Algorithms for Permutation Groups

Jonathan Conder

Department of Mathematics
The University of Auckland

Supervisor: Eamonn O'Brien

A dissertation submitted in partial fulfillment of the requirements for the degree of BSc(Hons) in Mathematics, The University of Auckland, 2012.

Abstract

We present two randomised algorithms to recognise the alternating or symmetric groups of a given degree. The first takes as input a permutation group G acting on some finite set Ω and determines whether $\mathrm{Alt}\,(\Omega) \leq G$. The second takes a black-box group G and an integer $n \geq 5$, and reports whether $G \simeq A_n$ or $G \simeq S_n$. If an isomorphism is found, the second algorithm returns functions which can be used to compute it in either direction.

We discuss important concepts from the theory of permutation groups, and prove several related results. To estimate probabilities for the success of each algorithm, we also present several results which are statistical in nature.

Contents

Chapter 1

Introduction

1.1 Motivation

A central tool in computational group theory is the Schreier-Sims algorithm for computing a strong generating set for a permutation group G [1, Chapter 4]. It takes as input a base for G, that is, a list of points in the permutation domain such that no element of G except the identity fixes them all. Among other applications, the resulting information can be used to compute the order of G, and it simplifies the task of deciding whether a given permutation is a member of G [1, p. 79]. This approach is particularly efficient if G has a small base relative to its degree. Many interesting groups have this property [1, p. 59], but there are important exceptions, such as the alternating and symmetric groups. Indeed, a base for the symmetric group can exclude only one point of the permutation domain; bases for the alternating group can omit at most two. As such, the Schreier-Sims algorithm performs badly for these groups. However, if G is known to be one of these groups, it is trivial to compute $|G|$ or determine whether some permutation lies in G. So it would be useful if we could identify these groups and handle them separately.

We present randomised algorithms to determine whether a given finite group is isomorphic to the symmetric or alternating group of a given degree. The first only answers this question for permutation representations of the given degree; the second works for every representation in which products, inverses and equality can be computed. In addition, the second algorithm produces an isomorphism between the input group and the corresponding permutation group, and these isomorphisms are constructive and realised efficiently.

1.2 Permutation groups

We use $\mathbb{N}$ to denote the natural numbers, including 0, and $\mathbb{P}$ for the positive integers. For each $n \in \mathbb{P}$ we write $\mathbb{N}_n$ for the set $\{0, 1, \ldots, n-1\}$, and $\mathbb{P}_n$ for $\{1, 2, \ldots, n\}$.

Definition 1.2.1. If $\Omega \neq \varnothing$, then $\mathrm{Sym}\,(\Omega) = \{f : \Omega \to \Omega \mid f \text{ is bijective}\}$ forms a group under the operation $\circ$ (function composition). It is the *symmetric group* on Ω. The symmetric group of *degree* n, written S_n, is $\mathrm{Sym}\,(\mathbb{P}_n)$.

In what follows we assume that Ω is an arbitrary non-empty set. The symbol $\circ$ will usually be omitted, and functions will act from the right rather than the left. For example, given $\omega \in \Omega$ and $g, h \in \mathrm{Sym}\,(\Omega)$ we write $\omega^{gh} = (\omega^g)^h$ to represent the application of g, followed by h, to ω. We use Δ^g to denote the image of some $\Delta \subseteq \Omega$ under g. The notation $\prod_{i=1}^{n} g_i = g_1 g_2 \ldots g_n$ represents the product of several elements $g_1, g_2, \ldots, g_n \in \mathrm{Sym}\,(\Omega)$. We adopt the convention that $\prod_{i=1}^{0} g_i = 1$, where $1 = 1_\Omega$ is the identity function. In other contexts 1 may also represent the trivial group $\{1_\Omega\}$.

Definition 1.2.2. A subgroup of a symmetric group is a *permutation group.*

Theorem 1.2.3 (Cayley)**.** Every group is isomorphic to some permutation group.

Proof. Let G be a group. For each $g \in G$ define the function $\theta_g : G \to G$ by $h^{\theta_g} = hg$ for all $h \in G$. It follows from the existence of g^{-1} that θ_g is a bijection, and hence $\theta_g \in \mathrm{Sym}\,(G)$. Now define the function $\phi : G \to \mathrm{Sym}\,(G)$ by $g^\phi = \theta_g$ for all $g \in G$. It is straightforward to check that ϕ is a group homomorphism. Indeed, $\theta_g \circ \theta_h = \theta_{gh}$ for all $g, h \in G$. This implies that $G^\phi \leq \mathrm{Sym}\,(G)$ is a permutation group. It remains to show that $G \simeq G^\phi$, which is straightforward because ϕ is an isomorphism from $G \to G^\phi$. Indeed, ϕ is onto its image G^ϕ, and is injective because if $\theta_g = \theta_h$ for some $g, h \in G$ then $g = 1^{\theta_g} = 1^{\theta_h} = h$. □

Definition 1.2.4. Let $g \in \mathrm{Sym}\,(\Omega)$. The set of *fixed points* of g is $\mathrm{fix}\,(g) = \{\omega \in \Omega \mid \omega^g = \omega\}$, and the *support* of g is $\mathrm{supp}\,(g) = \Omega \setminus \mathrm{fix}\,(g)$.

Definition 1.2.5. Let $n \in \mathbb{P} \setminus \{1\}$ and $\omega_0, \omega_1, \ldots, \omega_{n-1} \in \Omega$ be pairwise distinct. We denote by $(\omega_0 \ \omega_1 \ \ldots \ \omega_{n-1})$ the permutation $g \in \operatorname{Sym}(\Omega)$ defined by $\omega_i^g = \omega_{(i+1) \bmod n}$ for all $i \in \mathbb{N}_n$, and $\omega^g = \omega$ for all remaining $\omega \in \Omega$. This function is a *cycle* of length n, or an *n-cycle*, and its support is $\{\omega_0, \omega_1, \ldots, \omega_{n-1}\}$. Two cycles $g, h \in \operatorname{Sym}(\Omega)$ are *disjoint* if $\operatorname{supp}(g) \cap \operatorname{supp}(h) = \varnothing$.

1.3 Examples of permutation groups

The definitions in this section, and the proofs of Lemmas 1.3.6 and 1.3.8, are inspired by [2].

Definition 1.3.1. Let $G \leq \operatorname{Sym}(\Omega)$. For each $\omega \in \Omega$, the set $G_\omega = \{g \in G \mid \omega^g = g\}$ is the *stabiliser* of ω in G. Given $\Delta \subseteq \Omega$, the *restriction* of G to Δ is $G|_\Delta = \bigcap_{\omega \in \Omega \setminus \Delta} G_\omega$. The *setwise stabiliser* of Δ in G is $G_\Delta = \{g \in G \mid \Delta^g = \Delta\}$.

Lemma 1.3.2. If $G \leq \operatorname{Sym}(\Omega)$, $\omega \in \Omega$ and $\Delta \subseteq \Omega$, then $G_\omega, G|_\Delta, G_\Delta \leq G$.

Proof. Clearly $1 \in G_\omega$. Also $\omega \in \operatorname{fix}(g) \cap \operatorname{fix}(h) = \operatorname{fix}(g^{-1}) \cap \operatorname{fix}(h) \subseteq \operatorname{fix}(g^{-1}h)$, and hence $g^{-1}h \in G_\omega$, for all $g, h \in G_\omega$. Therefore $G_\omega \leq G$.
Hence $G|_\Delta = \bigcap_{\delta \in \Omega \setminus \Delta} G_\delta \leq G$, as the set of subgroups of G is closed under intersection. Clearly $1 \in G_\Delta$. Let $g, h \in G_\Delta$. Then $\Delta^g = \Delta$, so that $\Delta^{g^{-1}} = \Delta^{gg^{-1}} = \Delta$ and hence $\Delta^{g^{-1}h} = \Delta^h = \Delta$. Therefore $g^{-1}h \in G_\Delta$, so $G_\Delta \leq G$. □

Definition 1.3.3. Let $G \leq \operatorname{Sym}(\Omega)$ and $\omega \in \Omega$. The *orbit* of ω under G is $\omega^G = \{\omega^g \mid g \in G\}$.

Definition 1.3.4. The *finitary symmetric group* on Ω is the set of elements of $\operatorname{Sym}(\Omega)$ with finite support. It is written $\operatorname{FSym}(\Omega) = \{f \in \operatorname{Sym}(\Omega) \mid \operatorname{supp}(f) \text{ is finite}\}$.

Lemma 1.3.5. The finitary symmetric group on Ω is a normal subgroup of $\operatorname{Sym}(\Omega)$.

Proof. Clearly $\operatorname{supp}(1) = \varnothing$ is finite, so $1 \in \operatorname{FSym}(\Omega)$. Now let $g, h \in \operatorname{FSym}(\Omega)$. Since $\operatorname{fix}(g) \cap \operatorname{fix}(h) \subseteq \operatorname{fix}(g^{-1}h)$, by definition $\operatorname{supp}(g^{-1}h) \subseteq \operatorname{supp}(g) \cup \operatorname{supp}(h)$, which is finite. Therefore $g^{-1}h \in \operatorname{FSym}(\Omega)$, which shows that $\operatorname{FSym}(\Omega) \leq \operatorname{Sym}(\Omega)$.
Let $x \in \operatorname{Sym}(\Omega)$ and $\omega \in \Omega$. Then g fixes ω if and only if $x^{-1}gx$ fixes ω^x. This implies that $\operatorname{supp}(x^{-1}gx) = \operatorname{supp}(g)^x$, which has the same cardinality as $\operatorname{supp}(g)$ since x is a bijection. Hence $x^{-1}gx \in \operatorname{FSym}(\Omega)$, which shows that $\operatorname{FSym}(\Omega) \trianglelefteq \operatorname{Sym}(\Omega)$. □

Lemma 1.3.6. Each $g \in \mathrm{FSym}(\Omega)$ is the product of a unique set of pairwise disjoint cycles.

Proof. Suppose to the contrary that some $g \in \mathrm{FSym}(\Omega)$ cannot be uniquely expressed as the product of a set of pairwise disjoint cycles, and choose g with $|\mathrm{supp}(g)|$ minimal. Then $g \neq 1$, as 1 is the product of zero cycles, and every other product of pairwise disjoint cycles has non-empty support. Therefore $\mathrm{supp}(g) \neq \varnothing$, and there exists $\omega \in \mathrm{supp}(g)$. Note that $\mathrm{supp}\left(g^i\right) \subseteq \mathrm{supp}(g)$ for all $i \in \mathbb{Z}$, so $\omega^{\langle g \rangle} \subseteq \mathrm{supp}(g)$ is finite. Hence there exist distinct $i, j \in \mathbb{Z}$ such that $\omega^{g^i} = \omega^{g^j}$. Choose i and j with $n := j - i \in \mathbb{P}$ minimal. Then $n \geq 2$, since $\omega = \omega^{g^j g^{-i}} = \omega^{g^n}$ and $\omega \notin \mathrm{fix}(g)$. Moreover $\omega, \omega^g, \ldots, \omega^{g^{n-1}}$ are pairwise distinct, which means $x := \left(\omega \; \omega^g \; \ldots \; \omega^{g^{n-1}}\right)$ is an n-cycle. Clearly g maps $\omega^{g^i} \mapsto \omega^{g^{(i+1) \bmod n}}$ for all $i \in \mathbb{N}_n$, so $h := x^{-1} g$ has support $\mathrm{supp}(g) \setminus \omega^{\langle g \rangle}$, and hence it can be uniquely expressed as the product of a set $X \subseteq \mathrm{FSym}(\Omega)$ of pairwise disjoint cycles, each of which fix $\omega^{\langle g \rangle}$ pointwise. Therefore $X \cup \{x\}$ is a set of pairwise disjoint cycles whose product is $hx = xh = g$.

This implies that g is the product of a different set $Y \subseteq \mathrm{FSym}(\Omega)$ of pairwise disjoint cycles. There is exactly one $y \in Y$ such that $\omega \in \mathrm{supp}(y)$. Since y is disjoint from the other cycles in Y, it maps $\omega \mapsto \omega^g$. Hence $\omega^g \notin \mathrm{fix}(y)$, and it follows by a straightforward induction argument that y maps $\omega^{g^i} \mapsto \omega^{g^{(i+1) \bmod n}}$ for all $i \in \mathbb{N}_n$. The remaining elements of Ω are fixed by y, since y is a cycle. Therefore $y = x$, so h is the product of the cycles in $Y \setminus \{y\}$, and hence $Y \setminus \{y\} = X$. This is a contradiction because $Y \neq X \cup \{x\}$. □

Definition 1.3.7. Let $g \in \mathrm{FSym}(\Omega)$. The *cycle structure* of g is the unique set $X \subseteq \mathrm{FSym}(\Omega)$ of pairwise disjoint cycles such that g is the product of the cycles in X. If $x \in X$ then g *contains* the cycle x. Moreover, if $m = |\mathrm{supp}(g)|$ and $n = |X|$, then the *parity* of g is $\pi(g) = (m - n) \bmod 2$. An *even* permutation is one with parity 0, and an *odd* permutation is one with parity 1.

Lemma 1.3.8. Let $g \in \mathrm{FSym}(\Omega)$. Then g can be expressed as a product of 2-cycles. If g can be written as the product of n 2-cycles, then $n \equiv \pi(g) \bmod 2$.

Proof. By Lemma 1.3.6, it suffices to show that every cycle can be expressed as a product of 2-cycles. To this end, let $n \in \mathbb{P}$ and $\omega_0, \omega_1, \ldots, \omega_n \in \Omega$ be pairwise distinct. Then

$$(\omega_0 \; \omega_1 \; \cdots \; \omega_n) = (\omega_0 \; \omega_1)(\omega_0 \; \omega_2) \ldots (\omega_0 \; \omega_n).$$

Now let $h, x \in \operatorname{FSym}(\Omega)$ such that x is a 2-cycle. Then h is the product of a unique set $X \subseteq \operatorname{FSym}(\Omega)$ of pairwise disjoint cycles, while $x = (\alpha\ \beta)$ for some distinct $\alpha, \beta \in \Omega$. If $\operatorname{supp}(h) \cap \{\alpha, \beta\} = \varnothing$, then $X \cup \{x\}$ is a set of pairwise disjoint cycles whose product is hx, so $\pi(hx) \equiv \pi(h) + 1 \bmod 2$. Otherwise, suppose that $\operatorname{supp}(h) \cap \{\alpha, \beta\} = \{\alpha, \beta\}$. Then there exist cycles $x_1, x_2 \in X$ such that $\alpha \in \operatorname{supp}(x_1)$ and $\beta \in \operatorname{supp}(x_2)$. Suppose that $x_1 \neq x_2$. Write $x_1 = (\alpha\ \omega_1\ \cdots\ \omega_m)$ and $x_2 = (\beta\ \sigma_1\ \cdots\ \sigma_n)$ for some $m, n \in \mathbb{P}$ and $\omega_1, \omega_2, \ldots, \omega_m, \sigma_1, \sigma_2, \ldots, \sigma_n \in \Omega$. It follows that

$$x_1 x_2 x = (\alpha\ \omega_1\ \cdots\ \omega_m)(\beta\ \sigma_1\ \cdots\ \sigma_n)(\alpha\ \beta) = (\alpha\ \omega_1\ \cdots\ \omega_m\ \beta\ \sigma_1\ \cdots\ \sigma_n),$$

and hence $\pi(hx) \equiv \pi(h) + 1 \bmod 2$. Otherwise $x_1 = x_2$, and there exist $m, n \in \mathbb{N}$ and $\omega_1, \omega_2, \ldots, \omega_m, \sigma_1, \sigma_2, \ldots, \sigma_n \in \Omega$ such that $x_1 = (\alpha\ \omega_1\ \cdots\ \omega_m\ \beta\ \sigma_1\ \cdots\ \sigma_n)$. Hence

$$x_1 x = (\alpha\ \omega_1\ \cdots\ \omega_m\ \beta\ \sigma_1\ \cdots\ \sigma_n)(\alpha\ \beta) = (\alpha\ \omega_1\ \cdots\ \omega_m)(\beta\ \sigma_1\ \cdots\ \sigma_n),$$

so $\pi(hx) \equiv \pi(h) - 1 \equiv \pi(h) + 1 \bmod 2$. For the remaining case, $|\operatorname{supp}(h) \cap \{\alpha, \beta\}| = 1$. Without loss of generality assume that $\operatorname{supp}(h) \cap \{\alpha, \beta\} = \{\alpha\}$. Then there exists $x_1 \in X$ such that $\alpha \in \operatorname{supp}(x_1)$ (whereas $\beta \in \operatorname{fix}(x_1)$). Write $x_1 = (\alpha\ \omega_1\ \cdots\ \omega_m)$ for some $m \in \mathbb{P}$ and $\omega_1, \omega_2, \ldots, \omega_m \in \Omega$. It follows that $\pi(hx) \equiv \pi(h) + 1 \bmod 2$, since

$$x_1 x = (\alpha\ \omega_1\ \cdots\ \omega_m)(\alpha\ \beta) = (\alpha\ \omega_1\ \cdots\ \omega_m\ \beta).$$

In summary, $\pi(hx) \equiv \pi(h) + 1 \bmod 2$ for all $h, x \in \operatorname{FSym}(\Omega)$ such that x is a 2-cycle. Now let $n \in \mathbb{N}$ and $x_1, x_2, \ldots, x_n \in \operatorname{FSym}(\Omega)$ be 2-cycles such that $g = \prod_{i=1}^{n} x_i$. Then

$$\pi(g) \equiv \pi(gx_n) - 1 \equiv \cdots \equiv \pi\left(g \prod_{i=0}^{n-1} x_{n-i}\right) - n \equiv \pi(1) - n \equiv n \bmod 2,$$

as required. □

Definition 1.3.9. The *alternating group* on Ω is $\operatorname{Alt}(\Omega) = \{g \in \operatorname{FSym}(\Omega) \mid g \text{ is even}\}$, and the alternating group of *degree* n, written A_n, is $\operatorname{Alt}(\mathbb{P}_n)$.

Lemma 1.3.10. The alternating group on Ω is a normal subgroup of $\operatorname{Sym}(\Omega)$, and hence $\operatorname{FSym}(\Omega)$. Moreover, if $|\Omega| \geq 2$ then $|\operatorname{FSym}(\Omega) : \operatorname{Alt}(\Omega)| = 2$.

Proof. Clearly $1 \in \operatorname{Alt}(\Omega)$, as $\pi(1) = 0$. Let $g, h \in \operatorname{Alt}(\Omega)$. By Lemma 1.3.8, $g = \prod_{i=1}^{m} x_i$ and $h = \prod_{i=1}^{n} y_i$ for some $m, n \in \mathbb{N}$ and 2-cycles $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n \in$

$\mathrm{FSym}\,(\Omega)$ such that $m \equiv n \equiv 0 \bmod 2$. It follows that $g^{-1}h = \prod_{i=0}^{m-1} x_{m-i} \prod_{i=1}^{n} y_i$ is even, and hence $g^{-1}h \in \mathrm{Alt}\,(\Omega)$. This shows that $\mathrm{Alt}\,(\Omega) \leq \mathrm{FSym}\,(\Omega) \leq \mathrm{Sym}\,(\Omega)$.

