm{Alt}(n)$ which is also primitive, we have $|G| = n!/2 = O(n!)$, which suggests that even in nontrivial cases, the bound cannot be significantly improved on without further restrictions.

From Lemma 2.57, we have that $|G| \leq n^{b(G)}$. Thus, we may find upper bounds on $|G|$ by finding upper bounds on $b(G)$. One of the first results in this direction came in 1889, when Bochert proved in [4] that for a primitive group G of degree n not containing the alternating group $\mathrm{Alt}(n)$, then $b(G) \leq n/2$. Compare this to Example 2.59 and Example 2.60, where we showed that $b(\mathrm{Sym}(n)) = n - 1$ and $b(\mathrm{Alt}(n)) = n - 2$, so the condition of not containing the alternating group immediately leads the upper bound on $b(G)$ improving by a factor of 2. Of course, since $\mathrm{Alt}(n)$ has index 2 in $\mathrm{Sym}(n)$, it is maximal, and thus every primitive group G of degree n, apart from $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$, has $b(G) \leq n/2$.

Improvements to these bounds have been made for primitive groups with certain additional properties. In 1984, Liebeck used the classification of finite simple groups and the O'Nan-Scott theorem to improve the bound on $b(G)$ for *non-large base* permutation groups.

Definition 6.1. A permutation group G of degree n is **large base** if there are integers m and $r \geq 1$ with

$$\mathrm{Alt}(m)^r \trianglelefteq G \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r),$$

where $\mathrm{Sym}(m)$ acts on k-element subsets of $\{1, \ldots, m\}$ for some k, and the wreath product has the product action of degree $n = \binom{m}{k}^r$ if $r > 1$.

(Note that here we mean that G contains a normal subgroup that is permutation isomorphic to $\mathrm{Alt}(m)^r$, where the action of each copy of $\mathrm{Alt}(m)$ is also on k-element subsets of $[m]$, and the direct product acts on r-tuples of these (see Example 2.20). Also, we mean that G is permutation isomorphic to a subgroup of the wreath product $\mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ with the product action. Such convention is common in permutation group literature, where inclusion or equality is up to permutation isomorphism.)

By this definition, $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ with their natural actions are large base, where we choose $m = n$ and $r = 1$; recall that $\mathrm{Sym}(n) \wr \mathrm{Sym}(1) \cong \mathrm{Sym}(n)$, and $\mathrm{Alt}(n) \trianglelefteq \mathrm{Sym}(n)$. Thus, the non-large base primitive groups exclude $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$, and there is no conflict with Bochert's result in [4].

Example 6.2. Recall that in Example 5.21, we showed that $\mathrm{Aut}(\Gamma) \cong \mathrm{Sym}(3) \wr C_2$; if we act on the leaf vertices $\{1, 2, 3, 6, 7, 8\}$, then we have a homomorphism $\mathrm{Aut}(\Gamma) \to H$ into a transitive group H of degree $n = 6$, and this is a

permutation isomorphism. However, the action $\mathrm{Sym}(3) \wr C_2$ is the imprimitive action of degree $2 \cdot 3 = 6$, so if we have $H \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ with the product action, we must have $6 = \binom{m}{k}^r$ with $r = 1$ and $(m, k) \in \{(6, 1), (4, 2)\}$. Now, we cannot have $(m, k) = (4, 2)$, since $|H| = 72 > 4!$. Thus $(m, k) = (6, 1)$, and we consider the natural action of $\mathrm{Sym}(6)$, and certainly $H \leq \mathrm{Sym}(6)$. But it has index 10 in $\mathrm{Sym}(6)$, thus does not contain $\mathrm{Alt}(6)$, and H is not large base. We can see that $b(H) = 4$ (using a similar argument to Example 2.66); note that $b(H) > n/2 = 3$, but H is not primitive ($\Sigma = \{\{1, 2, 3\}, \{6, 7, 8\}\}$ is a system of imprimitivity), so there is no contradiction with Bochert's result.

The following result by Liebeck is found in [20], which is an improvement on Bochert's result.

Theorem 6.3 (Liebeck, 1984). *Let G be a primitive group of degree n. Then one of the following holds:*

(i) G is large base; or

(ii) $b(G) < 9 \log n$.

Thus, if a primitive group is large base, then it has a "large base" in the sense that the minimal base size satisfies $b(G) \geq 9 \log n$. The result was proven in context improving lower bounds on $\mu(G)$, the **minimal degree** of $G \leq \mathrm{Sym}(\Omega)$, which is the smallest number of points moved by any non-identity element in G, i.e.

$$\mu(G) = \min_{g \in G \setminus \{1\}} |\{\alpha \in \Omega : \alpha^g \neq \alpha\}|.$$

For example, $\mu(\mathrm{Alt}(n)) = 3$ for $n \geq 3$, since $\mathrm{Alt}(n)$ contains 3-cycles (which move 3 points) but no transpositions (which move 2 points). From the relation that $b(G)\mu(G) \geq n$ for any transitive group G of degree n (see [7] for proof), Liebeck concludes that either G is large base, or that $\mu(G) > n/(9 \log n)$. The best result that was previously available, due to Babai in [2], was that $\mu(G) > (1/2)(\sqrt{n} - 1)$ as long as $\mathrm{Alt}(n) \not\leq G$ (which would give, by properties of big-O,

$$b(G) < 2\sqrt{n}\left(1 - \frac{1}{\sqrt{n}}\right)^{-1} = 2\sqrt{n}\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right) = 2\sqrt{n} + O(1) = O(\sqrt{n}),$$

i.e. a square-root bound on $b(G)$); the logarithmic bound on $b(G)$ in Liebeck represented a major improvement, and has been seen as a remarkable result [23].

Liebeck's proof of Theorem 6.3 in [20] is approached in four steps. Firstly, a reduction to simple socle is performed: supposing the theorem is true for primitive groups with a nonabelian simple socle, then considering arbitrary primitive G to prove part (i) of the theorem. Then, by considering cases in the O'Nan-Scott theorem, Liebeck shows that it suffices to assume $\mathrm{Soc}(G) = T$ is simple. The second step uses the classification of finite simple groups to analyse the structure of the nonabelian simple socle T, leading to the conclusion that T is an alternating group, a group of Lie type, or a sporadic group, or that $|G| < n^9$. The third step shows that these non-large base groups from step two satisfy (ii) in Theorem 6.3, and step four uses the previous steps to complete the proof.

In 2019, Halasi, Liebeck and Maróti show in Theorem 1.1 of [14] that the minimal base size of an arbitrary primitive group of degree n satisfies $b(G) \leq 2(\log |G|/\log n) + 24$, with the multiplicative constant 2 being best possible, answering the well-known *Pyber's conjecture* of the existence of a universal constant c with $b(G) < c(\log |G|/\log n)$ for all primitive groups G, which was open until initially proven in 2018. In particular, [14] shows that for most non-large base primitive groups G, the minimal base size satisfies $b(G) \leq 2\lfloor \log n \rfloor + 26$; in 2020, "most" was improved to *"all"* [23].

In 2021, building on the previously mentioned results of Liebeck in [20] and Halasi, Liebeck and Maróti in [14], Moscatiello and Roney-Dougal improve the bound on $b(G)$ to $\lceil \log n \rceil + 1$ for non-large base primitive groups, with one exception. The following is Theorem 1 in this paper [23]; it is the main result.

Theorem 6.4 (Moscatiello and Roney-Dougal, 2021). *Let G be primitive group of degree n. If G is non-large base, then either:*

(i) G is the Mathieu group M_{24} in its 5-transitive action of degree 24; or

(ii) $b(G) \leq \lceil \log n \rceil + 1$.

Moreover, there are infinitely many G that are non-large base, for which $b(G) > \log n + 1$.

The **Mathieu groups** are five sporadic simple permutation groups M_{11}, M_{12}, M_{22}, M_{23} and M_{24} of degree 11, 12, 22,

23 and 24 respectively, with multiply transitive actions. They were introduced by Mathieu between 1861 and 1873, and were the first sporadic simple groups to be discovered. The final observation in Theorem 6.4 considers groups G with $\log n + 1 < b(G) \leq \lceil \log n \rceil + 1$ (aside from the one exception of M_{24}), which would require that $b(G) = \lceil \log n \rceil + 1$ and that n is not a power of 2.