Let $x \in \mathrm{Sym}\,(\Omega)$. Then $x^{-1}gx = \prod_{i=1}^{m} x^{-1}x_i x$ is an even permutation, since $x^{-1}x_i x$ is a 2-cycle with support $\mathrm{supp}\,(x_i)^x$, for all $i \in \mathbb{P}_m$. Therefore $x^{-1}gx \in \mathrm{Alt}\,(\Omega)$, and hence $\mathrm{Alt}\,(\Omega) \trianglelefteq \mathrm{Sym}\,(\Omega)$. This implies that $\mathrm{Alt}\,(\Omega) \trianglelefteq \mathrm{FSym}\,(\Omega)$.

Suppose that $|\Omega| \geq 2$. Then there exists a 2-cycle $y \in \mathrm{FSym}\,(\Omega)$, and $g \mapsto gy$ is a bijection between $\mathrm{Alt}\,(\Omega)$ and $\mathrm{FSym}\,(\Omega) \setminus \mathrm{Alt}\,(\Omega)$. Therefore $|\mathrm{FSym}\,(\Omega) : \mathrm{Alt}\,(\Omega)| = 2$. □

Chapter 2

Identifying permutation groups

2.1 Motivation

The aim of this chapter is to present an algorithm which, given a permutation group G acting on some finite set Ω, determines whether G is $\mathrm{Alt}\,(\Omega)$ or $\mathrm{Sym}\,(\Omega)$. It is a one-sided Monte Carlo algorithm, which means that it may (with a user-specified probability) incorrectly report that G is not $\mathrm{Alt}\,(\Omega)$ or $\mathrm{Sym}\,(\Omega)$. However, it only reports that G is $\mathrm{Alt}\,(\Omega)$ or $\mathrm{Sym}\,(\Omega)$ if this is true. The first step towards this is to identify some properties of permutation groups (transitivity and primitivity) which the alternating and symmetric groups possess, and can be decided efficiently by a computer. If the input group has one of these properties, it is not difficult to determine (using a one-sided Monte Carlo algorithm) whether it contains $\mathrm{Alt}\,(\Omega)$. Otherwise, the algorithm can report with certainty that G is not $\mathrm{Alt}\,(\Omega)$ or $\mathrm{Sym}\,(\Omega)$. The final algorithm is described in [1, pp. 226-7], but many of the preliminary results, namely Theorems 2.3.1 and 2.3.9, Corollary 2.3.2 and Lemma 2.3.6, are taken from [2].

2.2 Primitive permutation groups

Definition 2.2.1. Let $G \leq \mathrm{Sym}\,(\Omega)$ and $\Sigma \subseteq \Omega$ be non-empty. Then G *acts* on Σ if $G|_{\Sigma} = G$. Suppose that G acts on Σ, and let $\Delta \subseteq \Sigma$. Then Δ is a *block* for G in Σ if Δ^g is either equal to or disjoint from Δ for all $g \in G$.

Example 2.2.2. Let $G \leq \operatorname{Sym}(\Omega)$ act on some $\Sigma \subseteq \Omega$. Then $\varnothing$, Σ and all singleton subsets of Σ are blocks for G in Σ. These are the *trivial* blocks for G.

Example 2.2.3. Let $G \leq \operatorname{Sym}(\mathbb{Z})$ be the group of permutations corresponding to addition in $\mathbb{Z}$ (this is the image $\mathbb{Z}^{\phi}$ from Theorem 1.2.3). Also let $n \in \mathbb{Z}$. Then $n\mathbb{Z}$ is a block for G in $\mathbb{Z}$. It is also a non-trivial block provided that $n \notin \{-1, 0, 1\}$.

Definition 2.2.4. Let $G \leq \operatorname{Sym}(\Omega)$ act on some $\Sigma \subseteq \Omega$. Then G acts *transitively* on Σ if for each pair $\alpha, \beta \in \Sigma$ there exists $g \in G$ such that $\alpha^g = \beta$ (equivalently, if $\sigma^G = \Sigma$ for all $\sigma \in \Sigma$). If, in addition, there are no non-trivial blocks for G in Σ, then G acts *primitively* on Σ. Moreover, if G acts transitively (primitively) on Ω, it is *transitive* (*primitive*).

Lemma 2.2.5. If $|\Omega| \neq 2$ then $\operatorname{Sym}(\Omega)$, $\operatorname{FSym}(\Omega)$ and $\operatorname{Alt}(\Omega)$ are primitive. Moreover, $\operatorname{Sym}(\Omega)$ and $\operatorname{FSym}(\Omega)$ are primitive even if $|\Omega| = 2$.

Proof. If $|\Omega| = 1$ then $\operatorname{Sym}(\Omega) = \operatorname{FSym}(\Omega) = \operatorname{Alt}(\Omega) = 1$ is clearly transitive. Suppose that $|\Omega| = 2$, and write $\Omega = \{\alpha, \beta\}$. Then $(\alpha\ \beta) \in \operatorname{FSym}(\Omega)$, so $\operatorname{Sym}(\Omega) = \operatorname{FSym}(\Omega)$ is transitive. Otherwise $|\Omega| > 2$. Let $\alpha, \beta \in \Omega$ be distinct. Then there is a third distinct $\gamma \in \Omega$, and $(\alpha\ \beta\ \gamma) = (\alpha\ \gamma)(\beta\ \gamma) \in \operatorname{Alt}(\Omega) \leq \operatorname{FSym}(\Omega) \leq \operatorname{Sym}(\Omega)$ maps $\alpha \mapsto \beta$. Therefore $\operatorname{Sym}(\Omega)$, $\operatorname{FSym}(\Omega)$ and $\operatorname{Alt}(\Omega)$ are transitive.
Now let $\Delta \subset \Omega$ with $|\Delta| \geq 2$. Then there exist distinct $\alpha, \beta \in \Delta$ and $\gamma \in \Omega \setminus \Delta$. It follows that $g := (\alpha\ \beta\ \gamma) \in \operatorname{Alt}(\Omega) \leq \operatorname{FSym}(\Omega) \leq \operatorname{Sym}(\Omega)$. But $\beta \in \Delta^g \cap \Delta$ and $\gamma \in \Delta^g \setminus \Delta$, which means Δ is not a block for $\operatorname{Sym}(\Omega)$, $\operatorname{FSym}(\Omega)$ or $\operatorname{Alt}(\Omega)$ in Ω. Therefore each group has no non-trivial blocks, so each is primitive except for $\operatorname{Alt}(\Omega)$ when $|\Omega| = 2$. □

We observe in Lemma 2.2.7 that A_2 is actually the only imprimitive permutation group with no non-trivial blocks.

Lemma 2.2.6. Let $G \leq \operatorname{Sym}(\Omega)$ act on some $\Sigma \subseteq \Omega$. Also let $\Delta \subseteq \Sigma$, and suppose that Δ is not a block for G in Σ. Then there exists $g \in G$ such that $\Delta^g \setminus \Delta \neq \varnothing \neq \Delta^g \cap \Delta$.

Proof. Since Δ is not a block for G in Σ, there exists $g \in G$ such that $\Delta^g \cap \Delta \neq \varnothing$ and $\Delta^g \neq \Delta$. If $\Delta^g \setminus \Delta \neq \varnothing$ then we are done. Otherwise $\Delta^g \subseteq \Delta$, so it cannot be the case that $\Delta \subseteq \Delta^g$. Hence there exists $\delta \in \Delta \setminus \Delta^g$. It follows that $\delta^{g^{-1}} \in \Delta^{g^{-1}} \setminus \Delta$, because if $\delta^{g^{-1}} \in \Delta$ then $\delta = \delta^{g^{-1}g} \in \Delta^g$. Moreover, there exists $\omega \in \Delta^g \cap \Delta$, which implies that $\omega^{g^{-1}} \in \Delta^{gg^{-1}} \cap \Delta^{g^{-1}} = \Delta^{g^{-1}} \cap \Delta$. Hence $\Delta^{g^{-1}} \setminus \Delta \neq \varnothing$ and $\Delta^{g^{-1}} \cap \Delta \neq \varnothing$, as required. □

Lemma 2.2.7. Let $G \leq \mathrm{Sym}\,(\Omega)$ act on some $\Sigma \subseteq \Omega$. Suppose that $|\Sigma| \geq 3$, and there are no non-trivial blocks for G in Σ. Then G acts primitively on Σ.

Proof. Suppose that G does not act transitively on Σ. Then there exists $\sigma \in \Sigma$ such that $\sigma^G \neq \Sigma$. Clearly $\sigma \in \sigma^G \neq \varnothing$. Suppose that $\left|\sigma^G\right| = 1$. Then $\Delta \coloneqq \Sigma \setminus \sigma^G \subset \Sigma$ is not a block for G in Σ, since $|\Delta| = |\Sigma| - 1 \geq 2$. By Lemma 2.2.6 there exists $g \in G$ such that $\Delta^g \setminus \Delta \neq \varnothing$. Since $\Delta^g \setminus \Delta \subseteq \Sigma \setminus \Delta = \sigma^G = \{\sigma\}$, it follows that $\sigma \in \Delta^g$. This leads to the contradiction $\sigma^{g^{-1}} \in \Delta = \Sigma \setminus \sigma^G$. Otherwise $\left|\sigma^G\right| \geq 2$, so σ^G is not a block for G in Σ. By Lemma 2.2.6, there exists $g \in G$ such that $\left(\sigma^G\right)^g \setminus \sigma^G \neq \varnothing$. Choose $\omega \in \left(\sigma^G\right)^g \setminus \sigma^G$. Then $\omega = \alpha^g$ for some $\alpha \in \sigma^G$. Furthermore, $\alpha = \sigma^h$ for some $h \in G$. But this implies that $\omega = \left(\sigma^h\right)^g = \sigma^{hg}$, which contradicts $\omega \notin \sigma^G$. Therefore G acts transitively on Σ, and since there are no non-trivial blocks for G in Σ it follows that G acts primitively on Σ. □

2.3 Identifying Alt (Ω) or Sym (Ω)

The following theorem is due to Jordan [3], and the proof we present can be found in [2, p. 77]. A few gaps have been filled for the case where Ω is infinite, which requires Lemma 2.2.6 and Zorn's Lemma. It can be used to identify a permutation group, by checking if it is primitive and searching for a 3-cycle. This is not the approach we adopt, but our algorithm relies on Jordan's result.

Theorem 2.3.1. Let $G \leq \mathrm{Sym}\,(\Omega)$ be primitive, and suppose it contains a 3-cycle x. Then $\mathrm{Alt}(\Omega) \leq G$.

Proof. For each $\Delta \subseteq \Omega$ let $A_\Delta = \mathrm{Alt}\,(\Omega)|_\Delta = \{g \in \mathrm{Alt}\,(\Omega) \mid \mathrm{supp}\,(g) \subseteq \Delta\}$. We note that A_Δ is a subgroup of $\mathrm{Alt}\,(\Omega)$ isomorphic to $\mathrm{Alt}\,(\Delta)$, although this fact will not be required for the proof. Let $\mathcal{W} = \{\Delta \subseteq \Omega \mid \mathrm{supp}\,(x) \subseteq \Delta \text{ and } A_\Delta \subseteq G\}$ be partially ordered by set inclusion. The only even permutations with support contained in $\mathrm{supp}\,(x)$ are 1, x and x^{-1}, so $A_{\mathrm{supp}(x)} = \left\{1, x, x^{-1}\right\} \subseteq G$ and hence $\mathrm{supp}\,(x) \in \mathcal{W}$. In particular $\mathcal{W} \neq \varnothing$. Let $\mathcal{D} \subseteq \mathcal{W}$ be a non-empty chain, and let $g \in A_{\bigcup \mathcal{D}}$. Then $\mathrm{supp}\,(g) \subseteq \bigcup \mathcal{D}$ is finite, so $\mathrm{supp}\,(g) \subseteq \Delta$ for some $\Delta \in \mathcal{D}$. It follows that $g \in A_\Delta \subseteq G$, which implies that

$A_{\bigcup \mathcal{D}} \subseteq G$. Therefore $\bigcup \mathcal{D} \in \mathcal{W}$ is an upper bound for $\mathcal{D}$. By Zorn's lemma it follows that there is a maximal element $\Delta \in \mathcal{W}$.[1]
Suppose for a contradiction that $\Delta \neq \Omega$. Since G is primitive and $|\Delta| \geq |\mathrm{supp}\,(x)| = 3$, it follows that Δ is not a block for G in Ω. By Lemma 2.2.6, there exists $g \in G$ such that $\Delta^g \setminus \Delta \neq \varnothing$ and $\Delta^g \cap \Delta \neq \varnothing$. Therefore there exist $\alpha \in \Delta^g \setminus \Delta$ and $\beta \in \Delta^g \cap \Delta$. Suppose that $|\Delta^g \cap \Delta| > 1$. Then there exists $\gamma \in \Delta^g \cap \Delta$ distinct from α and β. These are all elements of Δ^g, so $\alpha = \tau^g$, $\beta = \mu^g$ and $\gamma = \nu^g$ for some distinct $\tau, \mu, \nu \in \Delta$. It follows that $(\alpha\ \beta\ \gamma) = g^{-1} (\tau\ \mu\ \nu)\, g \in G$, since $(\tau\ \mu\ \nu) \in A_\Delta \subseteq G$. Otherwise $|\Delta^g \cap \Delta| = 1$, and hence $\Delta^g \cap \Delta = \{\beta\}$. Since $|\Delta| \geq 3$ we can choose a 3-cycle $(\beta\ \gamma\ \delta) \in A_\Delta \subseteq G$. Also choose $\varepsilon \in \Delta^g$ distinct from α and β, which will not be γ or δ since $\gamma, \delta \in \Delta$. Then $\alpha = \tau^g$, $\beta = \mu^g$ and $\varepsilon = \nu^g$ for some distinct $\tau, \mu, \nu \in \Delta$. It follows that $(\alpha\ \beta\ \varepsilon) = g^{-1} (\tau\ \mu\ \nu)\, g \in G$, since $(\tau\ \mu\ \nu) \in A_\Delta \subseteq G$. Therefore

$$(\alpha\ \beta\ \gamma) = (\alpha\ \beta\ \varepsilon)\,(\delta\ \gamma\ \beta)\,(\varepsilon\ \beta\ \alpha)\,(\beta\ \gamma\ \delta) = \left[(\alpha\ \beta\ \varepsilon)^{-1}, (\beta\ \gamma\ \delta)\right] \in G.$$

In either case, there exists a $\gamma \in \Delta$ such that $(\alpha\ \beta\ \gamma) \in G$. Let $\Gamma = \Delta \cup \{\alpha\} \supset \Delta$, so that $\Gamma \notin \mathcal{W}$. This implies that $A_\Gamma \nsubseteq G$, so there exists $y \in \mathrm{Alt}\,(\Omega) \setminus G$ such that $\mathrm{supp}\,(y) \subseteq \Gamma$. Clearly $\alpha^y \neq \alpha$, since otherwise $y \in A_\Delta \subseteq G$. In fact $\alpha^y \in \Delta$, since if $\alpha^y \notin \Gamma$ then it is a fixed point of y, so that $\alpha^{yy} = \alpha^y$ and y is not injective. Now let $z \in A_\Delta$ map $\alpha^y \mapsto \gamma$ (take $z = 1$ if $\alpha^y = \gamma$, or else $z = (\alpha^y\ \gamma\ \varepsilon)$ for some $\varepsilon \in \Delta \setminus \{\alpha^y, \gamma\}$). Then $yz\,(\alpha\ \beta\ \gamma) \in \mathrm{Alt}\,(\Omega)$ fixes α and elements of $\Omega \setminus \Gamma$, which means it lies in $A_\Delta \subseteq G$. Since $z\,(\alpha\ \beta\ \gamma) \in G$ as well, it follows that $y \in G$, which is a contradiction. Therefore $\Delta = \Omega$, which implies that $\mathrm{Alt}\,(\Omega) = A_\Omega \subseteq G$. □

Corollary 2.3.2. Let $G \leq \mathrm{Sym}\,(\Omega)$ be primitive, and suppose it contains a 2-cycle $x = (\alpha\ \beta)$. Then $\mathrm{FSym}\,(\Omega) \leq G$.

Proof. If $|\Omega| \leq 2$ then $G = \langle x \rangle = \mathrm{Sym}\,(\Omega)$. Otherwise $|\Omega| \geq 3$, so that $\mathrm{supp}\,(x) = \{\alpha, \beta\}$ is not a block for G in Ω. Therefore $\{\alpha, \beta\}^g \cap \{\alpha, \beta\} \neq \varnothing$ and $\{\alpha, \beta\}^g \neq \{\alpha, \beta\}$ for some $g \in G$. Without loss of generality take $\{\alpha, \beta\}^g = \{\alpha, \gamma\}$ for some $\gamma \in \Omega$ distinct from α and β. Then either $\alpha^g = \alpha$ and $\beta^g = \gamma$, or $\alpha^g = \gamma$ and $\beta^g = \alpha$. In both cases it follows

[1] This relies on the axiom of choice, which is not required when Ω is finite. To show this, suppose $\mathcal{W}$ has no maximal element. Then each member of $\mathcal{W}$ is properly contained within another one, so we can find an infinite strictly increasing sequence $\mathrm{supp}\,(x) = \Delta_0 \subset \Delta_1 \subset \cdots$ of members of $\mathcal{W}$. But then $\left|\Delta_{|\Omega|}\right| > |\Omega|$, which contradicts $\Delta_{|\Omega|} \subseteq \Omega$.

that

$$(\alpha\ \beta\ \gamma) = (\beta\ \alpha)\, g^{-1}\, (\alpha\ \beta)\, g = [x, g] \in G.$$

Therefore $\mathrm{Alt}\,(\Omega) \leq G$ by Theorem 2.3.1. Since $\mathrm{Alt}\,(\Omega) < \langle (\alpha\ \beta)\,, \mathrm{Alt}\,(\Omega)\rangle \leq \mathrm{FSym}\,(\Omega)\,,$ it follows from Lemma 1.3.10 that $\mathrm{FSym}\,(\Omega) = \langle (\alpha\ \beta)\,, \mathrm{Alt}\,(\Omega)\rangle \leq G.$ □

We aim to generalise this result to a larger class of cycles of prime length, for the case where Ω is finite. To do so, we require several preliminary results.

Lemma 2.3.3. Let $G \leq \mathrm{Sym}\,(\Omega)$ act on some $\Sigma \subseteq \Omega$. Suppose that $p \coloneqq |\Sigma|$ is prime, and there is a p-cycle $x \in G$. Then G acts primitively on Σ.