Example 6.5. Recall that in Example 5.22, we showed that the action of the Rubik's group on the corner stickers yields a homomorphism into a permutation group $\tilde{G}$ of degree $n = 24$, that is permutation isomorphic to $\mathrm{Sym}(8) \ltimes 3^7 \leq C_3 \wr \mathrm{Sym}(8)$ (with the imprimitive action of degree 24). Suppose that $\tilde{G} \leq \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ with the product action; then we must have $m = 24$ and $r = k = 1$, so that $24 = \binom{m}{k}^r$. But $|\tilde{G}| < 24!/2$, so $\tilde{G}$ does not contain $\mathrm{Alt}(24)$, and $\tilde{G}$ is not large base.

Similar analysis shows that the Rubik's group G with degree $n = 48$ is non-large base; we have $b(G) = 18$. Note that even though $b(G) < 9 \log n \approx 50$ (the bound from Liebeck, Theorem 6.3), we have $b(G) > \lceil \log n \rceil + 1 = 7$ (the bound from Theorem 6.4). This is no contradiction, since G is not primitive.

Finally, we recall that G acts on the corners Σ of the cube (which are blocks of size 3) primitively; the resulting primitive group is the full symmetric group $\mathrm{Sym}(\Sigma) \cong \mathrm{Sym}(8)$ of degree $n = 8$ (see Example 2.41). This is large base, with $m = 8$ and $r = k = 1$ (it certainly contains $\mathrm{Alt}(8)$), and the results in this section do not apply (it has minimal base size $n - 1 = 7$).

Next, we present Theorem 5 from [23], which is a more detailed version of Theorem 6.4. It mostly investigates the case in (ii) above of $\log n + 1 \leq b(G) \leq \lceil \log n \rceil + 1$, which collapses to $b(G) = \lceil \log n \rceil + 1$.

Theorem 6.6 (Moscatiello and Roney-Dougal, 2021). *Let G be primitive subgroup of $\mathrm{Sym}(\Omega)$ with $|\Omega| = n$. Then $b(G) \geq \log n + 1$ if and only if G is one of following:*

(i) A subgroup of $\mathrm{AGL}_d(2)$ with $b(G) = d + 1 = \log n + 1$.

(ii) The symplectic group $\mathrm{Sp}_d(2)$ with $d \geq 4$; then $\log n + 1 < b(G) = \lceil \log n \rceil + 1$.

(iii) A Mathieu group M_n in its natural permutation representation with $n \in \{12, 23, 24\}$. If $n = 12$ or 23 then $b(G) = \lceil \log n \rceil + 1$, while if $n = 24$ then $b(G) = 7 > \lceil \log n \rceil + 1$.

The infinite number of primitive groups G of degree n with $b(G) > \log n + 1$, as mentioned in Theorem 6.4, is demonstrated by case (ii) in the more detailed theorem above; in case (i), it is conditional on the existence of such subgroups $G \leq \mathrm{AGL}_d(2)$ with $b(G) = d + 1$. Thus, the authors conclude the paper [23] with a question:

Question 6.7 (Moscatiello and Roney-Dougal, 2021). *Which primitive groups $G \leq \mathrm{Sym}(n)$ satisfy $b(G) = \log n + 1$?*

Of course, we require that $\log n$ is an integer, so that n is a power of 2. By Theorem 6.6, we must have $G \leq \mathrm{AGL}_d(2)$ for some d (indeed, $\mathrm{AGL}_d(2)$ acts on $n = 2^d$ points; all other cases in the theorem have $b(G) > \log n + 1$), and if d is even then it is noted in [23] that groups such as the split extension $2^d : \mathrm{Sp}_d(2)$ have this property (we will assume this in the rest of this thesis). Are there any more such groups? What about for odd d? Investigating this question forms the remainder of this thesis.

6.2 Primitive subgroups of affine groups with given minimal base size

The main result of this section is as follows.

Theorem 6.8. *Let G be a primitive subgroup of $\mathrm{AGL}_d(2)$ for some d, with the induced action of degree $n = 2^d$.*

(i) For $d = 1$, there is no such G with $b(G) = d + 1 = \log n + 1$.

(ii) For odd $3 \leq d \leq 9$ and $d = 2$, if $b(G) = d + 1 = \log n + 1$, then G is the affine group $\mathrm{AGL}_d(2)$.

(iii) For even $4 \leq d \leq 10$, if $b(G) = d + 1 = \log n + 1$, then G is either $\mathrm{AGL}_d(2)$ or $2^d : \mathrm{Sp}_d(2)$.

Our approach to this result is to use GAP to iterate over potential primitive groups $G \leq \mathrm{AGL}_d(2)$ for some d and compute a bound on $b(G)$ to eliminate those groups for which a base of size less than $d + 1$ is found. Using the FinInG

(finite incidence geometry) package, we use a permutation representation of $\mathrm{AGL}_d(2)$ (a subgroup of $\mathrm{Sym}(2^d)$). Note that if a base of size r is found for G, then $b(G) \leq r$, so if $r < d+1$, we may eliminate such G.

To compute a base for G, GAP has the built-in command `BaseOfGroup`, which uses the (randomised) Schreier-Sims algorithm. However, in various test cases, we find that when compared to our implementation of the greedy base algorithm (Algorithm 4.2) analysed in Blaha [3], the greedy algorithm sometimes finds a smaller base than the built-in command. For instance, when running a modified version of the program that proves Theorem 6.8 with $d = 6$, a permutation group G of degree 64 and order 3 612 672 (in fact, a primitive subgroup of $\mathrm{AGL}_6(2)$) was found, for which `BaseOfGroup` finds a base of size $7 = d+1$, while `GreedyBase` finds a base of size $5 < d+1$; this led to a number of false positives in an initial analysis. (See the appendix for GAP code verifying this.)

Thus, in the procedure to prove the main theorem, we use our implementation of `GreedyBase` instead of `BaseOfGroup` to compute a base for G (see appendix for implementation). Both algorithms are fast; as discussed earlier, the greedy base algorithm is a polynomial-time algorithm. Of course, neither algorithm necessarily finds a minimum base for G, but in conjunction with Theorem 4.18, we see that a greedy base for G has size at most $\lceil b(G)\log\log n\rceil + b(G) = \lceil b(G)\log d\rceil + b(G) = O(b(G)\log d)$, which is fine for our purposes (and in practice does not lead to any issues for our result — all subgroups with $b(G) < d+1$ have been identified).

The remainder of this section is dedicated to our approach to proving Theorem 6.8, which is an original proof. Note that all subgroups take the induced subgroup action.

Proof of main theorem. First, we consider $d = 1$ in case (i). First note that $|\mathrm{AGL}_1(2)| = 2^1(2^1 - 1) = 2$, so if G is a primitive subgroup then $G = \mathrm{AGL}_1(2)$ (the trivial subgroup is not transitive, thus not primitive). By Proposition 5.29, $b(\mathrm{AGL}_1(2)) = 1 < d+1$. This proves the result for case (i).

Fix $2 \leq d \leq 10$; first, note that if G is the affine group $\mathrm{AGL}_d(2)$, then by Proposition 5.29, $b(G) = d+1$. It remains to check proper primitive subgroups G of $\mathrm{AGL}_d(2)$ to identify those with $b(G) = d+1$. To do so, we adopt a "brute force approach" with a number of optimisations. It uses the following observations to avoid checking *all* primitive subgroups of $\mathrm{AGL}_d(2)$, especially at any given stage in the process:

1. *Once we find a subgroup G with $b(G) < d+1$, we do not need to consider any of its (proper) subgroups.* This is due to Lemma 2.58, which says that if $H \leq G$, then $b(H) \leq b(G) < d+1$.
2. *If we find a non-primitive (imprimitive or intransitive) subgroup G, we do not need to consider any of its subgroups.* This is because subgroups of non-primitive groups (that act on Ω) are non-primitive: suppose $\Sigma = \{\Delta^g : g \in G\}$ is a system of imprimitivity for G transitive, where Δ is a block. Then for transitive $H \leq G$, Δ is clearly a block for the induced H-action, and $\Sigma = \{\Delta^h : h \in H\}$ is a system of imprimitivity for H. If G is intransitive, then there is $\alpha \in \Omega$ with $\alpha^G \neq \Omega$; then $\alpha^H \subseteq \alpha^G$ for $H \leq G$, so H is intransitive.
3. *If we have G with $b(G) = d+1$, we may recursively check maximal subgroups.* This is because $\mathrm{AGL}_d(2)$ is finite, so for arbitrary $H \leq G$, we have a *finite* subgroup series
$$H = H_0 < H_1 < \cdots < H_k = G$$
where each H_i is maximal in H_{i+1} (else insert intermediate groups in the series). Thus, if $b(H) = d+1$, then we must have $b(H_i) = d+1$ for all i, by observation 1 above; recursively checking maximal subgroups will guarantee that we eventually find H.
4. *At each stage, it suffices to check maximal subgroups up to conjugacy.* This is because Proposition 2.62 implies that $b(G^\sigma) = b(G)$ for all $\sigma \in \mathrm{Sym}(\Omega)$, where G acts on Ω, so that we may consider a representative from each conjugacy class of subgroups. Moreover, if G is maximal, then G^σ is also maximal by Lemma 2.27, which implies that checking only maximal subgroups up to conjugacy will not overlook any conjugacy classes of subgroups. This observation also leads to a significant improvement over the naïve approach, since the size of a conjugacy class of subgroups may be large. However, it means that the subgroups found by the process are unique only up to conjugacy.