Proof. Clearly $\mathrm{supp}\,(x) = \Sigma$, so G acts transitively on Σ. Enumerate Σ as $\sigma_0, \sigma_1, \ldots, \sigma_{p-1}$ in such a way that $x = (\sigma_0\ \sigma_1\ \ldots\ \sigma_{p-1})\,$. Let $\Delta \subset \Sigma$ with $|\Delta| \geq 2$. Then there exist distinct $i, j \in \mathbb{N}_p$ such that $\sigma_i, \sigma_j \in \Delta$. Without loss of generality, we can assume that $i < j$. Clearly $g \coloneqq x^{j-i} \in G$ maps $\sigma_k \mapsto \sigma_{(k+j-i) \bmod p}$ for all $k \in \mathbb{N}_p$, and hence $\sigma_i^g = \sigma_j \in \Delta^g \cap \Delta$. Suppose for a contradiction that $\Delta^g = \Delta$. Then $\sigma_i^{g^n} \in \Delta$ for all $n \in \mathbb{N}$, by a straightforward induction argument. Let $k \in \mathbb{N}_p$ be such that $\sigma_k \in \Sigma \setminus \Delta$. Also, note that $j - i \in \mathbb{N}_p \setminus \{0\}$ has a multiplicative inverse, say m, in $\mathbb{N}_p \setminus \{0\}$. It follows that $\sigma_k = \sigma_{(i+(j-i)n) \bmod p} = \sigma_i^{g^n} \in \Delta$, where $n \coloneqq m\,(p + k - i) \in \mathbb{N}$. This contradicts $\sigma_k \notin \Delta$, so $\Delta^g \neq \Delta$. Therefore Δ is not a block for G in Σ, which implies that G acts primitively on Σ. □

Lemma 2.3.4. Let $G \leq \mathrm{Sym}\,(\Omega)$ and $g \in G$. Also let $\Delta \subseteq \Omega$, and suppose that $G|_\Delta$ acts primitively on Δ. Then $G|_\Gamma$ acts primitively on $\Gamma \coloneqq \Delta^g$.

Proof. Clearly each $h \in G|_\Gamma$ fixes every $\omega \in \Omega \setminus \Gamma$, and hence $G|_\Gamma$ acts on Γ. Now let $\alpha, \beta \in \Gamma$. Then there exist $\gamma, \delta \in \Delta$ such that $\alpha = \gamma^g$ and $\beta = \delta^g$. Since $G|_\Delta$ acts transitively on Δ, there also exists $h \in G|_\Delta$ such that $\gamma^h = \delta$. It follows that $\alpha^{g^{-1}hg} = \gamma^{hg} = \delta^g = \beta$. If $\varepsilon \in \Omega \setminus \Gamma$ then $\varepsilon^{g^{-1}} \notin \Delta$, so ε is fixed by $g^{-1}hg$, which therefore lies in $G|_\Gamma$. This shows that $G|_\Gamma$ acts transitively on Γ.

Let $\Lambda \subset \Gamma$ with $|\Lambda| \geq 2$. Then $\Lambda^{g^{-1}} \subset \Delta$ and $\left|\Lambda^{g^{-1}}\right| = |\Lambda| \geq 2$, so $\Lambda^{g^{-1}}$ is not a block for $G|_\Delta$ in Δ. Hence there exists $h \in G|_\Delta$ such that $\Lambda^{g^{-1}h} \cap \Lambda^{g^{-1}} \neq \varnothing$ but $\Lambda^{g^{-1}h} \neq \Lambda^{g^{-1}}$. It follows that $\Lambda^{g^{-1}hg} \cap \Lambda \neq \varnothing$ but $\Lambda^{g^{-1}hg} \neq \Lambda$. Therefore Λ is not a block for $G|_\Gamma$ in Γ, since $g^{-1}hg \in G|_\Gamma$ as shown above. This implies that $G|_\Gamma$ acts primitively on Γ. □

Lemma 2.3.5. Let $G, H \leq \mathrm{Sym}(\Omega)$ act primitively on some $\Delta, \Gamma \subseteq \Omega$ respectively. Further, suppose that $\Delta \cap \Gamma \neq \varnothing$. Then $\langle G, H\rangle$ acts primitively on $\Delta \cup \Gamma$.

Proof. Since $\langle G, H\rangle|_{\Delta\cup\Gamma} \leq \langle G, H\rangle$ contains both G and H, it also contains $\langle G, H\rangle$, which implies that $\langle G, H\rangle = \langle G, H\rangle|_{\Delta\cup\Gamma}$ acts on $\Delta \cup \Gamma$. If $|\Delta \cup \Gamma| \leq 2$ then $\Delta \cup \Gamma$ is one of Δ or Γ, and the result is clear. Otherwise $|\Delta \cup \Gamma| \geq 3$. Let $\Lambda \subset \Delta \cup \Gamma$ with $|\Lambda| \geq 2$. Then there exists $\omega \in (\Delta \cup \Gamma) \setminus \Lambda$. Without loss of generality assume that $\omega \in \Delta$.

Suppose that $\Lambda \subseteq \Delta$. Then $\Lambda \subset \Delta$ since $\omega \in \Delta \setminus \Lambda$. This implies that Λ is not a block for G in Δ, so there exists $g \in G$ such that Λ^g is neither disjoint from, nor equal to, Λ. Since $g \in G \leq \langle G, H\rangle$, it follows that Λ is not a block for $\langle G, H\rangle$ in $\Delta \cup \Gamma$.

Now suppose that $\Lambda \cap \Delta = \varnothing$. Then $\Lambda \subseteq \Gamma$, and in fact $\Lambda \subset \Gamma$: if $\Lambda = \Gamma$ it would contain $\Delta \cap \Gamma \neq \varnothing$ (but $\Lambda \cap \Delta = \varnothing$). As above, it follows that Λ is not a block for $\langle G, H\rangle$ in $\Delta \cup \Gamma$.

Otherwise $\Lambda \not\subseteq \Delta$ and $\Lambda \cap \Delta \neq \varnothing$, so there exist $\gamma \in \Lambda \setminus \Delta$ and $\delta \in \Lambda \cap \Delta$. Since G acts transitively on Δ, there exists $g \in G \leq \langle G, H\rangle$ such that $\delta^g = \omega$. Therefore $\omega \in \Lambda^g \setminus \Lambda$, which implies that $\Lambda^g \neq \Lambda$. Moreover g fixes γ, since $\mathrm{supp}(g) \subseteq \Delta$, and hence $\gamma \in \Lambda^g \cap \Lambda \neq \varnothing$. This shows that Λ is not a block for $\langle G, H\rangle$ in $\Delta \cup \Gamma$.

Therefore $\langle G, H\rangle$ acts primitively on $\Delta \cup \Gamma$, by Lemma 2.2.7. □

Lemma 2.3.6. Suppose that $|\Omega| \geq 2$, and let $G \leq \mathrm{Sym}(\Omega)$ be primitive. Then G_ω is a maximal subgroup of G for all $\omega \in \Omega$.

Proof. Let $\omega, \upsilon \in \Omega$ be distinct. Since G is transitive, there exists $g \in G$ such that $\omega^g = \upsilon \neq \omega$. Therefore $g \in G \setminus G_\omega \neq \varnothing$. Now let $H \leq G$ with $G_\omega < H$. Then there exists $h \in H \setminus G_\omega$, so that $\omega \notin \mathrm{fix}(h)$. Since $\omega, \omega^h \in \omega^H$, this implies that $\left|\omega^H\right| \geq 2$. Suppose for a contradiction that $\omega^H \neq \Omega$. Then ω^H is not a block for G in Ω, as G is primitive. Hence by Lemma 2.2.6, there exists $g \in G$ such that $\left(\omega^H\right)^g \cap \omega^H \neq \varnothing \neq \left(\omega^H\right)^g \setminus \omega^H$. Therefore $\omega^{h_1 g} = \omega^{h_2}$ and $\omega^{h_3 g} \notin \omega^H$ for some $h_1, h_2, h_3 \in H$. In particular $h_3 g \notin H$, which implies that $g \notin H$. But $\omega^{h_1 g h_2^{-1}} = \omega^{h_2 h_2^{-1}} = \omega$, so that $h_1 g h_2^{-1} \in G_\omega \leq H$ and hence $g \in H$. This is a contradiction, so $\omega^H = \Omega$. Now let $g \in G$. Then $\omega^g \in \omega^H$, so there exists $h \in H$ such that $\omega^h = \omega^g$. It follows that $\omega^{gh^{-1}} = \omega$, so that $gh^{-1} \in G_\omega \leq H$ and hence $g \in H$. This implies that $G \subseteq H$, which shows that G_ω is maximal. □

Lemma 2.3.7. Let G be a cyclic group generated by $x \in G$. Then $\mathrm{Aut}(G)$ is abelian.

Proof. Let $\alpha, \beta \in \mathrm{Aut}\,(G)$. Then $x^\alpha = x^i$ and $x^\beta = x^j$ for some $i, j \in \mathbb{Z}$. Also let $g \in G$, so that $g = x^k$ for some $k \in \mathbb{Z}$. It follows that $g^\alpha = \left(x^k\right)^\alpha = (x^\alpha)^k = \left(x^i\right)^k = \left(x^k\right)^i = g^i$. Similarly, $g^\beta = g^j$ for all $g \in G$. Therefore $g^{\alpha\beta} = \left(g^i\right)^\beta = g^{ij} = g^{ji} = \left(g^j\right)^\alpha = g^{\beta\alpha}$ for all $g \in G$, which implies that $\alpha\beta = \beta\alpha$. Hence $\mathrm{Aut}\,(G)$ is abelian. □

Lemma 2.3.8. Let $G \leq \mathrm{Sym}\,(\Omega)$ and $x \in G$. Also let $N = N_G\,(C)$ be the normaliser of $C := \langle x \rangle$ in G. Then x commutes with every element of N', the derived group of N.

Proof. For each $n \in N$ define the function $\theta_n : C \to C$ by $y^{\theta_n} = n^{-1}yn$ for all $y \in C$. These functions are well-defined since $n^{-1}Cn = C$ for all $n \in N$. In fact they are automorphisms of C, for the same reason that $g \mapsto n^{-1}gn$ is an automorphism of G. Thus we can define a homomorphism $\phi : N \to \mathrm{Aut}\,(C)$ by $n^\phi = \theta_n$ for all $n \in N$. Lemma 2.3.7 implies that $\mathrm{Aut}\,(C)$ is abelian, so

$$[m,n]^\phi = \left(m^{-1}n^{-1}mn\right)^\phi = \left(m^{-1}\right)^\phi \left(n^{-1}\right)^\phi m^\phi n^\phi = \left(m^\phi\right)^{-1} m^\phi \left(n^\phi\right)^{-1} n^\phi = 1$$

for each $m, n \in N$. This implies that $N' \leq \mathrm{Ker}\,(\phi)$. Now let $g \in N'$. Then $g^\phi = 1$ and hence $g^{-1}xg = x^{\theta_g} = x^{g^\phi} = x$. Thus $xg = gx$ as required. □

We now prove our main result on primitive permutation groups. The following proof is again taken from [2], except for the base case, which requires that we construct a 3-cycle rather than a 2-cycle. This error is identified in [4]. A correct, but less detailed, proof appears in [5].

Theorem 2.3.9. Suppose that Ω is finite, and let $G \leq \mathrm{Sym}\,(\Omega)$ be primitive. Further, suppose that G contains a p-cycle x for some prime $p \leq |\Omega| - 3$. Then $\mathrm{Alt}\,(\Omega) \leq G$.

Proof. By Theorem 2.3.1 and Corollary 2.3.2, we may assume $p \geq 5$. Let $n = |\Omega| - p$, so that $n \geq 3$. We shall proceed by induction on n, but defer the base case $n = 3$. So assume that $n \geq 4$ and the result is true for $|\Omega| - p = n - 1$. Then $p \leq |\Omega| - 4$, and every subgroup of G that contains x and acts primitively on some $\Delta \subset \Omega$, with $|\Delta| = |\Omega| - 1$, will also contain $\mathrm{Alt}\,(\Delta)$. We proceed to find such a subgroup.

Let $\mathcal{W} = \{\Delta \subset \Omega \mid G|_\Delta \text{ acts primitively on } \Delta\}$ be partially ordered by set inclusion. By Lemma 2.3.3 $\mathrm{supp}\,(x) \in \mathcal{W}$, since $|\mathrm{supp}\,(x)| = p < |\Omega|$. Hence there exists a maximal $\Delta \in \mathcal{W}$ containing $\mathrm{supp}\,(x)$, as Ω is finite.[2] Since $\Delta \subset \Omega$ and $|\Delta| \geq p \geq 2$, this is not

[2] For a more detailed explanation, see footnote 1.

a block for G in Ω. So by Lemma 2.2.6, there exists $g \in G$ such that $\Delta^g \setminus \Delta \neq \varnothing$ and $\Delta^g \cap \Delta \neq \varnothing$. Therefore $\Delta \subset \Delta^g \cup \Delta$, and hence $\Delta^g \cup \Delta \notin \mathcal{W}$. But Lemma 2.3.4 implies that $\Delta^g \in \mathcal{W}$, so by Lemma 2.3.5 $G|_{\Delta^g \cup \Delta}$ acts primitively on $\Delta^g \cup \Delta$. It follows that $\Delta^g \cup \Delta = \Omega$, and

$$|\Omega| = |\Delta^g \cup \Delta| = |\Delta^g| + |\Delta| - |\Delta^g \cap \Delta| < 2\,|\Delta|\,,$$

since clearly $|\Delta^g| = |\Delta|\,$. Now let $\omega \in \Omega \setminus \Delta$, and $g \in G_\omega$. Then

$$|\Omega| \geq |\Delta^g \cup \Delta| = |\Delta^g| + |\Delta| - |\Delta^g \cap \Delta| = 2\,|\Delta| - |\Delta^g \cap \Delta| > |\Omega| - |\Delta^g \cap \Delta|\,,$$

and hence $|\Delta^g \cap \Delta| > 0$. Moreover $\omega \notin \Delta^g \cup \Delta$, since $\omega^g = \omega$. Therefore $\Delta^g \cup \Delta \subset \Omega$, and hence Lemmas 2.3.4 and 2.3.5 imply that $\Delta^g \cup \Delta \in \mathcal{W}$. Since Δ is finite, and maximal in $\mathcal{W}$, it follows that $\Delta^g = \Delta$. Therefore $g \in G_\Delta$, which shows that $G_\omega \leq G_\Delta$. Also $G_\Delta < G$ as Δ is not a block for G in Ω. Hence by Lemma 2.3.6, $G_\omega = G_\Delta$ for all $\omega \in \Omega \setminus \Delta$.

Let $\Gamma = \Omega \setminus \Delta$, and suppose for a contradiction that $|\Gamma| \geq 2$. Then Γ is not a block for G in Ω, so by Lemma 2.2.6 there exists $g \in G$ such that $\Gamma^g \cap \Gamma \neq \varnothing$ and $\Gamma^g \setminus \Gamma \neq \varnothing$. Choose $\gamma \in \Gamma^g \cap \Gamma$ and $\delta \in \Gamma^g \setminus \Gamma$, so that $\gamma = \alpha^g$ and $\delta = \beta^g$ for some $\alpha, \beta \in \Gamma$. Moreover $\delta \in \Delta$, since $\delta \notin \Gamma = \Omega \setminus \Delta$. Since $G|_\Delta$ acts transitively on Δ, there exists $h \in G|_\Delta \leq G$ such that $\delta^h \neq \delta$. However $\gamma^h = \gamma$, as $\gamma \notin \Delta$ and hence $G|_\Delta \leq G_\gamma$. It follows that $ghg^{-1} \in G$ fixes α but not β, both of which lie in $\Gamma = \Omega \setminus \Delta$. This contradicts $G_\alpha = G_\Delta = G_\beta$, so $|\Gamma| < 2$ and hence $|\Gamma| = 1$.

It follows that $|\Delta| = |\Omega| - 1$. Moreover $x \in G|_\Delta$, which acts primitively on $\Delta \in \mathcal{W}$, since $\operatorname{supp}(x) \subseteq \Delta$. Therefore $\operatorname{Alt}(\Delta) \leq G|_\Delta$, by the induction hypothesis. This implies that G contains a 3-cycle, as $|\Delta| \geq p > 3$ and $G|_\Delta \leq G$. By Theorem 2.3.1 it follows that $\operatorname{Alt}(\Omega) \leq G$, which completes the inductive step.

For the base case $|\Omega| = p + n = p + 3$, so $|\operatorname{Sym}(\Omega)| = |\Omega|! = (p+3)!$ and hence p, which is at least 5, does not divide $\frac{1}{p}\,|\operatorname{Sym}(\Omega)|\,$. Therefore 1 and p are the only powers of p that divide $|G|\,$, as $|G|$ divides $|\operatorname{Sym}(\Omega)|\,$. It follows that $C \coloneqq \langle x \rangle$ is a Sylow p-subgroup of G.

Now let $N = N_G(C)$ be the normaliser of C in G. If $\omega \in \operatorname{fix}(x)$ and $n \in N$, then $nxn^{-1} \in C$ fixes ω, so $(\omega^n)^x = \omega^{nxn^{-1}n} = \omega^n$ and hence $\omega^n \in \operatorname{fix}(x)\,$. Therefore each $n \in N$ fixes $\operatorname{fix}(x)\,$. Furthermore, for each distinct $\omega, \sigma \in \operatorname{fix}(x)$ there exists $n \in N$ which fixes ω but not σ. To show this, suppose to the contrary that $N_\omega = (N_\omega)_\sigma$ for some distinct $\omega, \sigma \in \operatorname{fix}(x)$. Then $C \leq (G_\omega)_\sigma \leq G_\omega$, since $\omega, \sigma \in \operatorname{fix}(y)$ for all $y \in C$. This implies that C is a Sylow p-subgroup of both G_ω and $(G_\omega)_\sigma$. Moreover, $N_\omega = (N_\omega)_\sigma$ is the normaliser of C in each of the stabilisers. Therefore $|G_\omega : N_\omega| \equiv |(G_\omega)_\sigma : N_\omega| \equiv 1 \bmod p$, by Sylow's Third Theorem, and since $|G_\omega : N_\omega| = |G_\omega : (G_\omega)_\sigma| \, |(G_\omega)_\sigma : N_\omega|$, it follows that $|G_\omega : (G_\omega)_\sigma| \equiv 1 \bmod p$. Now write $\Gamma = \{\gamma\}$. Then there exists $g \in G$ such that $\gamma^g = \omega$, as G is transitive. It follows that $\Delta^g = (\Omega \setminus \{\gamma\})^g = \Omega \setminus \{\omega\}$, so by Lemma 2.3.4 $G_\omega = \cap_{\delta \in \Omega \setminus \Delta^g} G_\delta = G|_{\Delta^g}$ acts primitively, thus transitively, on $\Omega \setminus \{\omega\}$. The Orbit-Stabiliser Theorem implies the contradiction

$$|G_\omega : (G_\omega)_\sigma| = \left|\sigma^{G_\omega}\right| = |\Omega \setminus \{\omega\}| = |\Omega| - 1 = p + 2 \not\equiv 1 \bmod p.$$

If we write $\operatorname{fix}(x) = \{\alpha, \beta, \gamma\}$, then there exist $m, n \in N$ such that m fixes α, but not β, and n fixes β, but not γ. Since $\operatorname{fix}(x)^m = \operatorname{fix}(x)^n = \operatorname{fix}(x)$, it follows that m swaps β with γ and n swaps γ with α. Now let $g = [m, n] \in N'$. Then

$$\begin{aligned}
\alpha^g &= \alpha^{m^{-1}n^{-1}mn} = \alpha^{n^{-1}mn} = \gamma^{mn} = \beta^n = \beta, \\
\beta^g &= \beta^{m^{-1}n^{-1}mn} = \gamma^{n^{-1}mn} = \alpha^{mn} = \alpha^n = \gamma, \\
\gamma^g &= \gamma^{m^{-1}n^{-1}mn} = \beta^{n^{-1}mn} = \beta^{mn} = \gamma^n = \alpha,
\end{aligned}$$

which implies that g contains $(\alpha\ \beta\ \gamma)$. By Lemma 2.3.8 $g = x^{-i} g x^i$ for all $i \in \mathbb{Z}$. Write $x = (\omega_0\ \omega_1\ \ldots\ \omega_{p-1})$ for some $\omega_0, \omega_1, \ldots, \omega_{p-1} \in \Omega$. Then $\omega_0^g \in \operatorname{supp}(x)$, since $g^{-1} \in N$ fixes $\operatorname{fix}(x)$. Therefore $\omega_0^g = \omega_i$ for some $i \in \mathbb{N}_p$, and hence

$$\omega_j^g = \omega_j^{x^{-j} g x^j} = \omega_0^{g x^j} = \omega_i^{x^j} = \omega_{(i+j) \bmod p}$$

for all $j \in \mathbb{N}_p$. It follows that g^p fixes each point of $\operatorname{supp}(x) = \{\omega_0, \omega_1, \ldots, \omega_{p-1}\}$, so $g^p = (\alpha\ \beta\ \gamma)^p$, which is either $(\alpha\ \beta\ \gamma)$ or $(\alpha\ \beta\ \gamma)^2 = (\alpha\ \gamma\ \beta)$ because $3 \nmid p$. This implies that $g^p \in N' \leq N \leq G$ is a 3-cycle, so by Theorem 2.3.1 $\operatorname{Alt}(\Omega) \leq G$. □

This theorem implies a similar result about transitive permutation groups, taken from [1].

Corollary 2.3.10. Suppose that Ω is finite, and let $G \leq \operatorname{Sym}(\Omega)$ be transitive. If there exists $x \in G$ and a prime p with $\frac{1}{2}|\Omega| < p \leq |\Omega| - 3$ such that x contains a p-cycle, then $\operatorname{Alt}(\Omega) \leq G$.

Proof. Let $\Delta \subseteq \operatorname{supp}(x)$ be the support of the p-cycle in the cycle structure of x. Then $\Delta^x = \Delta$ and $|\Delta| = p$, so $(\operatorname{supp}(x) \setminus \Delta)^x = \operatorname{supp}(x) \setminus \Delta$ and $|\operatorname{supp}(x) \setminus \Delta| \leq |\Omega| - p$. Therefore each $\omega \in \operatorname{supp}(x) \setminus \Delta$ will be fixed by x^i for some $i \in \mathbb{P}$ with $i \leq |\Omega| - p$. This implies that $x^{(|\Omega|-p)!} \in G$ is a p-cycle. It remains to show that G is primitive.

Suppose to the contrary that G is not primitive. Then there exists a non-trivial block Δ for G in Ω. This means that $2 \leq |\Delta| < |\Omega|$, and Δ^g is either equal to or disjoint from Δ for all $g \in G$. As G is transitive, it follows that $\Sigma \coloneqq \{\Delta^g \mid g \in G\}$ is a partition of Ω into sets of size $|\Delta|$. In particular, $|\Delta| \leq \frac{1}{2}|\Omega|$. For each $g \in G$ define the function $\theta_g : \Sigma \to \Sigma$ by $\Gamma^{\theta_g} = \Gamma^g$ for all $\Gamma \in \Sigma$. Then each θ_g is a bijection, with inverse $\theta_{g^{-1}}$. Hence we can define a homomorphism $\phi : G \to \operatorname{Sym}(\Sigma)$ by $g^\phi = \theta_g$ for all $g \in G$. Clearly

$$\operatorname{Ker}(\phi) = \{g \in G \mid \Gamma^g = \Gamma \text{ for all } \Gamma \in \Sigma\} \leq \langle \operatorname{Sym}(\Omega)|_\Gamma \mid \Gamma \in \Sigma\rangle \simeq (S_n)^m,$$

where $m \coloneqq |\Sigma|$ and $n \coloneqq |\Delta|$. By the First Isomorphism Theorem, $|G| = |G^\phi| |\operatorname{Ker}(\phi)|$ divides $m! \times (n!)^m$. But $2 \leq n \leq \frac{1}{2}|\Omega|$, so that $m \leq \frac{1}{2}|\Omega|$ and hence $m, n < p$. This implies that p does not divide $m! \times (n!)^m$, so it cannot divide $|G|$, which is a contradiction because $x^{(|\Omega|-p)!} \in G$ has order p. Therefore G is primitive, so by Theorem 2.3.9 $\operatorname{Alt}(\Omega) \leq G$. □

2.4 An algorithm to identify $\operatorname{Alt}(\Omega)$ or $\operatorname{Sym}(\Omega)$

The above results give some simple criteria which can be used to determine whether a given permutation group is isomorphic to one of the symmetric or alternating groups. They lead to a randomised Monte Carlo algorithm which can answer this question efficiently. The following lemma can be used to find the probability that such an algorithm will succeed.

Lemma 2.4.1. Suppose that Ω is finite, and let $G \leq \operatorname{Sym}(\Omega)$ with $\operatorname{Alt}(\Omega) \leq G$. Let $q \in \mathbb{P}$ and suppose that $\frac{1}{2}|\Omega| < q \leq |\Omega| - 2$. Then $\frac{1}{q}|G|$ elements of G contain a q-cycle. If $G = \operatorname{Sym}(\Omega)$, then this also holds for $q \in \{|\Omega|, |\Omega| - 1\}$.

Proof. There are $\binom{|\Omega|}{q}$ choices for subsets of Ω with size q. Since $q > \frac{1}{2}|\Omega|$, choosing a different set here gives rise to a different permutation. Once one has been chosen, the number of possible q-cycles to act on it is $(q-1)!$. The remaining elements of Ω can be permuted amongst themselves in an arbitrary way, and the number of possible ways is $(|\Omega| - q)!$. If $G = \mathrm{Sym}\left(\Omega\right)$, this implies that the number of choices for x is

$$\binom{|\Omega|}{q}(q-1)!\,(|\Omega|-q)! = \frac{|\Omega|!\,(q-1)!\,(|\Omega|-q)!}{q!\,(|\Omega|-q)!} = \frac{|\Omega|!}{q} = \frac{1}{q}\left|\mathrm{Sym}\left(\Omega\right)\right| = \frac{1}{q}\left|G\right|.$$

Otherwise $G = \mathrm{Alt}\left(\Omega\right)$, so only even permutations can be counted. However, the number of sets of size q and q-cycles on a given set remains the same. If q is odd, then the q-cycle contributes an even number of 2-cycles to x, so the number of possible permutations of the remaining elements will be $\left|A_{|\Omega|-q}\right| = \frac{1}{2}\left(|\Omega|-q\right)!$. Otherwise q is even, so the q-cycle contributes an odd number of 2-cycles to x, and the number of possible permutations of the remaining elements is $\left|S_{|\Omega|-q} \setminus A_{|\Omega|-q}\right| = \frac{1}{2}\left(|\Omega|-q\right)!$. Therefore the number of choices for x is

$$\binom{|\Omega|}{q}(q-1)!\frac{1}{2}\,(|\Omega|-q)! = \frac{|\Omega|!\,(q-1)!\,(|\Omega|-q)!}{2q!\,(|\Omega|-q)!} = \frac{|\Omega|!}{2q} = \frac{1}{q}\left|\mathrm{Alt}\left(\Omega\right)\right| = \frac{1}{q}\left|G\right|.$$

□

Lemma 2.4.2. Given $n \in \mathbb{P}$, a group $G \leq S_n$ and a constant $\varepsilon \in (0,1)$, Algorithm 1 reports whether $A_n \leq G$. The probability that it claims $A_n \nleq G$ when $A_n \leq G$ is at most ε.

Proof. If G is not transitive, then $A_n \nleq G$ unless $n = 2$, by Lemma 2.2.5. Any permutation group of degree 2 contains $A_2 = 1$, so the algorithm is correct in this case. Otherwise G is transitive, and by Corollary 2.3.10 it suffices to exhibit a p-cycle $x \in G$ such that p is a prime between $\left\lfloor \frac{n}{2} \right\rfloor + 1$ and $n - 3$. If $A_n \nleq G$ such a cycle will not be found, so the algorithm will correctly report failure. Otherwise $A_n \leq G$, and by Lemma 2.4.1 the proportion of such cycles in G is the sum p given on line 4. If there are no such elements, then $n \leq 7$ and a brute-force approach is efficient. Otherwise, the probability that none of $c \in \mathbb{P}$ random elements of G have the required cycle length is $q := (1-p)^c$. If $c > \log_{1-p}(\varepsilon)$ then $q < \varepsilon$. □

Algorithm 1 $IsAlternatingOrSymmetric(G, \varepsilon)$.

```
if $IsTransitive\,(G)$ then
    $n := Degree\,(G)$;
    $P := PrimesInInterval\left(\left\lfloor \frac{n}{2} \right\rfloor + 1, n - 3\right)$;
    $p := Sum\left[\frac{1}{q} \;\middle|\; q \in P\right]$;

    if $p = 0$ then
        return $|G| \geq \frac{n!}{2}$;
    end if;

    $c := \left\lceil \log_{1-p}(\varepsilon) \right\rceil$;
    $R := RandomProcess\,(G)$;

    for $i := 1$ to $c$ do
        $g := Random\,(R)$;
        $s := CycleStructure\,(g)$;
        if $LongestCycleLength\,(s) \in P$ then
            return true;
        end if;
    end for;

    return false;
else
    return $n = 2$;
end if;
```

Chapter 3

Constructive recognition of A_n and S_n

3.1 Motivation

The algorithm presented in the previous chapter only works for permutation representations of groups, using as it does the concepts of transitivity, primitivity and cycles. In this section we take a more general approach, which only requires that we can compute gh, g^{-1} and decide whether $g = h$, for elements g and h of the input group G. These so-called black-box groups include matrix groups and permutation groups. However, they do not include finitely-presented groups, as the equality of two elements in such a group is, in general, impossible to check. Nevertheless, we make use of finite presentations for the alternating group of degree $n \in \mathbb{P}$ in order to establish an isomorphism between A_n and a subgroup of G. Once this isomorphism has been constructed, it can be computed in either direction. Most of the algorithms we present are described in [6]; we have filled in the implementation details and made adjustments to ensure their correctness, in particular for the cases $5 \leq n \leq 10$, which are not covered in [6].

3.2 Presentations for the alternating groups

The following presentations for the alternating groups are due to Carmichael [7]. Their proofs are omitted. The second is stated incorrectly in [6], but [8] is a reliable, and accessible, source containing the original presentations.

Theorem 3.2.1. Let $n \in \mathbb{P}$ with $n \geq 4$. If n is odd, then A_n has presentation

$$\left\langle s, t \;\middle|\; t^3, s^{n-2}, (st)^n, \left(ts^{-1}ts\right)^2, \left(ts^{-2}ts^2\right)^2, \dots, \left(ts^{-\frac{n-3}{2}}ts^{\frac{n-3}{2}}\right)^2 \right\rangle;$$

otherwise A_n has presentation

$$\left\langle s, t \;\middle|\; t^3, s^{n-2}, (st)^{n-1}, \left(t^{-1}s^{-1}ts\right)^2, \left(ts^{-2}ts^2\right)^2, \dots, \left(t^{(-1)^{\frac{n-2}{2}}}s^{-\frac{n-2}{2}}ts^{\frac{n-2}{2}}\right)^2 \right\rangle.$$

These presentations are useful for our purposes since they completely describe the alternating groups without reference to their permutation representations. We connect these descriptions in the following way, in order to exploit the permutation structure in a general context.

Definition 3.2.2. Let $n \in \mathbb{P}$ with $n \geq 4$. If n is odd, the *standard generators* for A_n are $(3\ 4\ \dots\ n)$ and $(1\ 2\ 3)$. Otherwise, they are $(1\ 2)(3\ 4\ \dots\ n)$ and $(1\ 2\ 3)$. If G is a group and $s, t \in G$ are such that there exists an isomorphism $\theta : \langle s, t \rangle \to A_n$ which maps s and t to the respective standard generators for A_n, then s and t are *alternating n-generators* within G.

Lemma 3.2.3. Let G be a group and $n \in \mathbb{P}$ with $n \geq 5$. If $s, t \in G$ satisfy the presentation for A_n given in Theorem 3.2.1, and $\langle s, t \rangle \neq 1$, then s and t are alternating n-generators within G.

Proof. Let F be the free group on two generators y and z. Then $F/N \simeq A_n$ for some $N \trianglelefteq F$, and by von Dyck's Theorem there exists a homomorphism $\phi : F/N \to \langle s, t \rangle$ which maps $Ny \mapsto s$ and $Nz \mapsto t$. Since A_n is simple (as $n \geq 5$), either $\operatorname{Ker}(\phi) = 1$ or $\operatorname{Ker}(\phi) = A_n$. The latter is impossible because $\langle s, t \rangle \neq 1$, and $s, t \in A_n^{\phi} \leq \langle s, t \rangle$, so ϕ is an isomorphism.

Now let $a = (3\ 4\ \dots\ n)$ and $b = (1\ 2\ 3)$. Then $b^3 = a^{n-2} = 1$, and $ab = (1\ 2\ \dots\ n)$ so $(ab)^n = 1$. Moreover $x^{-1}bx = (1\ 2\ 3^x)$ for all $x \in ((A_n)_1)_2$ so $ba^{-k}ba^k = \left(1\ 3^{a^k}\right)(2\ 3)$ has order 2 for all $k \in \left\{1, 2, \dots, \frac{n-3}{2}\right\}$. If n is odd, it follows that a and b satisfy the presentation for A_n given in Theorem 3.2.1.

Otherwise, relabel $a = (1\ 2)(3\ 4\ \dots\ n)$. Then $b^3 = a^{n-2} = 1$, and $ab = (1\ 3\ 4\ \dots\ n)$ so $(ab)^{n-1} = 1$. The remaining relations are satisfied by a and b, since the effect of $(1\ 2)$

is to invert each b conjugated by odd powers of a, and this is cancelled by inverting the leading b.

By another application of von Dyck's theorem and the fact that A_n is simple, there exists an isomorphism $\psi : F/N \to \langle a, b \rangle$ which maps $Ny \mapsto a$ and $Nz \mapsto b$. It follows that $\phi^{-1}\psi$ is an isomorphism which maps $s \mapsto a$ and $t \mapsto b$. □

In order to make use of these presentations, we need algorithms to check whether they are satisfied by a given pair of generators. It should be clear that the following two algorithms fit this purpose.

Algorithm 2 *CheckOddGenerators* (n, s, t) .

```
if $t^3 \neq 1$ or $s^{n-2} \neq 1$ or $(st)^n \neq 1$ then
    return false;
else
    $g_1 := t$;
    $g_2 := t$;

    for $k := 1$ to $\frac{n-3}{2}$ do
        $g_1 := g_1 s$;
        $g_2 := g_2 s^{-1}$;

        if $(g_2 g_1)^2 \neq 1$ then
            return false;
        end if;
    end for;

    return true;
end if;
```

Lemma 3.2.4. Let G be a group. Given odd $n \in \mathbb{P}$ with $n \geq 4$ and $s, t \in G$ with $\langle s, t \rangle \neq 1$, Algorithm 2 determines whether s and t are alternating n-generators within G.

Proof. Follows from Lemma 3.2.3. □

Algorithm 3 $CheckEvenGenerators\,(n, s, t)$.

```
if $t^3 \neq 1$ or $s^{n-2} \neq 1$ or $(st)^{n-1} \neq 1$ then
    return false;
else
    $g_1 := t$;
    $g_2 := 1$;
    $p := 1$;

    for $k := 1$ to $\frac{n-2}{2}$ do
        $g_1 := g_1 s$;
        $g_2 := g_2 s^{-1}$;
        $p := -p$;

        if $(t^p g_2 g_1)^2 \neq 1$ then
            return false;
        end if;
    end for;

    return true;
end if;
```

Lemma 3.2.5. Let G be a group. Given even $n \in \mathbb{P}$ with $n \geq 4$ and $s, t \in G$ with $\langle s, t \rangle \neq 1$, Algorithm 3 determines whether s and t are alternating n-generators within G.

Proof. Follows from Lemma 3.2.3. □

3.3 Computing the inverse image of a permutation

Given alternating n-generators s and t within a black-box group G, we know there exists an associated isomorphism $\theta : \langle s, t \rangle \to A_n$, but have no method of computing it. However, we are able to write every permutation $a \in A_n$ as a word in s^θ and t^θ involving only products and inverses. Since θ is an isomorphism, and we can compute products and inverses in G, the corresponding word in s and t evaluates to $a^{\theta^{-1}}$. Before describing this algorithm in detail, we present a simple variant which works for S_n rather than A_n. This is useful if G is isomorphic to S_n, and helps to illustrate the main idea of the corresponding procedure for A_n.

Definition 3.3.1. Let $n \in \mathbb{P}$ with $n \geq 3$. The *standard generators* for S_n are $(1\ 2\ \ldots\ n)$ and $(1\ 2)$. If G is a group and $s, t \in G$ are such that there exists an isomorphism $\theta : \langle s, t \rangle \to S_n$ with $s^\theta = (1\ 2\ \ldots\ n)$ and $t^\theta = (1\ 2)$, then s and t are *symmetric n-generators* within G.

Lemma 3.3.2. Let G be a group. Given $n \in \mathbb{P}$ with $n \geq 3$, symmetric n-generators s' and t' within G, and $a \in S_n$, Algorithm 4 returns $a^{\theta^{-1}}$, where $\theta : \langle s', t' \rangle \to S_n$ is the isomorphism associated with s' and t'.

Proof. Let X be the cycle structure of a. Define a relation $\preceq$ on $X \times X$ by $x \preceq y$ if and only if the least element of $\operatorname{supp}(x)$ is at most that of $\operatorname{supp}(y)$. Then $\preceq$ is a total ordering on X, which may be listed in order as $x_1, x_2, \ldots, x_m$, where $m := |X|$. If $x \in X$ then $x = (i\ j_1\ j_2\ \ldots\ j_k)$ for some $k \in \mathbb{P}$ and $j_1, j_2, \ldots j_k \in \mathbb{P}_n$, where i is the least element of $\operatorname{supp}(x)$, and hence $x = (i\ j_1)(i\ j_2) \ldots (i\ j_k)$. Thus we aim to express $(i\ j)$ as a word in s^θ and t^θ, for each pair $i, j \in \mathbb{P}_n$ with $i < j$.