These observations can be adapted for any group, to find (primitive) subgroups H with $b(H) > r$ for any given r, by simply replacing "d" with "r". If we wish to ignore the condition of primitivity, we may simply ignore observation 2 above.

Below, we present the generalised recursive algorithm for an arbitrary permutation group G, based on the above observations, that allows us to find all (primitive) proper subgroups $H \leq G$ with $b(H) > r$. In particular, if $b(H) > r$, then the algorithm identifies H up to conjugacy; however, it could also incorrectly identify H with $b(H) \leq r$ in the process. Any (conjugacy classes of) subgroups H omitted certainly have $b(H) \leq r$. (An alternative is to use a brute force approach to compute $b(H)$ exactly, but this is much more inefficient, and comes with few, if any, advantages.)

1: **procedure** GetSubgrpBase(G, r, L) ▷ Finds all primitive $H \leq G$ with $b(H) > r$, storing in list L
2: $\tilde{L} \leftarrow [\,]$ ▷ Initialise new list for newly found candidates
3: **for** representatives $M < G$ of conjugacy classes of maximal subgroups of G **do** ▷ Observation 4 above
4: **if** M is primitive **then** $\ell \leftarrow$ Length(GreedyBase(M)) ▷ Can drop condition of primitivity here
5: **if** $\ell > r$ **then** add M to L and $\tilde{L}$ ▷ Primitive candidate for $b(M) > r$
6: **for** H in $\tilde{L}$ **do**
7: $L \leftarrow$ GetSubgrpBase(H, r, L) ▷ Recursively run on candidates H in $\tilde{L}$
8: **return** L ▷ L now contains all $H < G$ with $b(H) > r$ up to conjugacy

Note that the algorithm does not check the initial group G itself, so this must be performed separately. See the appendix for an implementation in GAP using the functions `GetSubgrpBase` and `GetSubgrpAGLBase` (for the special case of $\mathrm{AGL}_d(2)$ and testing for $G \leq \mathrm{AGL}_d(2)$ with $b(G) > d$, i.e. $b(G) = d+1$); these also print out various information about the subgroups identified in the process.

Let us now return to the notation of Theorem 6.8, where G is a primitive proper subgroup of $\mathrm{AGL}_d(2)$ for given $2 \leq d \leq 10$. Running `GetSubgrpAGLBase( d )` yields the following (see appendix for output):

- If $d = 2$, no groups G are found. (2 maximal primitive subgroups M are considered, but each has $b(M) < d+1$.)
- If $d = 3$, no groups G are found. (3 maximal primitive subgroups M are considered, but each has $b(M) < d+1$.)
- If $d = 4$, one group G is found, which must be $2^4 : \mathrm{Sp}_4(2)$.
- If $d = 5$, no groups G are found. (2 maximal primitive subgroups M are considered, but each has $b(M) < d+1$.)
- If $d = 6$, one group G is found, which must be $2^6 : \mathrm{Sp}_6(2)$.
- If $d = 7$, no groups G are found. (2 maximal primitive subgroups M are considered, but each has $b(M) < d+1$.)
- If $d = 8$, one group G is found, which must be $2^8 : \mathrm{Sp}_8(2)$.
- If $d = 9$, no groups G are found. (5 maximal primitive subgroups M are considered, but each has $b(M) < d+1$.)
- If $d = 10$, one group G is found, which must be $2^{10} : \mathrm{Sp}_{10}(2)$.

(Note that in each case for which a group G is found for some d, it has the correct order to be $2^d : \mathrm{Sp}_d(2)$; to verify this, observe that its order is $2^d |\mathrm{Sp}_d(2)| = 2^d |\mathrm{GO}_{d+1}(2)|$ by Theorem 5.33, which we verify in GAP.)

In the case that $d = 2$ or $3 \leq d \leq 9$ is odd, we see that there are no proper subgroups $G \leq \mathrm{AGL}_d(2)$ with $b(G) = d+1$, which completes case (ii) of the theorem. In the remaining case that $4 \leq d \leq 10$ is even, we see that if $G \leq \mathrm{AGL}_d(2)$ satisfies $b(G) = d+1$, then G must be $2^d : \mathrm{Sp}_d(2)$; combining this with the observation by Moscatiello and Roney-Dougal in [23] that $b(2^d : \mathrm{Sp}_d(2)) = d+1$ completes case (iii) and the entire proof. □

This result seems to suggest that the groups identified by Moscatiello and Roney-Dougal in [23] are possibly the only primitive groups with the given property; any counterexamples must be subgroups of the affine group over $\mathbb{F}_2$ of dimension at least 11, which are large groups, and finding such groups would perhaps be surprising. A limitation of our proof approach is that it only works practically for $d \leq 10$, due to memory and computational time constraints, but is nevertheless an interesting approach. In particular, the group identified for $d = 10$ has order $25\,410\,822\,678\,459\,187\,200 \approx 2.5 \cdot 10^{19}$ and thus has many subgroups. Without a more systematic way of describing its maximal primitive subgroups, this approach cannot be used for larger values of d: the case that $d = 9$ took 5 mins, the case that $d = 10$ took 100 mins, and the case that $d = 11$ took over 48 hours without returning a result.

A more efficient identification of maximal primitive subgroups in $\mathrm{AGL}_d(2)$, such as if a classification result exists, could lead to a vast improvement in the running time of the `GetSubgrpAGLBase` algorithm, and potentially lead to this approach being useful to verify results for larger values of d. This is because at each stage, the procedure often identified

only 2–5 primitive subgroups; the majority of the time spent is GAP attempting to find maximal subgroups up to conjugacy. Additionally, other algorithms to find bases and minimal base size could be employed, but the greedy algorithm is already quite fast and performs well.

Based on this discussion and the behaviour in Theorem 6.8, we summarise and conclude with the following conjecture in the direction of Question 6.7.

Conjecture 6.9. *A primitive group $G \leq \mathrm{Sym}(n)$ satisfies $b(G) = \log n + 1$ if and only if G is one of the following:*

(i) $n = 2^d$ with $d \geq 2$, and G is the affine group $\mathrm{AGL}_d(2)$; or

(ii) $n = 2^d$ with $d \geq 4$ even, and G is the split extension $2^d : \mathrm{Sp}_d(2)$.

Our theorem and prior results from [23] show that this is true for $n < 2^{11}$. Any counterexamples must be permutation groups of degree $n = 2^d$ with $d \geq 11$ that are a subgroup of $\mathrm{AGL}_d(2)$.

References

[1] Analyzing Rubik's Cube with GAP. URL: https://www.gap-system.org/Doc/Examples/rubik.html.

[2] Laszlo Babai. On the order of uniprimitive permutation groups. *The Annals of Mathematics*, 113(3):553, 1981. doi:10.2307/2006997.

[3] Kenneth D. Blaha. Minimum bases for permutation groups: The greedy approximation. *Journal of Algorithms*, 13(2):297–306, 1992. doi:10.1016/0196-6774(92)90020-D.

[4] Alfred Bochert. Ueber die zahl der verschiedenen werthe, die eine function gegebener buchstaben durch vertauschung derselben erlangen kann. *Mathematische Annalen*, 33(4):584–590, 1889. doi:10.1007/bf01444035.

[5] Cynthia A. Brown, Larry Finkelstein, and Paul W. Purdom. Backtrack searching in the presence of symmetry. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 99–110. Springer Berlin Heidelberg, 1989. doi:10.1007/3-540-51083-4_51.

[6] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, 1999. doi:10.1017/cbo9780511623677.

[7] Peter J. Cameron, Peter M. Neumann, and Jan Saxl. On groups with no regular orbits on the set of subsets. *Archiv der Mathematik*, 43(4):295–296, 1984. doi:10.1007/bf01196649.

[8] John J. Cannon and George Havas. Algorithms for groups. *Australian Computer Journal*, 24(2):51–60, 1992. doi:10.48550/arXiv.math/9406203.

[9] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and Eamonn A. O'Brien. Generating random elements of a finite group. *Communications in Algebra*, 23(13):4931–4948, 1995. doi:10.1080/00927879508825509.

[10] Hannah J. Coutts, Martyn Quick, and Colva M. Roney-Dougal. The primitive permutation groups of degree less than 4096. *Communications in Algebra*, 39(10):3526–3546, 2011. doi:10.1080/00927872.2010.515521.

[11] John D. Dixon and B. Mortimer. The primitive permutation groups of degree less than 1000. *Mathematical Proceedings of the Cambridge Philosophical Society*, 103:213–238, 1988. doi:10.1017/S0305004100064793.

[12] John D. Dixon and Brian Mortimer. *Permutation Groups*. Springer New York, 1996. doi:10.1007/978-1-4612-0731-3.

[13] Michael R. Garey and David S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., USA, 1990.

[14] Zoltán Halasi, Martin W. Liebeck, and Attila Maróti. Base sizes of primitive groups: Bounds with explicit constants. *Journal of Algebra*, 521:16–43, 2019. doi:10.1016/j.jalgebra.2018.10.043.

[15] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of Computational Group Theory*. Chapman and Hall/CRC, New York, 2005. doi:10.1201/9781420035216.

[16] Alexander Hulpke. Constructing transitive permutation groups. *Journal of Symbolic Computation*, 39(1):1–30, 2005. doi:10.1016/j.jsc.2004.08.002.

[17] Zvonimir Janko. A new finite simple group with abelian 2-Sylow subgroups. *Proceedings of the National Academy of Sciences*, 53(3):657–658, 1965. doi:10.1073/pnas.53.3.657.

[18] R. Karp. Reducibility among combinatorial problems. In R. Miller and J. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972. doi:10.1007/978-1-4684-2001-2_9.

[19] Donald E. Knuth. Efficient representation of perm groups. *Combinatorica*, 11(1):33–43, 1991. doi:10.1007/bf01375471.

[20] Martin W. Liebeck. On minimal degrees and base sizes of primitive permutation groups. *Archiv der Mathematik*, 43(1):11–15, 1984. doi:10.1007/bf01193603.

[21] Donald Livingstone. On a permutation representation of the Janko group. *Journal of Algebra*, 6(1):43–55, 1967. doi:10.1016/0021-8693(67)90012-9.

[22] László Lovász. Matroid matching and some applications. *Journal of Combinatorial Theory, Series B*, 28(2):208–236, 1980. doi:10.1016/0095-8956(80)90066-0.

[23] Mariapia Moscatiello and Colva M. Roney-Dougal. Base sizes of primitive permutation groups. *Monatshefte für Mathematik*, 198(2):411–443, 2021. doi:10.1007/s00605-021-01599-5.

[24] Colva M. Roney-Dougal. The primitive permutation groups of degree less than 2500. *Journal of Algebra*, 292(1):154–183, 2005. doi:10.1016/j.jalgebra.2005.04.017.

[25] Colva M. Roney-Dougal and William R. Unger. The affine primitive permutation groups of degree less than 1000. *Journal of Symbolic Computation*, 35(4):421–439, 2003. doi:10.1016/s0747-7171(03)00031-2.

[26] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Springer New York, 1995. doi:10.1007/978-1-4612-4176-8.

[27] Charles C. Sims. Computational methods in the study of permutation groups. In John Leech, editor, *Computational Problems in Abstract Algebra*, pages 169–183. Pergamon, 1970. doi:https://doi.org/10.1016/B978-0-08-012975-4.50020-5.

[28] Charles C. Sims. The existence and uniqueness of Lyons' group. In *Finite Groups '72, Proceedings of the the Gainesville Conference on Finite Groups*, pages 138–141. Elsevier, 1973. doi:10.1016/s0304-0208(08)71841-3.

[29] Michael Sipser. *Introduction to the Theory of Computation*. Course Technology, Boston, MA, 3rd edition, 2013.

[30] Ronald Solomon. A brief history of the classification of the finite simple groups. *Bulletin of the American Mathematical Society*, 38(3):315–352, 2001. doi:10.1090/s0273-0979-01-00909-0.

[31] Ronald Solomon. The classification of finite simple groups: A progress report. *Notices of the American Mathematical Society*, 65(06):1, 2018. doi:10.1090/noti1689.

[32] D.E. Taylor. *The Geometry of the Classical Groups*. Sigma Series in Pure Mathematics 9. Heldermann Verlag, 1992.

Appendix A

Appendix — theory of permutation groups

Note that Adobe Acrobat allows you to copy the following code without line numbers. All code in this thesis is implemented and tested in GAP version 4.12.0.

A.1 Rubik's group

Here is GAP code relevant to Example 2.41. First we define the Rubik's group $G \leq \mathrm{Sym}(48)$.

```
U := ( 1, 3, 8, 6)( 2, 5, 7, 4)( 9,33,25,17)(10,34,26,18)(11,35,27,19);;
L := ( 9,11,16,14)(10,13,15,12)( 1,17,41,40)( 4,20,44,37)( 6,22,46,35);;
F := (17,19,24,22)(18,21,23,20)( 6,25,43,16)( 7,28,42,13)( 8,30,41,11);;
R := (25,27,32,30)(26,29,31,28)( 3,38,43,19)( 5,36,45,21)( 8,33,48,24);;
B := (33,35,40,38)(34,37,39,36)( 3, 9,46,32)( 2,12,47,29)( 1,14,48,27);;
D := (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40);;
G := Group( U, L, F, R, B, D );
```

Then, we compute orbits, restrict the action to GC (which acts on corners), look at maximal blocks under this action (which are the corners), then analyse the primitive action on corners (which is GCBhom).

```
gap> Order( G );
43252003274489856000
gap> R*U*R^(-1)*U^(-1);
(1,27,35,33,9,3)(2,21,5)(8,30,25,43,19,24)(26,34,28)
gap> Order( last );
6
gap> R*U;
(1,3,38,43,11,35,27,32,30,17,9,33,48,24,6)(2,5,36,45,21,7,4)(8,25,19)(10,34,26,29,31,28,18)
gap> Order( last );
105
gap> corners := Orbit( G, 1 ); # corner stickers
[ 1, 6, 40, 27, 8, 35, 16, 41, 32, 25, 48, 3, 11, 24, 46, 33, 43, 17, 30, 14, 19, 9, 22, 38 ]
gap> Orbit( G, 2 ); # edge stickers
[ 2, 5, 12, 7, 36, 10, 47, 4, 28, 45, 34, 13, 29, 44, 20, 42, 26, 21, 37, 15, 31, 18, 23, 39
    ]
gap> GC := Action( G, corners );
<permutation group with 6 generators>
gap> GChom := ActionHomomorphism( G, corners ); # transitive action on corner stickers (
    relabels)
```

```
<action homomorphism>
gap> NrMovedPoints( GC );
24
gap> Order( GC );
88179840
gap> F;
(6,25,43,16)(7,28,42,13)(8,30,41,11)(17,19,24,22)(18,21,23,20)
gap> GChom( F ); # image of F under action on corner stickers
(2,10,17,7)(5,19,8,13)(14,23,18,21)
gap> MB := MaximalBlocks( GC, corners );
[ [ 1, 6, 22 ], [ 2, 13, 18 ], [ 3, 15, 20 ], [ 4, 12, 16 ], [ 5, 10, 21 ], [ 7, 8, 23 ], [ 9,
     11, 24 ], [ 14, 17, 19 ] ]
gap> MBorig := List( [ 1..8 ], i -> corners{MB[i]} ); # maximal block using original
    labelling
[ [ 1, 35, 9 ], [ 6, 11, 17 ], [ 40, 46, 14 ], [ 27, 3, 33 ], [ 8, 25, 19 ], [ 16, 41, 22 ],
    [ 32, 48, 38 ], [ 24, 43, 30 ] ]
gap> GCB := Action( GC, MB, OnSets );
Group([ (1,2,4,3), (1,3,6,5), (1,5,8,2), (3,4,7,6), (5,6,7,8), (2,8,7,4) ])
gap> GCBhom := ActionHomomorphism( GC, MB ); # primitive action on corners (action on blocks)
<action homomorphism>
gap> NrMovedPoints( GCB );
8
gap> Order( GCB );
40320
gap> Factorial(8); # Thus GCB is Sym(8)
40320
gap> GChom(F);
(2,10,17,7)(5,19,8,13)(14,23,18,21)
gap> GCBhom(last); # image of F under primitive action on corners
(2,5,8,6)
gap> List( [ 2, 5, 8, 6 ], i -> MBorig[i] ); # convert to original labelling
[ [ 6, 11, 17 ], [ 8, 25, 19 ], [ 24, 43, 30 ], [ 16, 41, 22 ] ]
```