The outer loop searches from 1 to $n-1$ for $i \in \operatorname{supp}(a)$. This has the effect of traversing the list $x_1, x_2, \ldots, x_m$. It is not necessary to consider $i = n$, because either $n \in \operatorname{fix}(a)$ or $n \in \operatorname{supp}(x)$ for some $x \in X$, in which case there is a smaller number in $\operatorname{supp}(x)$.

Algorithm 4 *PermutationToElement* (n, s', t', a) .

```
$g \coloneqq 1$;
$s \coloneqq s't'$;                                   ▷ $s = (2\ 3\ \ldots\ n)$
$t \coloneqq t'$;                                     ▷ $t = (1\ 2)$

for $i \coloneqq 1$ to $n - 1$ do
    $j \coloneqq i$;
    $k \coloneqq j^a$;

    while $j \neq k$ do
        $h \coloneqq t^{s^{k-i-1}}$;                  ▷ $h = (i\ k)$
        $g \coloneqq gh$;

        $a \coloneqq a\,(j\ k)$;
        $j \coloneqq k$;
        $k \coloneqq j^a$;
    end while;

    $t \coloneqq t^{s'}$;
    $s \coloneqq st$;
end for;

return $g$;
```

If $\operatorname{supp}(a) = \varnothing$, then $a^{\theta^{-1}} = 1$, and the algorithm returns $g = 1$. Otherwise it finds the smallest $i \in \operatorname{supp}(x_1)$, and the inner loop runs through successive images k of i under x_1. This loop attempts to construct $h \in G$ such that $h^\theta = (i\ k)$. Once found, g is multiplied by h. At the end a is adjusted to fix $j := k^{x_1^{-1}}$, and the cycle in a which was $(j\ k\ \dots)$ becomes $(k\ \dots)$, or 1 if $k^{x_1} = i$. This ensures that the loop terminates at the appropriate time and members of $\operatorname{supp}(x_1)$ are not encountered again by the outer loop. If $k^{x_1} \neq i$, the new cycle $(k\ \dots)$ maps k to the same point as x_1. Once the inner loop has finished $g^\theta = x_1$, and $a = x_2 x_3 \dots x_m$ fixes every point preceding i, so by induction it remains to show that line 10 is correct.

We claim that, during each pass $i \in \mathbb{P}_{n-1}$ of the outer loop, $s^\theta = ((i+1)\ (i+2)\ \dots\ n)$ and $t^\theta = (i\ (i+1))$.[1] Since $s = s't'$ and $t = t'$ initially, this is clear for the case $i = 1$. Suppose it also holds for some $i \in \mathbb{P}_{n-2}$. Then $t^\theta = (i\ (i+1))^{(1\ 2\ \dots\ n)} = ((i+1)\,(i+2))$ in pass $i{+}1$ of the outer loop, and hence $s^\theta = ((i+1)\ (i+2)\ \dots\ n)\,t^\theta = ((i+2)\ (i+3)\ \dots\ n)$. By induction, this proves the claim. Therefore $\left(t^{s^{k-i-1}}\right)^\theta = \left(i\ (i+1)^{s^{k-i-1}}\right) = (i\ k)$ for all $i, k \in \mathbb{P}_n$ with $i < k$, so h is assigned to the correct element of G on line 10. □

Theorem 3.3.3. Let G be a group. Given $n \in \mathbb{P}$ with $n \geq 4$, alternating n-generators s and t within G, and $a \in A_n$, Algorithm 5 returns $a^{\theta^{-1}}$, where $\theta : \langle s, t\rangle \to A_n$ is the isomorphism associated with s and t.

Proof. Let X be the cycle structure of a, and list X in the order described in the proof of Lemma 3.3.2 as $x_1, x_2, \dots, x_m$, where $m := |X|$. Again we decompose a as a product of 2-cycles, but are no longer able to reconstruct an individual 2-cycle within G. By Lemma 1.3.8 this decomposition has an even number of 2-cycles, so we may insert $((n-1)\ n)\,(n\ (n-1))$ between every second pair of 2-cycles. We now aim to express $(i\ j)\,((n-1)\ n)$, or its inverse, as a word in s^θ and t^θ for all $i, j \in \mathbb{P}_n$ with $i < j$.

First, we comment on some differences from the approach taken by Algorithm 4. The outer loop need not consider $i \in \{n-1, n\}$ unless $x_m = ((n-1)\ n)$, which only contributes $(n\,(n-1))\,x_m = 1$ to a. Each time a 2-cycle from a is processed, the variable p switches from 1 to 2 or vice-versa. This keeps track of whether the next 2-cycle y from a should have $((n-1)\ n)$ on its right or left, which dictates whether we aim to

[1] For simplicity, we adopt the convention that $(n) = 1$ in the expression for s^θ.

Algorithm 5 $EvenPermutationToElement\,(n, s, t, a)\,.$

```
$g \coloneqq 1;$
$p \coloneqq 1;$
$q \coloneqq 1 + (n \bmod 2)\,;$

for $i \coloneqq 1$ to $n - 2$ do
    $j \coloneqq i;$
    $k \coloneqq j^a;$

    while $j \neq k$ do
        if $i = n - 2$ then
            if $k = n$ then
                $h \coloneqq t^p;$                              ▷ $t = ((n-2)\ \ (n-1)\ \ n)$
            else
                $h \coloneqq t^{3-p};$                          ▷ $t^2 = ((n-1)\ \ (n-2)\ \ n)$
            end if;
        else if $k \leq n - 2$ then
            $h_1 \coloneqq \left(t^{s^{n-i-3}}\right)^p;$       ▷ $t^{s^{n-i-3}} = (i\ \ (i+1)\ \ (n-1))$
            $h_2 \coloneqq (h_1^s)^q\,;$                        ▷ $\left(t^{s^{n-i-2}}\right)^q = ((i+1)\ \ i\ n)$
            $h \coloneqq h_2 h_1 h_2;$

            if $k > i + 1$ then
                $c \coloneqq t^{s^{k-i-2}};$
                if $IsOdd\,(k - i)$ then
                    $h \coloneqq h^{c^q};$                      ▷ $c^q = (i\ k\ \ (i+1))$
                else
                    $h \coloneqq h^{c^2};$                      ▷ $c^2 = (i\ k\ \ (i+1))$
                end if;
            end if;
        else
            $h_1 \coloneqq t^{s^{n-i-3}};$                      ▷ $h_1 = (i\ \ (i+1)\ \ (n-1))$
            $h_2 \coloneqq h_1^s;$                              ▷ $h_2^q = ((i+1)\ \ i\ n)$
```

Algorithm 5 *EvenPermutationToElement* (n, s, t, a) (continued).

```
            if $k < n$ xor $p \neq 1$ then
                $h := h_2^q h_1$;
            else
                $h := h_1^2 h_2^{3-q}$;
            end if;
        end if;

        $g := gh$;
        $p := 3 - p$;

        $a := a\,(j\ k)$;
        $j := k$;
        $k := j^a$;
    end while;

    if $q \neq 1$ then
        $t := t^{st}$;
        $s := st$;
    else
        $u := st$;
        $t := t^2$;
        $u := t^u$;
        $s := stu^2$;
        $t := u$;
    end if;

    $q := 3 - q$;
end for;

return $g$;
```

express $y\left((n-1)\ \ n\right)$ or its inverse as a word in s^θ and t^θ. The exponent p is only ever used on 3-cycles, so the value 2 is equivalent to -1 (in tests, squaring a matrix was faster than computing its inverse). A similar equivalence holds for the variable q, which is 1 if and only if $n-i$ is odd.

We claim that, during each pass $i \in \mathbb{P}_{n-2}$ of the outer loop, $t^\theta = (i\ \ (i+1)\ \ (i+2))$ and[2]

$$s^\theta = \begin{cases} ((i+2)\ \ (i+3)\ \ \ldots\ \ n), & \text{if } q \neq 1, \\ (i\ \ (i+1))\,((i+2)\ \ (i+3)\ \ \ldots\ \ n), & \text{otherwise.} \end{cases}$$

Since s and t are alternating n-generators, and q initially describes whether n is odd or even, this is clear for the case $i=1$. Suppose it also holds for some $i \in \mathbb{P}_{n-3}$. Further, suppose that $q \neq 1$ in pass i of the outer loop. Then $q=1$ in pass $i+1$ of the outer loop, and

$$t^\theta = (i\ \ (i+1)\ \ (i+2))^{((i+2)\ (i+3)\ \ldots\ n)(i\ (i+1)\ (i+2))} = ((i+1)\ \ (i+2)\ \ (i+3))$$

as required. Similarly

$$s^\theta = ((i+2)\ \ (i+3)\ \ \ldots\ \ n)\, t^\theta = ((i+1)\ \ (i+2))\,((i+3)\ \ (i+4)\ \ \ldots\ \ n)\,.$$

Otherwise $q=1$ in pass i of the outer loop, so $q \neq 1$ in pass $i+1$ and

$$t^\theta = ((i+1)\ \ i\ \ (i+2))^{(i\ (i+1))((i+2)\ (i+3)\ \ldots\ n)(i\ (i+1)\ (i+2))} = ((i+1)\ \ (i+2)\ \ (i+3))\,,$$

as required. Moreover

$$\begin{aligned} s^\theta &= (i\ \ (i+1))\,((i+2)\ \ (i+3)\ \ \ldots\ \ n)\,((i+1)\ \ i\ \ (i+2))\left(t^2\right)^\theta \\ &= ((i+3)\ \ (i+4)\ \ \ldots\ \ n)\,. \end{aligned}$$

By induction, this proves the claim.

Now let $i,k \in \mathbb{P}_n$ with $i<k$. Suppose that $i=n-2$, so that $k \in \{n-1,n\}$. If $k=n$, then $(i\ k)\,((n-1)\ \ n) = ((n-2)\ \ (n-1)\ \ n)$, which is equal to t^θ in pass i of the loop. As a 3-cycle, raising this to the power of p will result in $((n-1)\ \ n)\,(i\ k)$ if necessary. Similarly, if $k=n-1$ then $(i\ k)\,((n-1)\,n) = ((n-2)\ \ n\ \ (n-1))$ and we take the opposite power.

[2] Again we adopt the convention that $(n)=1$ in the expressions for s^θ.

Otherwise, suppose that $k \leq n-2$. Then $\left(t^{s^{n-i-3}}\right)^{\theta} = (i\ \ (i+1)\ \ (n-1))$, since $q = 1$ only when $n-i-3$ is even and hence $\left(s^{n-i-3}\right)^{\theta}$ always fixes i and $i+1$. Conjugating this 3-cycle by s and raising to the power q gives $((i+1)\ \ i\ n)$, and hence h^{θ} is either

$$((i+1)\ \ i\ n)\,(i\ \ (i+1)\ \ (n-1))\,((i+1)\ \ i\ n) = (i\ \ (i+1))\,((n-1)\ \ n)$$

or its inverse, depending on the value of p (since $(h_2 h_1 h_2)^{-1} = h_2^{-1} h_1^{-1} h_2^{-1}$). To reach $(i\ k)\,((n-1)\ \ n)$ we conjugate this by $(i\ k\ \ (i+1))$, which is either $(c^q)^{\theta}$ or $\left(c^2\right)^{\theta}$ depending on whether $k-i$ is odd or even.

Lastly $k \in \{n-1, n\}$. As in the previous case, $(h_2^q h_1)^{\theta} = (i\ n\ \ (n-1))$. This is either $(i\ k)\,((n-1)\ \ n)$ or its inverse, depending on whether k is $n-1$ or n. □

3.4 Determining the image a black-box group element

Computing the inverse image of a permutation is relatively straightforward because we can use the structure of the input permutation to our advantage. This approach is not available for the other direction, but we can build up knowledge about an element of a black-box group by manipulating it within the group. In particular, by evaluating the commutator of two elements we can determine whether the supports of their images intersect. This is especially useful if one of their images is already known. With this in mind, we describe algorithms which compute the inverse images of a variety of permutations within a black-box group.

Definition 3.4.1. Let $n, k \in \mathbb{P}$ with $n \geq 4$ and $k \leq n-2$. If s, t are alternating n-generators within some group G, with associated isomorphism $\theta : \langle s, t\rangle \to A_n$, then the *initial k elements* of $\langle s, t\rangle$ are $t = (1\ 2\ 3)^{\theta^{-1}}, (1\ 2\ 4)^{\theta^{-1}}, \ldots, (1\ 2\ \ (k+2))^{\theta^{-1}}$.

Lemma 3.4.2. Let $n \in \mathbb{P}$ with $n \geq 5$. If $x, y \in A_n$ are respectively a 3-cycle and a 5-cycle, then $\operatorname{supp}(x) \cap \operatorname{supp}(y) = \varnothing$ if and only if $[x, y] = 1$. Hence, if G is a group and $g, h \in G$ are such that there exists a monomorphism $\theta : G \to S_n$ under which g^{θ} is a 3-cycle and h^{θ} is composed of disjoint 5-cycles, then $\operatorname{supp}\left(g^{\theta}\right) \cap \operatorname{supp}\left(h^{\theta}\right) = \varnothing$ if and only if $[g, h] = 1$.

Proof. If $\operatorname{supp}(x) \cap \operatorname{supp}(y) = \varnothing$, it is clear that $xy = yx$. Conversely, suppose that the supports of x and y intersect at some $i \in \mathbb{P}_n$. Since $|\operatorname{supp}(y) \setminus \operatorname{supp}(x)| \geq 2$, we may choose i with $i^y \notin \operatorname{supp}(x)$. Then $i^{yx} = i^y \neq i^{xy}$ because $i \neq i^x$, so $[x, y] \neq 1$. □

Algorithm 6 $\mathit{DomainCover}\,(n, s, t, E)$.

```
$k \coloneqq \lfloor n/5 \rfloor$;
$m \coloneqq \lfloor \log_2(k) \rfloor + 1$;

$a \coloneqq E_1 E_2^2 E_3$;                                          ▷ $a = (1\ 2\ 3\ 4\ 5)$
$X \coloneqq \left[ \begin{Bmatrix} a, & \textbf{if } m \le j < 2m \\ 1, & \textbf{otherwise} \end{Bmatrix} \middle| \; j \in [1, \ldots, 2m] \right]$;

$a \coloneqq E_4 E_5^2 E_6 E_7^2 E_8 E_4^2$;                               ▷ $a = (6\ 7\ 8\ 9\ 10)$

for $i \coloneqq 2$ to $k$ do
    for $j \coloneqq 1$ to $m$ do
        if $\mathit{BitwiseAnd}\left(i, 2^{m-j}\right) \neq 0$ then
            $X_j \coloneqq X_j a$;
        else
            $X_{m+j} \coloneqq X_{m+j} a$;
        end if;
    end for;

    $a \coloneqq a^{s^5}$;                ▷ $a = ((5i+1)\ (5i+2)\ (5i+3)\ (5i+4)\ (5i+5))$
end for;

return $X$;
```

Lemma 3.4.3. Let G be a group and $n \in \mathbb{P}$ with $n \geq 10$. Define $k = \lfloor n/5 \rfloor$ and for each $i \in \mathbb{P}_k$ define $x_i = ((5i-4)\ (5i-3)\ (5i-2)\ (5i-1)\ (5i)) \in A_n$. Let m be the number of bits required to store k. Given n, alternating n-generators s and t within G, and a list E of the initial 8 elements of $\langle s, t \rangle$, Algorithm 6 returns a list X containing $2m$ elements of $\langle s, t \rangle$. The cycle structure of the image of X_j in A_n is contained in $\{x_i \mid i \in \mathbb{P}_k\}$ for all $j \in \mathbb{P}_{2m}$. If $i \in \mathbb{P}_k$ and $j \in \mathbb{P}_m$, then the image of X_j contains x_i if and only if the j^{th} most significant bit of i among the lowest m is 1, and the image of X_{j+m} contains x_i if and only if this bit is 0.

Proof. Clearly $\lfloor \log_2(k) \rfloor + 1$ is the number of bits required to store k. Let $\theta : \langle s, t \rangle \to A_n$ be the isomorphism associated with s and t. After line 4

$$a^\theta = \left(E_1 E_2^2 E_3\right)^\theta = (1\ 2\ 3)\,(1\ 4\ 2)\,(1\ 2\ 5) = (1\ 2\ 3\ 4\ 5) = x_1,$$

and X_m^θ is the only element of X among the first m which contains x_1. Every time X is modified, a cycle is added to exactly one of X_j or X_{j+m} for each $j \in \mathbb{P}_m$. After line 7

$$\begin{aligned} a^\theta &= \left(E_4 E_5^2 E_6 E_7^2 E_8 E_4^2\right)^\theta = (1\ 2\ 6)\,(1\ 7\ 2)\,(1\ 2\ 8)\,(1\ 9\ 2)\,(1\ 2\ 10)\,(1\ 6\ 2) \\ &= (6\ 7\ 8\ 9\ 10) = x_2, \end{aligned}$$

and following this, conjugating by s^5 maps a^θ to the next member of $\{x_i \mid i \in \mathbb{P}_k\}$. The if statement ensures that the correct relationship holds between the cycle structure of the images of members of X and the binary expansion of elements of $\mathbb{P}_k$. □

Algorithm 7 *ConjugateMap* (s, t, i, j) .

```
if $i < 3$ then
    if $j < 3$ then
        return $t^{j-i}$;
    else
        return $t^{3-i} s^{j-3}$;
    end if;
else
    return $s^{j-i}$;
end if;
```

Lemma 3.4.4. Let G be a group and $n \in \mathbb{P}$ with $n \geq 4$. Given alternating n-generators s and t within G, and $i, j \in \mathbb{P}_n$ such that $i \leq j$, Algorithm 7 returns $c \in \langle s, t \rangle$ such that $i^{c^\theta} = j$, where $\theta : \langle s, t \rangle \to A_n$ is the isomorphism associated with s and t.

Proof. If $i \leq j < 3$ then either $i = j$ or $i = 1$ and $j = 2$. In either case the image of t^{j-i} maps $i \mapsto j$. Otherwise $j \geq 3$. If $i < 3$ then the images of t^{3-i} and s^{j-3} respectively map $i \mapsto 3$ and $3 \mapsto j$ so their composition maps $i \mapsto j$. Otherwise $3 \leq i \leq j$ and $\left(s^{j-i}\right)^\theta$ maps $i \mapsto j$. □

Lemma 3.4.5. Let G be a group and $n \in \mathbb{P}$ with $n \geq 4$. If G is isomorphic to S_n, and $s, t \in G$ are alternating n-generators within G, with associated isomorphism $\theta : \langle s, t \rangle \to A_n$, there exists an isomorphism $\theta' : G \to S_n$ such that $g^{\theta'} = g^\theta$ for all $g \in \langle s, t \rangle$.