The following code is relevant to Example 2.71, using the above definition of G.

```
gap> Base := BaseOfGroup( G );
[ 1, 3, 6, 8, 2, 4, 5, 7, 12, 13, 14, 15, 16, 21, 23, 24, 29, 31 ]
gap> Length( Base );
18
gap> H := FreeGroup("u","l","f","r","b","d");
<free group on the generators [ u, l, f, r, b, d ]>
gap> h := GroupHomomorphismByImages( H, G, GeneratorsOfGroup( H ), GeneratorsOfGroup( G ) );
[ u, l, f, r, b, d ] -> [ (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19),
  (1,17,41,40)(4,20,44,37)(6,22,46,35)(9,11,16,14)(10,13,15,12), (6,25,43,16)(7,28,42,13)
    (8,30,41,11)(17,19,24,
    22)(18,21,23,20), (3,38,43,19)(5,36,45,21)(8,33,48,24)(25,27,32,30)(26,29,31,28),
  (1,14,48,27)(2,12,47,29)(3,9,46,32)(33,35,40,38)(34,37,39,36), (14,22,30,38)(15,23,31,39)
    (16,24,32,40)(41,43,48,
    46)(42,45,47,44) ]
gap> x := Random( G ); # random element of Rubik's group
(1,27,32,6,43,14,22)(2,28,13,37,18,15,47,42,31)(3,38,17,24,46,41,9)(5,26)
    (7,44,39,23,45,34,21,20,12)(11,30,40,16,35,33,48)(29,36)
```

```
gap> PreImagesRepresentative( h, x ); # factorise into generators using GAP and stabiliser chains (equivalent to solving)
l*f^-1*l^-1*f*u*f*u^-1*f^2*l*f*l^-1*u^-1*l^-1*u*l*u^-1*l*u*f*u^-1*f^-1*l^-2*u*l*f^-1*l*f*(l^-1*u)^2*b^-1*u*b*l*u*l^-1*f^-1*l^-1*f*l^2*u*l^-1*u*l*b^-1*u^-1*b*l*d*f^2\
*d^-1*l*f^-1*u*l^-1*f*u^-1*l*d^-1*l*b*d*u^-2*b^-1*r^-1*b*u^-1*r*f^-1*u*d^-2
gap> Length( last );
78
gap> x = L*F^(-1)*L^(-1)*F*U*F*U^(-1)*F^2*L*F*L^(-1)*U^(-1)*L^(-1)*U*L*U^(-1)*L*U*F*U^(-1)*F^(-1)*L^(-2)*U*L*F^(-1)*L*F*(L^(-1)*U)^2*B^(-1)*U*B*L*U*L^(-1)*F^(-1)*L^(-1)*F*L^2*U*L^(-1)*U*L*B^(-1)*U^(-1)*B*L*D*F^2*D^(-1)*L*F^(-1)*U*L^(-1)*F*U^(-1)*L*D^(-1)*L*B*D*U^(-2)*B^(-1)*R^(-1)*B*U^(-1)*R*F^(-1)*U*D^(-2);
true
```

The following code is relevant to Example 4.3, using the above definition of G.

```
GBase := GreedyBase( G );
[ 1, 2, 4, 3, 5, 7, 6, 12, 8, 13, 14, 15, 21, 16, 23, 24, 29, 39 ]
gap> Length( GBase );
18
gap> Stabilizer( G, GBase, OnTuples ); # verify that it is base
Group(())
gap> Stabilizer( G, [ 1, 2, 4, 3, 5, 7, 6, 12, 8, 13, 14, 15, 21, 16, 23, 24, 29 ], OnTuples ); # remove edge sticker; not a base
Group([ (31,45)(39,47) ])
gap> Stabilizer( G, [ 1, 2, 4, 3, 5, 7, 6, 12, 8, 13, 14, 15, 21, 16, 23, 24, 39 ], OnTuples ); # remove corner sticker; not a base
Group([ (29,36)(31,45) ])
```

A.2 Random elements and the constructive membership problem

Here is an implementation of Algorithm 2.67 in GAP as the function RandomElt:

```
RandomElt := function( SC ) # SC is stabiliser chain, encodes G
  local g, o, t;
  g := ();
  while SC.generators <> [ ] do
    o := Random( SC.orbit ); # uniformly random orbit element
    # get corresponding uniformly random element in transversal
    t := InverseRepresentative( SC, o )^(-1);
    g := t * g;
    SC := SC.stabilizer; # proceeds to next stabiliser in chain
  od;
  return g;
end;
```

Here is an implementation of Algorithm 2.69 in GAP as the function Membership (using two subfunctions):

```
Factorisation := function( SC, g ) # SC is stabiliser chain, encodes G
  local B, i, h, tInv, fact;
  B := BaseStabChain( SC ); # gets base B
  i := 0;
  h := g;
```

```
  fact := [ ]; # factorisation
  while SC.generators <> [ ] do # while stabiliser not trivial
    i := i + 1;
    if not IsBound( SC.transversal[B[i]^h] ) then
      return [ h, i, fact ];
    fi;
    tInv := InverseRepresentative( SC, B[i]^h );
    h := h * tInv;
    fact := Concatenation( [ tInv^(-1) ], fact );
    SC := SC.stabilizer; # proceeds to next stabiliser in chain
  od;
  return [ h, i, fact ];
end;

Strip := function( SC, g ) # SC is stabiliser chain, encodes G
  local fact;
  fact := Factorisation( SC, g );
  return [ fact[1], fact[2] ];
end;

Membership := function( SC, g ) # SC is stabiliser chain, encodes G
  return Strip( SC, g )[1] = ();
end;
```

Here is the modified version of `RandomElt` which prints out intermediate choices of $t_i \in T_i$ and calculations $g \in G$, as used in Example 2.68:

```
RandomEltPrint := function( SC ) # SC is stabiliser chain, encodes G
  local g, o, t, i;
  g := ();
  i := 0;
  while SC.generators <> [ ] do
    i := i + 1;
    o := Random( SC.orbit ); # uniformly random orbit element
    # get corresponding uniformly random element in transversal
    t := InverseRepresentative( SC, o )^(-1);
    g := t * g;
    Print( "i = ", i,":\tt_i = ", t, "\tg <- ", g, "\n" );
    SC := SC.stabilizer; # proceeds to next stabiliser in chain
  od;
  return g;
end;
```

Here is the modified version of `Membership` which prints out values of $t_i \in T_i$ and h, as used in Example 2.70:

```
FactorisationPrint := function( SC, g ) # SC is stabiliser chain, encodes G
  local B, i, h, tInv, fact;
  B := BaseStabChain( SC ); # gets base B
  i := 0;
  h := g;
  fact := [ ]; # factorisation
  while SC.generators <> [ ] do # while stabiliser not trivial
    i := i + 1;
```

```
    if not IsBound( SC.transversal[B[i]^h] ) then
      return [ h, i, fact ];
    fi;
    tInv := InverseRepresentative( SC, B[i]^h );
    h := h * tInv;
    Print( "i = ", i, ":\tt_", i, " = ", tInv^(-1), ",\th <- ", h, "\n" );
    fact := Concatenation( [ tInv^(-1) ], fact );
    SC := SC.stabilizer; # proceeds to next stabiliser in chain
  od;
  return [ h, i, fact ];
end;

StripPrint := function( SC, g ) # SC is stabiliser chain, encodes G
  local fact;
  fact := FactorisationPrint( SC, g );
  return [ fact[1], fact[2] ];
end;

MembershipPrint := function( SC, g ) # SC is stabiliser chain, encodes G
  return StripPrint( SC, g )[1] = ();
end;
```

Stabiliser chain for automorphism group of graph

Here is some more output relevant to Example 2.66:

```
gap> G := Group([ (1,6)(2,7)(3,8)(4,5),(1,2),(1,3),(2,3),(6,7),(6,8),(7,8) ]); # generators
Group([ (1,6)(2,7)(3,8)(4,5), (1,2), (1,3), (2,3), (6,7), (6,8), (7,8) ])
gap> SC := StabChain( G, B ); # stabiliser chain of G with respect to base B
<stabilizer chain record, Base [ 4, 1, 2, 6, 7 ], Orbit length 2, Size: 72>
gap> StrongGeneratorsStabChain( SC ); # get strong generating set for G
[ (7,8), (6,7), (6,8), (2,3), (1,2), (1,3), (1,6)(2,7)(3,8)(4,5) ]
gap> SizeStabChain( SC ); # gets |G|
72
gap> OrbitStabChain( SC, 1 ); # gets 1^G
[ 1, 6, 2, 7, 3, 8 ]
gap> OrbitStabChain( SC, 4 ); # gets 4^G
[ 4, 5 ]
gap> IndicesStabChain( SC ); # gets indexes of stabilisers in chain SC
[ 2, 3, 2, 3, 2 ]
gap> ListStabChain( SC );
[ <stabilizer chain record, Base [ 4, 1, 2, 6, 7 ], Orbit length 2, Size: 72>,
  <stabilizer chain record, Base [ 1, 2, 6, 7 ], Orbit length 3, Size: 36>,
  <stabilizer chain record, Base [ 2, 6, 7 ], Orbit length 2, Size: 12>,
  <stabilizer chain record, Base [ 6, 7 ], Orbit length 3, Size: 6>,
  <stabilizer chain record, Base [ 7 ], Orbit length 2, Size: 2>,
  rec( generators := [  ], genlabels := [  ], identity := (),
      labels := [ (), (7,8), (2,3)(7,8), (1,6)(2,7)(3,8)(4,5), (6,7,8), (1,2,3)(6,7,8) ] ) ]
gap> ElementsStabChain( SC ); # lists all elements of G
[ (), (7,8), (6,7), (6,7,8), (6,8,7), (6,8), (2,3), (2,3)(7,8), (2,3)(6,7), (2,3)(6,7,8),
  (2,3)(6,8,7), (2,3)(6,8), (1,2), (1,2)(7,8), (1,2)(6,7), (1,2)(6,7,8), (1,2)(6,8,7),
```

```
  (1,2)(6,8), (1,2,3), (1,2,3)(7,8), (1,2,3)(6,7), (1,2,3)(6,7,8), (1,2,3)(6,8,7),
  (1,2,3)(6,8), (1,3,2), (1,3,2)(7,8), (1,3,2)(6,7), (1,3,2)(6,7,8), (1,3,2)(6,8,7),
  (1,3,2)(6,8), (1,3), (1,3)(7,8), (1,3)(6,7), (1,3)(6,7,8), (1,3)(6,8,7), (1,3)(6,8),
  (1,6)(2,7)(3,8)(4,5), (1,6)(2,7,3,8)(4,5), (1,6,2,7)(3,8)(4,5), (1,6,2,7,3,8)(4,5),
  (1,6,3,8,2,7)(4,5), (1,6,3,8)(2,7)(4,5), (1,6)(2,8,3,7)(4,5), (1,6)(2,8)(3,7)(4,5),
  (1,6,2,8,3,7)(4,5), (1,6,2,8)(3,7)(4,5), (1,6,3,7)(2,8)(4,5), (1,6,3,7,2,8)(4,5),
  (1,7,2,6)(3,8)(4,5), (1,7,3,8,2,6)(4,5), (1,7)(2,6)(3,8)(4,5), (1,7,3,8)(2,6)(4,5),
  (1,7)(2,6,3,8)(4,5), (1,7,2,6,3,8)(4,5), (1,7,2,8,3,6)(4,5), (1,7,3,6)(2,8)(4,5),
  (1,7)(2,8,3,6)(4,5), (1,7,3,6,2,8)(4,5), (1,7)(2,8)(3,6)(4,5), (1,7,2,8)(3,6)(4,5),
  (1,8,3,7,2,6)(4,5), (1,8,2,6)(3,7)(4,5), (1,8,3,7)(2,6)(4,5), (1,8)(2,6)(3,7)(4,5),
  (1,8,2,6,3,7)(4,5), (1,8)(2,6,3,7)(4,5), (1,8,3,6)(2,7)(4,5), (1,8,2,7,3,6)(4,5),
  (1,8,3,6,2,7)(4,5), (1,8)(2,7,3,6)(4,5), (1,8,2,7)(3,6)(4,5), (1,8)(2,7)(3,6)(4,5) ]
gap> SiftedPermutation( SC, (4,5) ); # result after sifting (4,5) through SC
(1,6)(2,7)(3,8)
gap> SiftedPermutation( SC, (1,2,3) );
()
gap> InverseRepresentative( SC, 4 ); # transversal element that maps 4 back to 4 in G
()
gap> InverseRepresentative( SC, 5 ); # transversal element that maps 5 back to 4 in G
(1,6)(2,7)(3,8)(4,5)
gap> # Analysing G_1 = Stab_G(4)
gap> SC1 := ListStabChain( SC )[2]; # considers subchain for G_1
<stabilizer chain record, Base [ 1, 2, 6, 7 ], Orbit length 3, Size: 36>
gap> OrbitStabChain( SC1, 1 ); # gets 1^{G_1}
[ 1, 2, 3 ]
gap> OrbitStabChain( SC1, 4 ); # gets 4^{G_1}
[ 4 ]
gap> OrbitStabChain( SC1, 5 ); # gets 5^{G_1}
[ 5 ]
gap> OrbitStabChain( SC1, 6 ); # gets 6^{G_1}
[ 6, 7, 8 ]
gap> ElementsStabChain( SC1 ); # lists all elements of G_1
[ (), (7,8), (6,7), (6,7,8), (6,8,7), (6,8), (2,3), (2,3)(7,8), (2,3)(6,7),
  (2,3)(6,7,8), (2,3)(6,8,7), (2,3)(6,8), (1,2), (1,2)(7,8), (1,2)(6,7),
  (1,2)(6,7,8), (1,2)(6,8,7), (1,2)(6,8), (1,2,3), (1,2,3)(7,8), (1,2,3)(6,7),
  (1,2,3)(6,7,8), (1,2,3)(6,8,7), (1,2,3)(6,8), (1,3,2), (1,3,2)(7,8), (1,3,2)(6,7),
  (1,3,2)(6,7,8), (1,3,2)(6,8,7), (1,3,2)(6,8), (1,3), (1,3)(7,8), (1,3)(6,7),
  (1,3)(6,7,8), (1,3)(6,8,7), (1,3)(6,8) ]
gap> InverseRepresentative( SC1, 3 ); # transversal element that maps 3 back to 1 in G_1
(1,3)
gap> # Random elements and membership
gap> g := Random( G ); # gets random element of G
(1,7,3,6)(2,8)(4,5)
gap> (4,5) in G; # checks membership in G
false
gap> (1,6,2,7,3,8)(4,5) in G; # checks membership in G
true
gap> H := Stabilizer( SymmetricGroup(8), [ 4, 5 ], OnTuples ) # H is the pointwise stabiliser
     of 4 and 5 in Sym(8)
Sym( [ 1, 2, 3, 6, 7, 8 ] )
gap> g := Random( H ); # gets random element of H
```

```
(1,8,6)(2,7)
gap> g in G; # checks membership in G
false
gap> g := Random( H ); # gets random element of H
(2,3)(6,7)
gap> g in G; # checks membership in G
true
```

Lines 28–41 describe all elements of $G = \mathrm{Aut}(\Gamma)$. Lines 62–67 describe all elements of $G_1 = \mathrm{Stab}_G(4)$.