Proof. Let $\phi : G \to S_n$ be an isomorphism. Then $\theta^{-1}\phi \in \operatorname{Aut}(A_n)$, so if $n \neq 6$ there exists $c \in S_n$ such that $a^{\theta^{-1}\phi} = a^c$ for all $a \in A_n$. Define $\theta' : G \to S_n$ by $g^{\theta'} = cg^\phi c^{-1}$ for all $g \in G$. Then θ' is clearly an isomorphism, and for all $g \in \langle s, t \rangle$

$$g^{\theta'} = cg^\phi c^{-1} = c\left(g^{\theta\theta^{-1}}\right)^\phi c^{-1} = c\left(g^\theta\right)^{\theta^{-1}\phi} c^{-1} = c\left(g^\theta\right)^c c^{-1} = g^\theta.$$

If $n = 6$, then some members of $\operatorname{Aut}(A_n)$ do not correspond to inner automorphisms of S_n. However, these so-called exceptional automorphisms are just restrictions of those for S_6. Hence there exists $\psi \in \operatorname{Aut}(S_n)$ such that $\psi|_{A_n} = \theta^{-1}\phi$, and we may proceed as above to show that $\theta' := \phi\psi^{-1}$ is an isomorphism from $G \to S_n$ such that $g^{\theta'} = g^\theta$ for all $g \in \langle s, t \rangle$. □

Definition 3.4.6. Let $n \in \mathbb{N}$ with $n \geq 5$, and $l \in \mathbb{P}_n$. If $P \subseteq \mathbb{P}_n$ contains l and $|P| = 5$, a 3-*combination of points about* l is a list consisting of all 3-element subsets of P, with no duplicates. Let s, t be alternating n-generators within some group G, and let $\theta : \langle s, t \rangle \to A_n$ be the associated isomorphism. A 3-*combination of cycles about* l is a list of elements of $\langle s, t \rangle$, each of which maps to a 3-cycle under θ, such that the list of the supports of these 3-cycles is a 3-combination of points about l (with no duplicates).

Example 3.4.7. Every list of the 3-element subsets of $\mathbb{P}_5$ is a 3-combination of points about 1. A corresponding 3-combination of cycles about 1 in A_5 is

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5), (1\ 3\ 4), (1\ 3\ 5), (1\ 4\ 5), (2\ 3\ 4), (2\ 3\ 5), (2\ 4\ 5), (3\ 4\ 5).$$

Algorithm 8 $ElementImage\,(n, s, t, E, X, S, T, l, g)$.

```
$m := |X|/2$;
$i := 0$;

for $j := 1$ to $m$ do
    for $k := 1$ to $|T|$ do
        if $\left[X_j, T_k^g\right] = 1$ then
            $b := 0$;
            $k' := k$;
            break;
        else if $\left[X_{j+m}, T_k^g\right] = 1$ then
            $b := 1$;
            $k' := k$;
            break;
        end if;
    end for;

    if $l \notin S_{k'}$ then
        for $k := 1$ to $|T|$ do
            if $S_k \setminus S_{k'} = \{l\}$ then
                $k'' := k$;
                break;
            end if;
        end for;
        if $\left[X_{j+bm}, T_{k''}^g\right] \neq 1$ then
            $b := 1 - b$;
        end if;
    end if;

    $i := 2i + b$;
end for;
```

Algorithm 8 *ElementImage* $(n, s, t, E, X, S, T, l, g)$ (continued).

```
$J \coloneqq [n + 1 - (n \bmod 5), \ldots, n]$;
if $0 < i$ and $5i \leq n$ then
    $J \coloneqq [5i + j \mid j \in [-4, \ldots, 0]] \cup J$;
end if;

$C \coloneqq \left[E_1, E_2^2 E_3, E_4^2 E_5, E_6^2 E_7, E_8^2 E_9\right]$;                    ▷ $C_i = (1\ (2i)\ (2i+1))$
$i \coloneqq 1$;

$c \coloneqq ConjugateMap(s, t, 1, l)$;
$H \coloneqq \left[C_k^{cg} \mid k \in [1, 2]\right]$;

for $j \in J$ do
    $c \coloneqq ConjugateMap(s, t, i, j)$;
    $i \coloneqq j$;
    for $k \coloneqq 1$ to $|C|$ do
        $C_k \coloneqq C_k^c$;
    end for;

    $N \coloneqq [0, 0]$;
    for $h \in C$ do
        for $k \coloneqq 1$ to 2 do
            if $[h, H_k] = 1$ then
                if $N_k \geq 1$ then
                    continue $j$;
                end if;
                $N_k \coloneqq N_k + 1$;
            end if;
        end for;
    end for;

    return $j$;
end for;
```

Theorem 3.4.8. Let G be a group isomorphic to either A_n or S_n for some $n \in \mathbb{P}$ with $n \geq 11$. Given n, alternating n-generators s and t within G, a list E of the initial 9 elements of $\langle s, t \rangle$, the list X returned by Algorithm 6, a point $l \in \mathbb{P}_n$, an element $g \in G$ and 3-combinations S and T of points and cycles about l, Algorithm 8 returns the image of l under g^θ, where $\theta : G \to S_n$ is the monomorphism determined by s and t (via Lemma 3.4.5 if $G \simeq S_n$).

Proof. The first stage of the algorithm narrows down the range in which l^{g^θ} can lie to at most 9 elements of $\mathbb{P}_n$, using the list X. Let $k = \lfloor n/5 \rfloor$ and m be the number of bits required to store k. By Lemma 3.4.3, m is initialised correctly on line 1. Suppose there exists $i \in \mathbb{P}_k$ such that $l^{g^\theta} \in \{5i-4, 5i-3, \ldots, 5i\}$. We claim that, by line 31, the algorithm has computed this value of i. Since $i \leq k$ has at most m non-zero bits, it suffices to show that the number b produced in pass j of the loop is the j^{th} most significant bit of i among the lowest m.

Let $P \subseteq \mathbb{P}_n$ be the 5-element set associated with S. The supports of X_j^θ and X_{j+m}^θ are disjoint, so one must contain less than 3 points of $P' := P^{g^\theta}$. Hence there exists a 3-element subset $Q \subseteq P'$ which is fixed pointwise by X_j^θ or X_{j+m}^θ. Since $Q^{(g^\theta)^{-1}}$ is a 3-element subset of P, it is the support of $T_{k'}^\theta$ for some $k' \in \mathbb{P}_{10}$. It follows that $\left(T_{k'}^g\right)^\theta$ has support Q, so it commutes with one of X_j^θ or X_{j+m}^θ. This ensures that k' is actually defined on line 17.

If $l \in S_{k'} = \operatorname{supp}\left(T_{k'}^\theta\right)$ then $l^{g^\theta} \in \operatorname{supp}\left(\left(T_{k'}^g\right)^\theta\right)$. By Lemma 3.4.2, this implies that l^{g^θ} lies outside the support of either X_j^θ or X_{j+m}^θ, whichever one commutes with $\left(T_{k'}^g\right)^\theta$. Assuming that $l^{g^\theta} \leq 5 \lfloor n/5 \rfloor$, it follows by Lemma 3.4.3 that b is defined correctly on lines 7 and 11. Otherwise, we search for $k'' \in \mathbb{P}_{10}$ such that $l \in S_{k''}$ and the other elements of $S_{k''}$ also lie in $S_{k'}$. This exists because S is a 3-combination of points about l. If $T_{k''}^g$ commutes with X_{j+bm} (as $T_{k'}^g$ did), then b is (correctly) defined in the same way as it was for the case $l \in S_{k'}$. Otherwise, the failure of $T_{k''}^g$ to commute with X_{j+bm} implies that l^{g^θ} lies in the support of X_{j+bm}, so by Lemma 3.4.3 the value of b should be (and is) reversed.

Therefore i is correctly computed provided that $l^{g^\theta} \leq 5k$. If this is not the case, then the computed value of i may not make sense (in particular, it might be 0). This possibility is excluded by the if statement on line 32, after which J is guaranteed to contain l^{g^θ}. Next, the algorithm computes the inverse images under θ of $(1\ 2\ 3)$, $(1\ 4\ 2)\,(1\ 2\ 5) = (1\ 4\ 5)$,

$(1\ 6\ 2)\,(1\ 2\ 7) = (1\ 6\ 7)$, $(1\ 8\ 2)\,(1\ 2\ 9) = (1\ 8\ 9)$ and $(1\ 10\ 2)\,(1\ 2\ 11) = (1\ 10\ 11)$. The intersection of the supports of each pair of these cycles is $\{1\}$. By Lemma 3.4.4, the supports of $H_1^\theta = (1\ 2\ 3)^{(cg)^\theta}$ and $H_2^\theta = (1\ 4\ 5)^{(cg)^\theta}$ intersect only at l^{g^θ}. Moreover, when the list is updated in pass j of the following loop, the supports of each pair of cycles intersect only at j.

Finally, the algorithm tests every point $j \in J$ to check whether $l^{g^\theta} = j$. If $l^{g^\theta} = j$, then H_1 and H_2 each commute with at most one member of C, as this only occurs when the supports of their images are equal. Conversely, suppose that each of H_1 and H_2 commute with at most one member of C. Then at least four members of C do not commute with H_1, which is not possible unless $j \in \operatorname{supp}\left(H_1^\theta\right)$, by the pigeonhole principle. A similar argument implies that $j \in \operatorname{supp}\left(H_2^\theta\right)$, and hence $j \in \operatorname{supp}\left(H_1^\theta\right) \cap \operatorname{supp}\left(H_2^\theta\right)$. Therefore $j = l^{g^\theta}$, which shows that the algorithm returns j if and only if $j = l^{g^\theta}$. □

Corollary 3.4.9. Let G be a group isomorphic to either A_n or S_n for some $n \in \mathbb{P}$ with $n \geq 11$. Given n, alternating n-generators s and t within G, a list E of the initial 9 elements of $\langle s, t\rangle$, the list X returned by Algorithm 6, and $g \in G$, Algorithm 9 returns the list $1^{g^\theta}, 2^{g^\theta}, \ldots, n^{g^\theta}$, where $\theta : G \to S_n$ is the monomorphism determined by s and t.

Proof. It suffices to show that the l^{th} call to Algorithm 8 is passed a pair of 3-combinations of points and cycles about l. The first pair calculated is for $l = 3$, which is correct because the nested loops traverse each subset $\{i, j, k\} \subseteq \mathbb{P}_5$ exactly once, and

$$\begin{aligned}\left(E_j E_k^2 E_i E_j^2\right)^\theta &= (1\ 2\ \ (j+2))\,(2\ 1\ \ (k+2))\,(1\ 2\ \ (i+2))\,(2\ 1\ \ (j+2)) \\ &= ((i+2)\ \ (j+2)\ \ (k+2))\end{aligned}$$

for all $i, j, k \in \mathbb{P}_5$ with $i < j < k$. For $l = 1$, the cycles computed map under θ to

$$\begin{gathered}(1\ 2\ 3)\,, (1\ 2\ 4)\,, (1\ 2\ 5)\,, (1\ 3\ 2)\,(1\ 2\ 4) = (1\ 3\ 4)\,, (1\ 3\ 2)\,(1\ 2\ 5) = (1\ 3\ 5)\,, \\ (1\ 4\ 2)\,(1\ 2\ 5) = (1\ 4\ 5)\,, (1\ 2\ 3)\,(1\ 4\ 2) = (2\ 3\ 4)\,, (1\ 2\ 3)\,(1\ 5\ 2) = (2\ 3\ 5)\,, \\ (1\ 2\ 4)\,(1\ 5\ 2) = (2\ 4\ 5)\,, (1\ 2\ 4)\,(1\ 5\ 2)\,(1\ 2\ 3)\,(1\ 4\ 2) = (3\ 4\ 5)\,.\end{gathered}$$

This reproduces Example 3.4.7. When $l = 2$ each point is increased by one, since

$$(1\ 2\ 3)\,(1\ 5\ 2) = (2\ 3\ 5)\,, (1\ 2\ 4)\,(1\ 6\ 2) = (2\ 4\ 6)\,, (1\ 2\ 5)\,(1\ 6\ 2) = (2\ 5\ 6)\,,$$

Algorithm 9 $ElementToPermutation\left(n, s, t, E, X, g\right).$

```
$S := [\,]$;
$T := [\,]$;

for $i := 1$ to $5$ do
    for $j := i + 1$ to $5$ do
        for $k := j + 1$ to $5$ do
            $h := E_j E_k^2 E_i E_j^2$;                    ▷ $h = ((i+2)\ \ (j+2)\ \ (k+2))$
            $Append\left(S, \{i+2, j+2, k+2\}\right)$;
            $Append\left(T, h\right)$;
        end for;
    end for;
end for;

$T' := \left[E_1, E_2, E_3, E_1^2 E_2, E_1^2 E_3, E_2^2 E_3, E_1 E_2^2, E_1 E_3^2, E_2 E_3^2, T_1\right]$;
$S' := \left[\{j - 2 \mid j \in J\} \mid J \in S\right]$;
$L := \left[ElementImage\left(n, s, t, E, X, S', T', 1, g\right)\right]$;

$T' := \left[E_1 E_2^2, E_1 E_3^2, E_1 E_4^2, E_2 E_3^2, E_2 E_4^2, E_3 E_4^2, T_1, T_2, T_4, T_7\right]$;
$S' := \left[\{j - 1 \mid j \in J\} \mid J \in S\right]$;
$Append\left(L, ElementImage\left(n, s, t, E, X, S, T', 2, g\right)\right)$;

for $l := 3$ to $n$ do
    $Append\left(L, ElementImage\left(n, s, t, E, X, S, T, l, g\right)\right)$;
    if $l \equiv 2 \bmod 5$ then
        $m := \min\{n - l, 5\}$;
        for $i := 1$ to $|T|$ do
            $S_i := \{j + m \mid j \in S_i\}$;
            $T_i := T_i^{s^m}$;
        end for;
    end if;
end for;

return $L$;
```

and the other cycles have been calculated earlier. For larger values of l we increase each number in the point sets by 5 when needed, and conjugate the cycles by $\left(s^5\right)^\theta$, which has the same effect on their supports. A smaller number is used if they would end up outside $\mathbb{P}_n$. □

3.5 Permutation groups of small degree

The algorithms of the previous section are closely based on those found in [6]. They only work for permutation groups of degree at least 11 (although the authors incorrectly claim that they are valid for degrees between 7 and 10). Indeed, the second part of Algorithm 8 constructs five 3-cycles whose supports intersect pairwise at a single point. We replace this part with a method which works for groups of smaller degree. However, it is not as efficient, so the original algorithm should still be used if the given degree is at least 11. This efficiency loss is mitigated for groups of small degree because the first part of Algorithm 8 is no longer necessary.

The new algorithm is similar, in that it evaluates commutators to extract information about the supports of permutations. Since groups of small degree (particularly A_5) contain relatively few 3-cycles which commute with each other, it helps to have additional information about the supports of those with a non-trivial commutator.

Lemma 3.5.1. Let $n \in \mathbb{P}$ with $n \geq 3$, and $x, y \in S_n$ be 3-cycles. If $[x, y] = 1$ then $\operatorname{supp}(x)$ and $\operatorname{supp}(y)$ are either disjoint or equal. Otherwise, if $[x, y]^2 = 1$ then $\operatorname{supp}(x) \cap \operatorname{supp}(y)$ intersect at exactly 2 points. If $[x, y]^2 \neq 1$ then $|\operatorname{supp}(x) \cap \operatorname{supp}(y)| = 1$.

Proof. If x and y are disjoint, then they clearly commute. Suppose that $\operatorname{supp}(x) = \operatorname{supp}(y)$, and write $x = (i\ j\ k)$ for some $i, j, k \in \mathbb{P}_n$. Then $y \in \{(i\ j\ k), (i\ k\ j)\}$, so $[x, y] = 1$. Otherwise $\operatorname{supp}(x)$ and $\operatorname{supp}(y)$ intersect in at most 2 points. Suppose there exist distinct $i, j \in \operatorname{supp}(x) \cap \operatorname{supp}(y)$. Without loss of generality write $x = (i\ j\ k)$ for some $k \in \mathbb{P}_n$. Then $y = (i\ j\ l)$ or $y = (i\ l\ j)$ for some $l \in \mathbb{P}_n$ with $l \neq k$. In the first case

$$[x, y] = (i\ k\ j)(i\ l\ j)(i\ j\ k)(i\ j\ l) = (i\ j)(k\ l),$$

and in the second

$$[x, y] = (i\ k\ j)(i\ j\ l)(i\ j\ k)(i\ l\ j) = (i\ l)(j\ k).$$

Therefore $[x,y]^2 = 1$, but $[x,y] \neq 1$. Otherwise there is a unique $i \in \operatorname{supp}(x) \cap \operatorname{supp}(y)$. Write $x = (i\ j\ k)$ and $y = (i\ l\ m)$ for some $j,k,l,m \in \mathbb{P}_n$ with $\{j,k\} \cap \{l,m\} = \varnothing$. Then

$$[x,y] = (i\ k\ j)\,(i\ m\ l)\,(i\ j\ k)\,(i\ l\ m) = (i\ l\ j)\,,$$

so $[x,y] \neq 1 \neq [x,y]^2$. This completes the proof, as every case has been considered. □

Theorem 3.5.2. Let G be a group isomorphic to either A_n or S_n for some $n \in \mathbb{P}$ with $n \geq 5$. Given n, alternating n-generators s and t within G, a list E of the initial 3 elements of $\langle s,t \rangle$, and $g \in G$, Algorithm 10 returns $1^{g^\theta}, 2^{g^\theta}, \ldots, n^{g^\theta}$, where $\theta : G \to S_n$ is the monomorphism determined by s and t.

Proof. As shown in Corollary 3.4.9, the list T reproduces Example 3.4.7. For reference,

$$(1\ 2\ 3)\,,(1\ 2\ 4)\,,(1\ 2\ 5)\,,(1\ 3\ 4)\,,(1\ 3\ 5)\,,(1\ 4\ 5)\,,(2\ 3\ 4)\,,(2\ 3\ 5)\,,(2\ 4\ 5)\,,(3\ 4\ 5)\,,$$

are the respective images of each member of T under θ. Therefore, in pass l of the outer loop, H_1^θ and H_2^θ are 3-cycles whose supports intersect only at l. In pass j of the next loop c^θ maps $1 \mapsto j$, by Lemma 3.4.4. So $l^{g^\theta} \in \operatorname{supp}\left(h_1^\theta\right)$ and $j \in \operatorname{supp}\left(h_2^\theta\right)$ at line 21. At this point, we aim to determine whether $j \in \operatorname{supp}\left(h_1^\theta\right)$. If this holds for all $h_1 \in \{H_1^g, H_2^g\}$, then $l^{g^\theta} = j$, since the supports of H_1^θ and H_2^θ intersect only at l. Otherwise, it is clear that $l^{g^\theta} \neq j$.