A.3 Wreath product and dihedral group

Here is GAP code relevant to Example 5.17:

```
tau := function( m, n )
  if m = 1 and n = 1 then return 1; fi;
  if m = 1 and n = 2 then return 3; fi;
  if m = 2 and n = 1 then return 2; fi;
  if m = 2 and n = 2 then return 4; fi;
  return 0;
end;

tauInv := function( i )
  if i = 1 then return [ 1, 1 ]; fi;
  if i = 3 then return [ 1, 2 ]; fi;
  if i = 2 then return [ 2, 1 ]; fi;
  if i = 4 then return [ 2, 2 ]; fi;
  return [ 0, 0 ];
end;

imprimActionD8 := function( i, g, w1, w2 )
  local m, n, w;
  m := tauInv( i )[1];
  n := tauInv( i )[2];
  if m^g = 1 then w := w1; else w := w2; fi;
  return tau( m^g, n^w );
end;

imprimActionD8List := function( g, w1, w2 )
  return [ imprimActionD8( 1, g, w1, w2 ), imprimActionD8( 2, g, w1, w2 ), imprimActionD8( 3,
     g, w1, w2 ), imprimActionD8( 4, g, w1, w2 ) ];
end;

imprimActionD8ListFull := function( )
  local perm, g, w1, w2, result;
  result := [];
  for g in SymmetricGroup(2) do
    for w1 in SymmetricGroup(2) do
      for w2 in SymmetricGroup(2) do
        perm := imprimActionD8List( g, w1, w2 );
        Add( result, [ g, w1, w2, perm, PermList(perm) ] );
```

```
      od;
    od;
  od;
  return result;
end;
```

The following is the output which is summarised in the table in the example:

```
gap> PrintArray(imprimActionD8ListFull());
[ [             (),             (),             (),  [ 1, 2, 3, 4 ],             () ],
  [             (),             (),          (1,2),  [ 1, 4, 3, 2 ],          (2,4) ],
  [             (),          (1,2),             (),  [ 3, 2, 1, 4 ],          (1,3) ],
  [             (),          (1,2),          (1,2),  [ 3, 4, 1, 2 ],      (1,3)(2,4) ],
  [          (1,2),             (),             (),  [ 2, 1, 4, 3 ],      (1,2)(3,4) ],
  [          (1,2),             (),          (1,2),  [ 4, 1, 2, 3 ],       (1,4,3,2) ],
  [          (1,2),          (1,2),             (),  [ 2, 3, 4, 1 ],       (1,2,3,4) ],
  [          (1,2),          (1,2),          (1,2),  [ 4, 3, 2, 1 ],      (1,4)(2,3) ] ]
```

Appendix B

Appendix — computing bases of subgroups of affine groups

B.1 Greedy base algorithm

Below is GAP code for an implementation of the greedy base algorithm from Algorithm 4.2 as GreedyBase:

```
GreedyBase := function( G, opt... ) # G is perm group (natural action), opt[1] is partial
    base
  local B, S, OLen, LargestOrbitList, LargestOrbitPos, b;
  if Length( opt ) = 0 then
    B := [ ]; # if not given then start with empty base
  else
    B := opt[1];
  fi;
  S := Stabilizer( G, B, OnTuples );
  while IsTrivial( S ) = false do
    # evaluate orbits in S and get element from a largest orbit
    OLen := OrbitLengthsDomain( S );
    LargestOrbitList := PositionsProperty( OLen, n -> ( n = Maximum( OLen ) ) );
    LargestOrbitPos := Random( LargestOrbitList );
    b := OrbitsDomain( S )[LargestOrbitPos][1];
    # add to base
    Add(B, b);
    S := Stabilizer( S, b );
    od;
  return B;
end;
```

The following example of a permutation group G of degree 64 shows that GreedyBase sometimes finds a smaller base than the built-in command BaseOfGroup:

```
gap> gens := [ (1,2)(3,4)(5,6)(7,8)(9,10)(11,12)(13,14)(15,16)(17,18)(19,20)(21,22)(23,24)
    (25,26)(27,28)(29,30)(31,32)(33,34)(35,36)(37,38)(39,40)(41,42)(43,44)(45,46)(47,
    48)(49,50)(51,52)(53,54)(55,56)(57,58)(59,60)(61,62)(63,64), (1,30)(2,29)(3,32)(4,31)
    (5,26)(6,25)(7,28)(8,27)(9,22)(10,21)(11,24)(12,23)(13,18)(14,17)(15,
    20)(16,19)(33,62)(34,61)(35,64)(36,63)(37,58)(38,57)(39,60)(40,59)(41,54)(42,53)(43,56)
```

```
    (44,55)(45,50)(46,49)(47,52)(48,51), (1,37)(2,38)(3,39)(4,40)(5,33)(6,
4   34)(7,35)(8,36)(9,45)(10,46)(11,47)(12,48)(13,41)(14,42)(15,43)(16,44)(17,53)(18,54)
    (19,55)(20,56)(21,49)(22,50)(23,51)(24,52)(25,61)(26,62)(27,63)(28,64)(29,
5   57)(30,58)(31,59)(32,60), (1,33)(2,34)(3,35)(4,36)(5,37)(6,38)(7,39)(8,40)(9,41)(10,42)
    (11,43)(12,44)(13,45)(14,46)(15,47)(16,48)(17,49)(18,50)(19,51)(20,
6   52)(21,53)(22,54)(23,55)(24,56)(25,57)(26,58)(27,59)(28,60)(29,61)(30,62)(31,63)(32,64),
    (1,48)(2,47)(3,46)(4,45)(5,44)(6,43)(7,42)(8,41)(9,40)(10,39)(11,
7   38)(12,37)(13,36)(14,35)(15,34)(16,33)(17,64)(18,63)(19,62)(20,61)(21,60)(22,59)(23,58)
    (24,57)(25,56)(26,55)(27,54)(28,53)(29,52)(30,51)(31,50)(32,49),
8  (1,60)(2,59)(3,58)(4,57)(5,64)(6,63)(7,62)(8,61)(9,52)(10,51)(11,50)(12,49)(13,56)(14,55)
    (15,54)(16,53)(17,44)(18,43)(19,42)(20,41)(21,48)(22,47)(23,46)(24,
9   45)(25,36)(26,35)(27,34)(28,33)(29,40)(30,39)(31,38)(32,37), (33,49)(34,50)(35,51)(36,52)
    (37,53)(38,54)(39,55)(40,56)(41,57)(42,58)(43,59)(44,60)(45,61)(46,
10  62)(47,63)(48,64), (9,17,33)(10,18,34)(11,19,35)(12,20,36)(13,21,37)(14,22,38)(15,23,39)
    (16,24,40)(25,49,41)(26,50,42)(27,51,43)(28,52,44)(29,53,45)(30,54,
11  46)(31,55,47)(32,56,48), (2,9)(3,17)(4,25)(5,33)(6,41)(7,49)(8,57)(11,18)(12,26)(13,34)
    (14,42)(15,50)(16,58)(20,27)(21,35)(22,43)(23,51)(24,59)(29,36)(30,
12  44)(31,52)(32,60)(38,45)(39,53)(40,61)(47,54)(48,62)(56,63) ];
13 gap> G := Group( gens );
14 <permutation group with 9 generators>
15 gap> NrMovedPoints( G );
16 64
17 gap> Order( G );
18 3612672
19 gap> BaseOfGroup( G );
20 [ 1, 2, 3, 5, 9, 17, 33 ]
21 gap> Size( last );
22 7
23 gap> GreedyBase( G );
24 [ 1, 10, 19, 37, 11 ]
25 gap> Size( last );
26 5
27 gap> Stabilizer( G, last2, OnTuples ); # check that we indeed have a base
28 Group(())
```

B.2 Program to find primitive subgroups with given minimal base size

Below is GAP code for the recursive program that was used to identify conjugacy classes of (primitive) proper subgroups G of $\mathrm{AGL}_d(2)$ (for given d) which may satisfy $b(G) = d + 1$. It includes the greedy base algorithm as described above (so that the code is fully self-contained).

Given $d \geq 1$, running `GetSubgrpAGLBase( d )` gives a list of candidate primitive subgroups of $\mathrm{AGL}_d(2)$ with minimal base size $d + 1$, according to the greedy base algorithm (which seemed to perform better than the built-in `BaseOfGroup` function which presented false positives).