Clearly $j \in \operatorname{supp}\left(h_1^\theta\right)$ whenever $h_1 \in \left\{h_2, h_2^2\right\}$. If h_1^θ commutes with h_2^θ, but is not equal to h_2^θ or its inverse $\left(h_2^2\right)^\theta$, then by Lemma 3.5.1 $j \notin \operatorname{supp}\left(h_1^\theta\right)$. In this case the algorithm moves on to test the next value of j. Otherwise, Lemma 3.5.1 is applied to determine the size S_k of $\operatorname{supp}\left(h_1^\theta\right) \cap \operatorname{supp}\left(h_2^\theta\right)$, where $h_2 = T_{5k-4}^c$ is one of T_1^c or T_6^c. If $S_1 = S_2 = 2$, then $j \in \operatorname{supp}\left(h_1^\theta\right)$, since the supports of $(T_1^c)^\theta$ and $(T_6^c)^\theta$ each contain two points apart from j, all four of which will lie in $\operatorname{supp}\left(h_1^\theta\right)$ unless $j \in \operatorname{supp}\left(h_1^\theta\right)$. Suppose that $S_1 = S_2 = 1$. If $j \in \operatorname{supp}\left(h_1^\theta\right)$, then j is the only point at which $\operatorname{supp}\left(h_1^\theta\right)$ intersects the support of $(T_k^c)^\theta$ for each $k \in \{2,3,4,5\}$. Therefore none of T_2^c, T_3^c, T_4^c or T_5^c commute with h_1. Conversely, if $j \notin \operatorname{supp}\left(h_1^\theta\right)$, then one other point from the supports of each of $(T_1^c)^\theta$ and $(T_6^c)^\theta$ lies outside $\operatorname{supp}\left(h_1^\theta\right)$, and together these form the support of $(T_k^c)^\theta$ for some $k \in \{2,3,4,5\}$. This permutation will commute with h_1^θ, and the algorithm will move on once it is found. Otherwise $S_1 \neq S_2$, so $S_k = 2$ and $S_{3-k} = 1$ for some $k \in \{1,2\}$. Let $t_1 = T_{5k-4}$ an $t_2 = T_{5(3-k)-4}$. Then m is defined so

Algorithm 10 $ElementToSmallDegreePermutation\,(n, s, t, E, g)$.

```
$T \coloneqq \left[E_1, E_2, E_3, E_1^2E_2, E_1^2E_3, E_2^2E_3, E_1E_2^2, E_1E_3^2, E_2E_3^2, E_2E_3^2E_1E_2^2\right]$;

$L \coloneqq [\,]$;
$H \coloneqq [T_1, T_6]$;                                   ▷ $H = [(1\ 2\ 3), (1\ 4\ 5)]$

for $l \coloneqq 1$ to $n$ do
    for $j \coloneqq 1$ to $n$ do
        if $j = 1$ then
            $c \coloneqq 1$;
        else
            $h \coloneqq ConjugateMap\,(s, t, j-1, j)$;
            $c \coloneqq ch$;
        end if;

        for $i \coloneqq 1$ to $|H|$ do
            $h_1 \coloneqq H_i^g$;
            $S \coloneqq [1, 1]$;

            for $k \coloneqq 1$ to $|S|$ do
                $h_2 \coloneqq T_{5k-4}^c$;

                if $h_2h_1 = 1$ or $h_2^2h_1 = 1$ then
                    continue $i$;
                else if $[h_1, h_2] = 1$ then
                    continue $j$;
                else if $[h_1, h_2]^2 = 1$ then
                    $S_k \coloneqq 2$;
                end if;
            end for;
```

Algorithm 10 *ElementToSmallDegreePermutation* (n, s, t, E, g) (continued).

```
            if $S_1 = S_2$ then
                if $S_1 = 1$ then
                    for $k \coloneqq 2$ to $5$ do
                        if $[h_1, T_k^c] = 1$ then
                            continue $j$;
                        end if;
                    end for;
                end if;
            else
                $m \coloneqq \left\{\begin{matrix} 6, & \textbf{if } S_1 > S_2 \\ 8, & \textbf{otherwise} \end{matrix}\right\}$;
                for $k \coloneqq 1$ to $2$ do
                    if $\left[h_1, T_{m+k}^c\right] = 1$ then
                        continue $j$;
                    end if;
                end for;
            end if;
        end for;

        $Append\,(L, j)$;
        break;
    end for;

    $c \coloneqq ConjugateMap\,(s, t, l, l+1)$;
    for $i \coloneqq 1$ to $|H|$ do
        $H_i \coloneqq H_i^c$;
    end for;
end for;

return $L$;
```

that $\left(T^c_{m+1}\right)^\theta$ and $\left(T^c_{m+2}\right)^\theta$ fix j and have supports which consist of two points from supp $\left(t^\theta_1\right)$ and one from supp $\left(t^\theta_2\right)$. To check this, see Example 3.4.7. If $j \in$ supp $\left(h^\theta_1\right)$, then exactly one of these points lies in supp $\left(h^\theta_1\right)$, and neither T^c_{m+1} nor T^c_{m+2} commute with h_1. Otherwise $j \notin$ supp $\left(h^\theta_1\right)$, and hence the support of either $\left(T^c_{m+1}\right)^\theta$ or $\left(T^c_{m+2}\right)^\theta$ is exactly supp $\left(h^\theta_1\right)$. One of these permutations will commute with h^θ_1, and the algorithm will continue when it is found.

If the end of the loop over i is reached, then one of the above conditions has ensured that $j \in$ supp $\left(h^\theta_1\right)$ for $h_1 = H^g_1$ and $h_1 = H^g_2$, and hence $l^{g^\theta} = j$. This information is added to the list L, which is returned once complete. □

3.6 Finding alternating generators

The algorithms of the previous two sections can be used to answer questions about a black-box group G isomorphic to A_n or S_n, for some given degree $n \in \mathbb{P}$. In order to apply them, we need alternating n-generators within G. The following algorithms are a significant step towards a general method for constructing them. However, they only work when provided with certain cycles as input. These algorithms are described in [6], but required some adjustments. In particular, lines 9-16 of Algorithm 11 are modifications that ensure it works correctly.

Lemma 3.6.1. Let G be a group isomorphic to A_n or S_n for some even $n \in \mathbb{P}$ with $n \geq 6$. Given n, a process R for generating random elements of G and $a, b \in G$ which map under some monomorphism $\theta : G \to S_n$ to an $(n-1)$-cycle and a 3-cycle respectively, Algorithm 11 returns alternating n-generators within G with probability at least $1 - \left(1 - \frac{3}{n}\right)^{2n/3}$.

Proof. Let l be the unique fixed point of a^θ. We aim to find $c \in G$ such that c^θ is a 3-cycle with $l \in$ supp $\left(c^\theta\right)$. Since $n \geq 5$, it suffices to search among conjugates of b in G. Indeed, if $x \in S_n$ is 3-cycle then $x^y = b^\theta$ for some $y \in S_n$. If $y \notin A_n$, choose a 2-cycle $z \in S_n$ disjoint from x, so that $x^{zy} = b^\theta$ and $zy \in A_n$. So the total number of conjugates c of b is $2\binom{n}{3}$, and there are $2\binom{n-1}{2}$ with $l \in$ supp $\left(c^\theta\right)$. The corresponding proportion is

$$\frac{2\binom{n-1}{2}}{2\binom{n}{3}} = \frac{(n-1)(n-2)}{2!}\frac{3!}{n(n-1)(n-2)} = \frac{3}{n}.$$

Algorithm 11 $FindEvenGenerators\,(R, n, a, b)$.

```
for $r := 1$ to $\lceil 2n/3 \rceil$ do
    $c := b^{Random(R)}$;

    if $[c^a, c] \neq 1$ then
        $c' := c^{a^2}$;
        if $[c', c] \neq 1$ and $\left[(c')^{a^2}, c\right] \neq 1$ then
            $t := [c^a, c]$;

            if $t^2 = 1$ then
                $d := c^{c^a}$;
                if $[d, d^a]^2 = 1$ then
                    return $ac, c$;
                else if $n \geq 8$ or $\left((ac)^{n-3} \neq 1$ and $\left(ac^2\right)^{n-3} \neq 1\right)$ then
                    return $ac^2, c^2$;
                end if;
            else if $n \geq 9$ or $\left((at)^3 \neq 1$ and $(at)^{n-3} \neq 1\right)$ then
                return $at, t$;
            end if;
        end if;
    end if;
end for;

return $1, 1$;
```

If $g, h \in G$ then $b^g = b^h$ if and only if g and h are in the same coset of the centraliser $C_G(b)$ of b in G. Each of these cosets has the same size, so finding a random conjugate of b is equivalent to taking a random element $g \in G$ and evaluating b^g. Therefore the probability that the algorithm will fail to find a 3-cycle $c \in G$ with $l \in \operatorname{supp}\left(c^\theta\right)$ is at most $\left(1 - \frac{3}{n}\right)^{2n/3}$.

If such a $c \in G$ is found, it does not commute with c^a, c^{a^2} and c^{a^4}. Indeed, l is fixed by $x := a^\theta$, x^2 and x^4, but the other points of $\operatorname{supp}\left(c^\theta\right)$ are not (since x has length at least 5). Moreover, these points do not map to each other under x, x^2 or x^4 (since x has odd length).

Write $c^\theta = (l\ i\ j)$, so that $[c^a, c]^\theta = (l\ j^x\ i^x)\,(l\ j\ i)\,(l\ i^x\ j^x)\,(l\ i\ j)$. If $i^x \neq j$ and $j^x \neq i$ then $[c^a, c]^2 \neq 1$, by Lemma 3.5.1. In this case, the algorithm returns *at* and t, where $t := [c^a, c]$ maps under θ to $(l\ i\ i^x)$. Without loss of generality write $l = 1$, $i = 2$ and $x = (2\ 3\ \ldots\ n)$, so that $t^\theta = (1\ 2\ 3)$ and $(at)^\theta = (1\ 2)\,(3\ 4\ \ldots\ n)$, which are the standard generators for A_n. In particular *at* has order $n - 2$, so the additional checks when $n < 9$ have no effect.

Otherwise $i^x = j$ or $j^x = i$, so $[c^a, c]^2 = 1$. In the first case $c^\theta = (l\ i\ i^x)$, so *ac* and c are alternating n-generators within G. Moreover, $d^\theta = (l\ i\ i^x)^{\left(l\ i^x\ i^{x^2}\right)} = \left(i^x\ i\ i^{x^2}\right)$ and hence the supports of d^θ and $(d^a)^\theta = \left(i^{x^2}\ i^x\ i^{x^3}\right)$ intersect at 2 points. Therefore $[d, d^a]$ has order 2, and the algorithm returns the correct elements. Otherwise $\left(c^2\right)^\theta = (l\ j\ j^x)$, so it is correct to return ac^2 and c^2. In this case $d^\theta = (l\ j^x\ j)^{\left(l\ j^{x^2}\ j^x\right)} = \left(j^{x^2}\ l\ j\right)$, so $(d^a)^\theta = \left(j^{x^3}\ l\ j^x\right)$ and $[d, d^a]$ has order 3. Since ac^2 and c^2 are alternating n-generators, $(ac)^{n-3} \neq 1 \neq \left(ac^2\right)^{n-3}$. In particular, the additional checks when $n < 8$ have no effect. This shows that the correct elements are returned whenever $l \in \operatorname{supp}\left(c^\theta\right)$.

Conversely, let $c \in G$ be a 3-cycle with $l \notin \operatorname{supp}\left(c^\theta\right)$ such that $[c^a, c] \neq 1$. Then the supports of c^θ and $(c^a)^\theta$ intersect in at most 2 points. If they intersect at exactly 2 points, then $[c^a, c]^2 = 1$ and $\operatorname{supp}\left(c^\theta\right) = \left\{i, i^x, i^{x^2}\right\}$ for some $i \in \operatorname{supp}(x)$ (since x has length at least 5). Without loss of generality write $i = 2$ and $x = (2\ 3\ \ldots\ n)$, so that c^θ is $(2\ 3\ 4)$ or $(2\ 4\ 3)$. If $n \geq 8$ then c commutes with c^{a^4}, whose image has support $\{6, 7, 8\}$. Otherwise, suppose that $c^\theta = (2\ 3\ 4)$. Then $d^\theta = (2\ 3\ 4)^{(3\ 4\ 5)} = (2\ 4\ 5)$, so $(d^a)^\theta = (3\ 5\ 6)$ and $[d, d^a]$ has order 3. Moreover $\left(ac^2\right)^\theta = (2\ 3\ \ldots\ n)\,(2\ 4\ 3) = (4\ 5\ \ldots\ n)$ has order $n-3$. Similarly, if $c^\theta = (2\ 4\ 3)$ then $d^\theta = (2\ 4\ 3)^{(3\ 5\ 4)} = (2\ 3\ 5)$, so $(d^a)^\theta = (3\ 4\ 6)$

and $[d, d^a]$ has order 3. The above calculation shows that $(ac)^\theta = (4\ 5\ \dots\ n)$ has order $n-3$. In every case the algorithm will move on to test the next random conjugate of b. Otherwise the supports of c^θ and $(c^a)^\theta$ intersect at exactly one point, and hence $[c^a, c]^2 \neq 1$. If c does not commute with c^{a^2} then $\mathrm{supp}\left(c^\theta\right)$ is either $\left\{i, i^x, i^{x^3}\right\}$ or $\left\{i, i^{x^2}, i^{x^3}\right\}$ for some $i \in \mathrm{supp}\,(x)$. Without loss of generality write $i = 2$ and $x = (2\ 3\ \dots\ n)$, so that $\mathrm{supp}\left(c^\theta\right)$ is either $\{2, 3, 5\}$ or $\{2, 4, 5\}$. If $n \geq 9$ it follows that c commutes with c^{a^4}. Otherwise, we claim that at has order 3 or $n-3$, where $t := [c^a, c]$. Indeed, t^θ is one of

$$\begin{aligned}
\left[(2\ 3\ 5)^x, (2\ 3\ 5)\right] &= (3\ 6\ 4)\,(2\ 5\ 3)\,(3\ 4\ 6)\,(2\ 3\ 5) = (3\ 5\ 4)\,,\\
\left[(2\ 5\ 3)^x, (2\ 5\ 3)\right] &= (3\ 4\ 6)\,(2\ 3\ 5)\,(3\ 6\ 4)\,(2\ 5\ 3) = (2\ 6\ 3)\,,\\
\left[(2\ 4\ 5)^x, (2\ 4\ 5)\right] &= (3\ 6\ 5)\,(2\ 5\ 4)\,(3\ 5\ 6)\,(2\ 4\ 5) = (2\ 6\ 5)\,,\\
\left[(2\ 5\ 4)^x, (2\ 5\ 4)\right] &= (3\ 5\ 6)\,(2\ 4\ 5)\,(3\ 6\ 5)\,(2\ 5\ 4) = (3\ 5\ 4)\,,
\end{aligned}$$

and hence $(at)^\theta$ is one of

$$\begin{aligned}
(2\ 3\ \dots\ n)\,(3\ 5\ 4) &= (2\ 5\ 6\ \dots\ n)\,,\\
(2\ 3\ \dots\ n)\,(2\ 6\ 3) &= (3\ 4\ 5)\,(6\ 7\ \dots\ n)\,,\\
(2\ 3\ \dots\ n)\,(2\ 6\ 5) &= (2\ 3\ 4)\,(6\ 7\ \dots\ n)\,,
\end{aligned}$$

where $(6\ 7\ \dots\ n)$ denotes 1 if $n = 6$. Since $n \in \{6, 8\}$, the orders of these are $n-3$ or 3. So in every case the algorithm will move on to test the next random conjugate of b. □

Lemma 3.6.2. Let G be a group isomorphic to either A_n or S_n for some odd $n \in \mathbb{P}$ with $n \geq 5$. Given n, a process R for generating random elements of G and $a, b \in G$ which map under some monomorphism $\theta : G \to S_n$ to an n-cycle and a 3-cycle respectively, Algorithm 12 returns alternating n-generators within G with probability at least $1 - \left(1 - \frac{6}{n+3}\right)^{\frac{n+3}{3}}$.

Proof. We aim to find $c \in G$ such that c^θ is a 3-cycle with support intersecting $\mathrm{supp}\left((c^a)^\theta\right)$. As argued in Lemma 3.6.1, it suffices to search the $2\binom{n}{3}$ conjugates of b for such a cycle. If $x = a^\theta$, there are no 3-cycles $y \in S_n$ such that $\mathrm{supp}\,(y) = \mathrm{supp}\,(y^x)$. The number with $|\mathrm{supp}\,(y) \cap \mathrm{supp}\,(y^x)| = 2$ is $2n$, since there are n choices for the point $i \in \mathrm{supp}\,(y)$ outside the intersection, and 2 choices for a cycle with support $\left\{i, i^x, i^{x^2}\right\}$.