The `GetSubgrpAGLBase` function relies on the function `GetSubgrpBase`; note that `GetSubgrpBase( r, G )` returns information about proper (primitive) subgroups H of a group G such that the greedy base algorithm finds no base of size at most r (thus are candidates for $b(H) > r$). Thus, the program can be easily adjusted to answer similar questions for different families of groups.

```
1 LoadPackage("FinInG");
```

```
2
3  GreedyBase := function( G, opt... ) # G is perm group (natural action), opt[1] is partial
       base
4    local B, S, OLen, LargestOrbitList, LargestOrbitPos, b;
5    if Length( opt ) = 0 then
6      B := [ ]; # if not given then start with empty base
7    else
8      B := opt[1];
9    fi;
10   S := Stabilizer( G, B, OnTuples );
11   while IsTrivial( S ) = false do
12     # evaluate orbits in S and get element from a largest orbit
13     OLen := OrbitLengthsDomain( S );
14     LargestOrbitList := PositionsProperty( OLen, n -> ( n = Maximum( OLen ) ) );
15     LargestOrbitPos := Random( LargestOrbitList );
16     b := OrbitsDomain( S )[LargestOrbitPos][1];
17     # add to base
18     Add(B, b);
19     S := Stabilizer( S, b );
20   od;
21   return B;
22 end;
23
24 GetSubgrpBase := function( r, G, opt... )
25   # gets proper subgrps H of G which are the only candidates (up to conjugacy) for b(H) > r (
       using greedy base alg)
26   # opt[1] = if only considering primitive subgrps, opt[2] = list of candidate subgrps found
       (for recursion)
27   local onlyPrim, M, res, newRes, num, max, greedyBase;
28   newRes := [ ];
29   if Length( opt ) = 0 then
30     onlyPrim := false;
31     res := [ ];
32   elif Length( opt ) = 1 then
33     onlyPrim := opt[1];
34     res := [ ];
35   else
36     onlyPrim := opt[1];
37     res := opt[2];
38   fi;
39   num := 0;
40   # compute maximal subgroups only up to conjugacy!
41   max := MaximalSubgroupClassReps( G );
42
43   Print( "Considered grp of size ", Size( G ), " with ", Size( GeneratorsOfGroup( G ) ), "
       gens:\n");
44   Print( "Found ", Size( max ), " maximal subgroups (up to conj)\n" );
45   for M in max do
46     if IsPrimitive( M ) or not onlyPrim then
47       num := num + 1;
48       greedyBase := GreedyBase( M );
```

```
      if Length( greedyBase ) > r then
        Add( res, M );
        Add( newRes, M );
      fi; # use greedy base alg
    fi;
  od;

  Print( "Considered ",  num, " maximal subgrps (up to conj)\n" );
  Print( "Found ", Size( newRes ), " subgrps that may have base of length > ", r, "\n" );
  Print( "GAP's base command finds bases of length:\n" );
  Display( List( newRes, M -> Size( BaseOfGroup( M ) ) ) );
  Print( "Greedy base alg finds bases of length:\n");
  Display( List( newRes, M -> Length( GreedyBase( M ) ) ) );
  for M in newRes do
    Print( "\n" );
    res := GetSubgrpBase( r, M, onlyPrim, res );
  od;
  return res;
end;

GetSubgrpAGLBase := function( d, opt... )
  # gets subgroups H of AGL(d,2) with b(H) = d+1 (only guess, using algorithm)
  # opt[1] = if only considering primitive subgrps
  local AffS, G, n, onlyPrim;
  if Length( opt ) = 0 then
    onlyPrim := true;
  else
    onlyPrim := opt[1];
  fi;
  AffS := AffineSpace( d, 2 );
  G := Action( AffineGroup( AffS ), Points( AffS ) ); # sets G = AGL(d,2) as perm group
  n := NrMovedPoints( G );
  if not n = 2^d then Error( "ops" ); fi;
  return GetSubgrpBase( d, G, onlyPrim );
end;
```

Program output for low dimensional affine groups

Below is output for $d = 2$:

```
gap> res2 := GetSubgrpAGLBase(2);
Considered grp of size 24 with 3 gens:
Found 3 maximal subgroups (up to conj)
Considered 2 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 2
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[  ]
```

Below is output for $d = 3$:

```
gap> res3 := GetSubgrpAGLBase(3);
Considered grp of size 1344 with 3 gens:
Found 5 maximal subgroups (up to conj)
Considered 3 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 3
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[  ]
```

Below is output for $d = 4$:

```
gap> res4 := GetSubgrpAGLBase(4);
Considered grp of size 322560 with 3 gens:
Found 7 maximal subgroups (up to conj)
Considered 4 maximal subgrps (up to conj)
Found 1 subgrps that may have base of length > 4
GAP's base command finds bases of length:
[ 5 ]
Greedy base alg finds bases of length:
[ 5 ]

Considered grp of size 11520 with 3 gens:
Found 8 maximal subgroups (up to conj)
Considered 5 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 4
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[ Group([ (3,7)(4,8)(9,10)(11,16)(12,15)(13,14), (2,7,13,10,3)(4,8,11,6,12)(5,14,16,15,9),
    (1,9)(2,10)(3,11)(4,12)
      (5,13)(6,14)(7,15)(8,16) ]) ]
```

Below is output for $d = 5$:

```
gap> res5 := GetSubgrpAGLBase(5);
Considered grp of size 319979520 with 3 gens:
Found 6 maximal subgroups (up to conj)
Considered 2 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 5
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[  ]
```

Below is output for $d = 6$:

```
gap> res6 := GetSubgrpAGLBase(6);
Considered grp of size 1290157424640 with 3 gens:
```

```
Found 10 maximal subgroups (up to conj)
Considered 5 maximal subgrps (up to conj)
Found 1 subgrps that may have base of length > 6
GAP's base command finds bases of length:
[ 7 ]
Greedy base alg finds bases of length:
[ 7 ]

Considered grp of size 92897280 with 8 gens:
Found 10 maximal subgroups (up to conj)
Considered 5 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 6
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[ <permutation group of size 92897280 with 8 generators> ]
```

Below is output for $d = 7$:

```
gap> res7 := GetSubgrpAGLBase(7);
Considered grp of size 20972799094947840 with 3 gens:
Found 8 maximal subgroups (up to conj)
Considered 2 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 7
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[  ]
```

Below is output for $d = 8$:

```
gap> res8 := GetSubgrpAGLBase(8);
Considered grp of size 1369104324918194995200 with 3 gens:
Found 11 maximal subgroups (up to conj)
Considered 4 maximal subgrps (up to conj)
Found 1 subgrps that may have base of length > 8
GAP's base command finds bases of length:
[ 9 ]
Greedy base alg finds bases of length:
[ 9 ]

Considered grp of size 12128668876800 with 10 gens:
Found 13 maximal subgroups (up to conj)
Considered 7 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 8
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[ <permutation group of size 12128668876800 with 10 generators> ]
```

Below is output for $d = 9$:

```
gap> res9 := GetSubgrpAGLBase(9);
Considered grp of size 358201502736997192984166400 with 3 gens:
Found 13 maximal subgroups (up to conj)
Considered 5 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 9
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[  ]
```

Below is output for $d = 10$:

```
gap> res10 := GetSubgrpAGLBase(10);
Considered grp of size 375234700595146883504949480652800 with 3 gens:
Found 17 maximal subgroups (up to conj)
Considered 8 maximal subgrps (up to conj)
Found 1 subgrps that may have base of length > 10
GAP's base command finds bases of length:
[ 11 ]
Greedy base alg finds bases of length:
[ 11 ]

Considered grp of size 25410822678459187200 with 12 gens:
Found 12 maximal subgroups (up to conj)
Considered 4 maximal subgrps (up to conj)
Found 0 subgrps that may have base of length > 10
GAP's base command finds bases of length:
[  ]
Greedy base alg finds bases of length:
[  ]
[ <permutation group of size 25410822678459187200 with 12 generators> ]
```

For even d, we may check that order is correct for $2^d : \mathrm{Sp}_d(2)$, by verifying that the groups identified have order equal to `2^d * Order( GeneralOrthogonalGroup( d + 1, 2 ) )` using the isomorphism $\mathrm{Sp}_d(2) \cong \mathrm{GO}_{d+1}(2)$; this is the case in every scenario.