Algorithm 12 $\mathit{FindOddGenerators}\,(R, n, a, b)$.

```
for $r := 0$ to $\lceil n/3 \rceil$ do
    $c := b^{Random(R)}$;

    if $[c, c^a] \neq 1$ then
        $c' := c^{a^2}$;                                        ▷ $1, 2 \in \mathrm{supp}\,(c)$
        if $(cc^a)^2 = 1$ then
            $d := c^{c'}$;                                      ▷ $\mathrm{supp}\,(c) = \{1, 2, 3\}$

            if $\left[d, d^{a^2}\right] = 1$ or $\left(n = 5 \text{ and } \left[d, d^{a^2}\right]^2 \neq 1\right)$ then
                return $ac^2, c$;                               ▷ $c = (1\ 2\ 3)$
            else
                return $ac, c^2$;                               ▷ $c = (1\ 3\ 2)$
            end if;
        else
            $d := c^{c^a}$;

            if $[d, d^a] = 1$ or $\left(\left[c, c^{c'}\right] \neq 1 \text{ and } \left[d, d^{a^2}\right] \neq 1 \text{ and } [d, d^a]^2 \neq 1\right)$ then
                $t := \left[c^2, c^a\right]$;                   ▷ $1^c = 2$
            else
                $t := \left[c, (c^a)^2\right]$;                 ▷ $2^c = 1$
            end if;

            return $at^2, t$;
        end if;
    end if;
end for;

return $1, 1$;
```

Moreover, the number with $|\mathrm{supp}\,(y) \cap \mathrm{supp}\,(y^x)| = 1$ is $2n\,(n-4)\,,$ since there are n choices for the point of intersection i, and $n-4$ choices for $j \in \mathbb{P}_n \setminus \left\{i^{x^{-2}}, i^{x^{-1}}, i, i^x\right\}$ such that $\mathrm{supp}\,(y) = \left\{i, j, i^{x^{-1}}\right\}.$
Therefore the number of conjugates of c of b such that c^θ is a 3-cycle with support intersecting $\mathrm{supp}\left((c^a)^\theta\right)$ is $2n\,(n-3)\,,$ and the corresponding proportion is

$$\frac{2n\,(n-3)}{2\binom{n}{3}} = n\,(n-3)\,\frac{3!}{n\,(n-1)\,(n-2)} = \frac{6\,(n-3)}{(n-1)\,(n-2)} \geq \frac{6}{n+3}.$$

So the probability that the algorithm will fail to find such a 3-cycle is at most $\left(1 - \frac{6}{n+3}\right)^{1+\frac{n}{3}}.$
If such a cycle c is found, it will not commute with c^a, since the supports of their images intersect, but cannot be equal. Hence there exists $i \in \mathrm{supp}\left(c^\theta\right)$ such that $i^x \in \mathrm{supp}\left(c^\theta\right)$ and $i^{x^{-1}} \notin \mathrm{supp}\left(c^\theta\right).$ Without loss of generality write $i = 1$ and $x = (1\ 2\ \ldots\ n)\,,$ so that $\mathrm{supp}\left(c^\theta\right) = \{1, 2, j\}$ for some $j \in \mathbb{P}_{n-1}$. If $j = 3$, then $(cc^a)^\theta$ is one of

$$(1\ 2\ 3)\,(2\ 3\ 4) = (1\ 3)\,(2\ 4) \text{ or } (1\ 3\ 2)\,(2\ 4\ 3) = (1\ 2)\,(3\ 4)\,.$$

and has order 2. Otherwise $(cc^a)^\theta$ is one of

$$(1\ 2\ j)\,(2\ 3\ j^x) = (1\ 3\ j^x\ 2\ j) \text{ or } (2\ 1\ j)\,(3\ 2\ j^x) = (1\ j\ j^x\ 3\ 2)\,,$$

and has order 5. Hence the algorithm distinguishes these cases correctly.
Suppose that $c^\theta = (1\ 2\ 3)\,.$ Then $d^\theta = (1\ 2\ 3)^{(3\ 5\ 4)} = (1\ 2\ 5)\,,$ which provided $n \geq 7$ commutes with $\left(d^{a^2}\right)^\theta = (3\ 4\ 7)\,.$ If $n = 5$ then $\left(d^{a^2}\right)^\theta = (3\ 4\ 2)$ and $\left[d, d^{a^2}\right]$ has order 3, by Lemma 3.5.1. In either case, the algorithm returns alternating n-generators because

$$c^\theta = (1\ 2\ 3) \text{ and } \left(ac^2\right)^\theta = (1\ 2\ \ldots\ n)\,(1\ 3\ 2) = (3\ 4\ \ldots\ n)\,.$$

Conversely, suppose that $c^\theta = (1\ 3\ 2)\,.$ Then $d^\theta = (1\ 3\ 2)^{(3\ 4\ 5)} = (1\ 4\ 2)$ does not commute with $\left(d^{a^2}\right)^\theta = (3\ 6\ 4)\,,$ provided $n \neq 5$. Otherwise the latter is $(3\ 1\ 4)\,,$ and $\left[d, d^{a^2}\right]^2 = 1$. The algorithm returns alternating n-generators for the same reason as above.
It remains to consider the case $4 \leq j \leq n-1$. Suppose that $c^\theta = (1\ 2\ j)\,.$ Then $\left(c^2\right)^\theta = (2\ 1\ j)$ and $(c^a)^\theta = (2\ 3\ j^x)\,,$ so $\left[c^2, c^a\right]^\theta = (1\ 2\ j)\,(3\ 2\ j^x)\,(2\ 1\ j)\,(2\ 3\ j^x) = (1\ 2\ 3)\,.$

Therefore t should be assigned to this commutator. Moreover $d^\theta = (1\ 2\ j)^{(2\ 3\ j^x)} = (1\ 3\ j)$, so if $[d, d^a] \neq 1$ then $j = 4$ (since $5 \leq j^x \leq n$). In this case $[d, d^a]$ has order 3, because $d^\theta = (1\ 3\ 4)$ and $(d^a)^\theta = (2\ 4\ 5)$. Furthermore $\left[d, d^{a^2}\right] \neq 1 \neq \left[c, c^{c'}\right]$, since $\left(d^{a^2}\right)^\theta$ is either $(3\ 5\ 6)$ or $(3\ 5\ 1)$ and $(c')^\theta$ is either $(3\ 4\ 6)$ or $(3\ 4\ 1)$, depending on whether $n = 5$. This shows that t is assigned correctly whenever $c^\theta = (1\ 2\ j)$.

Conversely, suppose that $c^\theta = (2\ 1\ j)$. Then $\left(c^2\right)^\theta = (1\ 2\ j)$, so t should be assigned to $\left[c, (c^a)^2\right]$. Moreover $d^\theta = (2\ 1\ j)^{(3\ 2\ j^x)} = (j^x\ 1\ j)$, which implies that $(d^a)^\theta = \left(j^{x^2}\ 2\ j^x\right)$. Therefore $[d, d^a] \neq 1$. It remains to show that one of the other expressions on line 17 is trivial. To this end, suppose that $\left[c, c^{c'}\right] \neq 1$. Then $j = 4$ or $j^{x^2} = 1$, since $(c')^\theta = \left(4\ 3\ j^{x^2}\right)$. In the first case $d^\theta = (1\ 4\ 5)$, so provided that $n \geq 7$ the image of d^{a^2} under θ is $(3\ 6\ 7)$. This implies that $\left[d, d^{a^2}\right] = 1$. If $n = 5$, then $(d^a)^\theta = (1\ 2\ 5)$ and hence $[d, d^a]$ has order 2. In the second case $j = n - 1$, so $d^\theta = (n\ 1\ \ (n-1))$ and $(d^a)^\theta = (1\ 2\ n)$. Therefore $[d, d^a]$ has order 2. It follows that one of the expressions on line 17 is trivial, and t is assigned correctly. □

3.7 Finding input cycles

The algorithms of the previous section reduce the problem of finding alternating generators to that of constructing cycles with certain lengths. In order to accomplish this, we search among random elements which give 1 when raised to a certain power. Several preliminary results are required before we can determine the probability that such an algorithm will succeed.

Definition 3.7.1. If $n \in \mathbb{P}$, then $d\,(n)$ is the number of divisors of n, and $D\,(n)$ is the sum of these divisors.

The first section of the following proof was inspired by [9].

Lemma 3.7.2. If $n \in \mathbb{P}$, then $d\,(n) \leq 24\sqrt[3]{n/315}$.

Proof. Let $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ be a prime factorisation of n, with $\alpha_i \in \mathbb{P}$ for all $i \in \mathbb{P}_r$. Then

$$d\,(n) = \prod_{i=1}^{r} (\alpha_i + 1)\,,$$

since each divisor of n is of the form $p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ for some $\beta_1, \beta_2, \dots, \beta_r \in \mathbb{N}$ with $\beta_i \leq \alpha_i$ for all $i \in \mathbb{P}_r$. It follows that

$$\frac{d\left(n\right)}{\sqrt[3]{n}} = \prod_{i=1}^{r} \frac{\alpha_i + 1}{p_i^{\alpha_i/3}}. \tag{3.1}$$

Now let $i \in \mathbb{P}_r$, and suppose that $p_i \geq 8$. Since $\alpha_i \geq 1$ and $\frac{1}{2} \leq \log\left(2\right)$,

$$\begin{aligned} \log\left(\alpha_i + 1\right) &= \int_1^{\alpha_i+1} \frac{dt}{t} = \int_1^2 \frac{dt}{t} + \int_2^{\alpha_i+1} \frac{dt}{t} \leq \int_1^2 \frac{dt}{t} + \int_2^{\alpha_i+1} \frac{dt}{2} \\ &= \log\left(2\right) + \frac{\alpha_i + 1 - 2}{2} \leq \log\left(2\right)\left(1 + \alpha_i - 1\right) = \log\left(2\right)\alpha_i \\ &= 3\log\left(2\right)\frac{\alpha_i}{3} = \log\left(8\right)\frac{\alpha_i}{3} \leq \log\left(p_i\right)\frac{\alpha_i}{3} = \log\left(p_i^{\alpha_i/3}\right). \end{aligned}$$

Therefore $\alpha_i + 1 \leq p_i^{\alpha_i/3}$, so $\frac{\alpha_i+1}{p_i^{\alpha_i/3}} \leq 1$. Otherwise $p_i < 8$. Define a function $f_i : \mathbb{R} \to \mathbb{R}$ by

$$f_i\left(x\right) = \frac{x+1}{p_i^{x/3}}$$

for all $x \in \mathbb{R}$. For each $x \in \mathbb{R}$, it follows from the quotient rule that

$$f_i'\left(x\right) = \frac{d}{dx}\frac{x+1}{p_i^{x/3}} = \frac{p_i^{x/3} - \left(x+1\right)p_i^{x/3}\log\left(p_i\right)/3}{p_i^{2x/3}} = \frac{1}{3p_i^{x/3}}\left(3 - \left(x+1\right)\log\left(p_i\right)\right).$$

Let $x_i = 3/\log\left(p_i\right) - 1$. Then $f_i'\left(x\right) > 0$ for all $x \in \left(-\infty, x_i\right)$ and $f_i'\left(x\right) < 0$ for all $x \in \left(x_i, \infty\right)$. By the Mean Value Theorem, $f_i|_{\mathbb{Z}}$ is maximised at $\lfloor x_i \rfloor$ or $\lceil x_i \rceil$. In particular $f_i\left(\alpha_i\right) \leq M_i$, where $M_i \coloneqq \max\left\{f_i\left(\lfloor x_i \rfloor\right), f_i\left(\lceil x_i \rceil\right)\right\}$ is given below.

p_i	$\lfloor x_i \rfloor$	$f_i\left(\lfloor x_i \rfloor\right)$	$\lceil x_i \rceil$	$f_i\left(\lceil x_i \rceil\right)$	M_i
2	3	2	4	$\frac{5}{\sqrt[3]{16}}$	2
3	1	$\frac{2}{\sqrt[3]{3}}$	2	$\frac{3}{\sqrt[3]{9}}$	$\frac{3}{\sqrt[3]{9}}$
5	0	1	1	$\frac{2}{\sqrt[3]{5}}$	$\frac{2}{\sqrt[3]{5}}$
7	0	1	1	$\frac{2}{\sqrt[3]{7}}$	$\frac{2}{\sqrt[3]{7}}$

To summarise, if $p_i \geq 8$ then the i^{th} term of (3.1) is at most 1; otherwise it is at most M_i. Since each prime appears at most once in (3.1),

$$\frac{d\left(n\right)}{\sqrt[3]{n}} = \prod_{i=1}^{r} \frac{\alpha_i + 1}{p_i^{\alpha_i/3}} \leq 2 \times \frac{3}{\sqrt[3]{9}} \times \frac{2}{\sqrt[3]{5}} \times \frac{2}{\sqrt[3]{7}} = \frac{24}{\sqrt[3]{315}}.$$

Therefore $d\left(n\right) \leq 24\sqrt[3]{n/315}$. □

Lemma 3.7.3. If $n \in \mathbb{P}$, then $D(n) < (4 + \log(n))\, n/2$.

Proof. Let $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } n\}$, $\Delta_1 = \{i \in \Delta \mid i < \sqrt{n}\}$ and $\Delta_2 = \{i \in \Delta \mid i \geq \sqrt{n}\}$. Then $i \leq N \coloneqq \lceil \sqrt{n} \rceil - 1$ for all $i \in \Delta_1$, so

$$\sum_{i \in \Delta_1} i \leq \sum_{i=1}^{N} i = \frac{N(N+1)}{2} = \frac{(\lceil \sqrt{n} \rceil - 1)\lceil \sqrt{n} \rceil}{2} < \frac{\sqrt{n}(\sqrt{n}+1)}{2} = \frac{n+\sqrt{n}}{2} \leq n.$$

Moreover, $n/i \in \mathbb{P}$ and $n/i \leq \sqrt{n}$, so that $n/i \leq \lfloor \sqrt{n} \rfloor$, for all $i \in \Delta_2$. It follows that

$$\begin{aligned}\sum_{i \in \Delta_2} i &= \sum_{i \in \Delta_2} \frac{n}{n/i} \leq \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n}{i} = n \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \int_{i-1}^{i} \frac{dt}{i} \leq n + n \sum_{i=2}^{\lfloor \sqrt{n} \rfloor} \int_{i-1}^{i} \frac{dt}{t} = n + n \int_{1}^{\lfloor \sqrt{n} \rfloor} \frac{dt}{t} \\ &= n + n \log\left(\lfloor \sqrt{n} \rfloor\right) \leq n + n \log\left(n^{\frac{1}{2}}\right) = n + \frac{n}{2}\log(n) = \frac{n}{2}(2 + \log(n)).\end{aligned}$$

Therefore $D(n) < n + (2 + \log(n))\, n/2 = (4 + \log(n))\, n/2$. □

Lemma 3.7.4. Let $n, p \in \mathbb{P}$ such that p is prime, $p^2 < n$ and each prime factor of n is larger than p. Then $d(np) \leq 48\sqrt[3]{n/315}$. Also let $\Gamma = \{i \in \mathbb{P}_n \mid i \text{ divides } np\}$. Then

$$\sum_{i \in \Gamma} i < \frac{4 + 2p + (\log(n) - 2\log(p))(1+p)}{2} n. \tag{3.2}$$

Proof. Each divisor of np is either k or kp for some $k \in \mathbb{P}$ with $k \mid n$. Since $p \nmid n$, these two cases never coincide. By Lemma 3.7.2, it follows that $d(np) = 2d(n) \leq 48\sqrt[3]{n/315}$. Furthermore, since np is the only divisor of np which lies outside $\mathbb{P}_n$,

$$\sum_{i \in \Gamma} i = D(n) + D(n)\, p - np = D(n)(1+p) - np.$$

Now let $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } n\}$, $\Delta_1 = \{i \in \Delta \mid i < \sqrt{n}\}$ and $\Delta_2 = \{i \in \Delta \mid i \geq \sqrt{n}\}$. Then $\sum_{i \in \Delta_1} i < n$, and $n/i \leq \lfloor \sqrt{n} \rfloor$ for all $i \in \Delta_2$, as shown in Lemma 3.7.3. Moreover, $n/i \geq p+1$ for all $i \in \Delta_2 \setminus \{n\}$, since each prime factor of n is at least $p+1$. Therefore

$$\begin{aligned}\sum_{i \in \Delta_2} i &= \sum_{i \in \Delta_2} \frac{n}{n/i} \leq n + \sum_{i=p+1}^{\lfloor \sqrt{n} \rfloor} \frac{n}{i} = n + n \sum_{i=p+1}^{\lfloor \sqrt{n} \rfloor} \int_{i-1}^{i} \frac{dt}{i} \leq n + n \sum_{i=p+1}^{\lfloor \sqrt{n} \rfloor} \int_{i-1}^{i} \frac{dt}{t} \\ &= n + n \int_{p}^{\lfloor \sqrt{n} \rfloor} \frac{dt}{t} = n + n\left(\log\left(\lfloor \sqrt{n} \rfloor\right) - \log(p)\right) \leq \frac{n}{2}(2 + \log(n) - 2\log(p)).\end{aligned}$$

It follows that $D(n) < (4 + \log(n) - 2\log(p))\, n/2$, and hence (3.2) holds. □

Lemma 3.7.5. Let $k, m, n \in \mathbb{P}$ and $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } mn\}$. If $k > 1$, then

$$\sum_{i\in\Delta} i^k < n^k \left(1 + \frac{m}{k-1}\right).$$

Proof. Suppose that $k > 1$. If $i \in \Delta$, then $i \leq n$ and hence $mn/i \geq m$. It follows that

$$\begin{aligned}\sum_{i\in\Delta} i^k &= \sum_{i\in\Delta}\left(\frac{mn}{mn/i}\right)^k \leq \sum_{i=m}^{mn}\left(\frac{mn}{i}\right)^k = n^k + (mn)^k \sum_{i=m+1}^{mn}\int_{i-1}^{i}\frac{dt}{i^k} \\ &\leq n^k + m^k n^k \sum_{i=m+1}^{mn}\int_{i-1}^{i}\frac{dt}{t^k} \leq n^k + m^k n^k \int_m^\infty \frac{dt}{t^k} \\ &= n^k + m^k n^k \left(\lim_{t\to\infty}\frac{1}{t^{k-1}(1-k)} - \frac{1}{m^{k-1}(1-k)}\right) \\ &= n^k + \frac{m^k n^k}{m^{k-1}(k-1)} = n^k\left(1 + \frac{m}{k-1}\right).\end{aligned}$$

□

Lemma 3.7.6. Let $k, n \in \mathbb{P}$, $m \in \mathbb{N}_n$ and $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } k(n-m)\}$. Suppose that $n - m \geq km$. Then $M := \max\Delta = n - m$.

Proof. Suppose that $M \neq n - m$. Then $M > n - m$ since $n - m \in \Delta$. Now suppose that $c := \gcd(M, n-m) > m$. Then

$$\frac{n-m}{c}c = n - m < M \leq n = \frac{n-m}{c}c + m < \left(\frac{n-m}{c} + 1\right)c,$$

which is a contradiction because there is no integer between $\frac{n-m}{c}$ and $\frac{n-m}{c} + 1$, but c divides M. Therefore $c \leq m$, so $m \neq 0$ and hence

$$k(n-m) \geq \operatorname{lcm}(M, n-m) = \frac{M(n-m)}{c} \geq \frac{Mkm}{m} > (n-m)k.$$

This is clearly a contradiction, so $M = n - m$. □

Lemma 3.7.7. Let $n \in \mathbb{P}$ and $k \in \mathbb{P}_n \setminus \{1\}$. Then there are $\frac{n!}{k(n-k)!}$ cycles of length k in S_n. If $m \in \mathbb{P}$ and $2 \leq n - m \leq n - k$ then there are $\frac{n!}{k(n-m)(m-k)!}$ permutations in S_n composed of (disjoint) cycles of length k and $n - m$. The same holds for A_n provided that $k - 1$ (respectively $n - m + k$) is even.

Proof. Let $k \in \mathbb{P}_n \setminus \{1\}$. There are $\binom{n}{k}$ choices for the support of a k-cycle, and $(k-1)!$ cycles with a given support. Hence there are

$$\binom{n}{k}(k-1)! = \frac{n!\,(k-1)!}{k!\,(n-k)!} = \frac{n!}{k\,(n-k)!} \tag{3.3}$$

cycles of length k in S_n. Now let $m \in \mathbb{P}$, and suppose that $k \leq n-m$. Given a k-cycle $x \in S_n$, the number of cycles of length $n-m$ in S_n which fix $\operatorname{supp}(x)$ is the same as the number of cycles of length $n-m$ in S_{n-k}, which is $\frac{(n-k)!}{(n-m)(m-k)!}$ according to (3.3). Therefore

$$\frac{n!}{k\,(n-k)!}\frac{(n-k)!}{(n-m)\,(m-k)!} = \frac{n!}{k\,(n-m)\,(m-k)!}$$

is the number of permutations in S_n composed of cycles of length k and $n-m$. A k-cycle has parity $(k-1)$ mod 2, and an element composed of cycles of length k and $n-m$ has parity $(k+n-m-2)$ mod 2. These are 0 if and only if $k-1$ (respectively $k+n-m$) is even. □

Theorem 3.7.8. Let $m \in \mathbb{N}$. For every $\varepsilon \in (0,\infty)$ there exists $N \in \mathbb{P}$ such that, for all $n \in \mathbb{P}$ with $n \geq N$, the number of permutations $g \in S_n$ such that $g^{m!(n-m)} = 1$ is less than $(n-1)!\,(1+\varepsilon)$.

Proof. Let $\varepsilon \in (0,\infty)$, and assume $\varepsilon < 3$ without loss of generality. Also let $k, N \in \mathbb{P}$ be such that $k \geq \frac{6m!}{\varepsilon}+2$ and $N \geq \max\left\{\left(\frac{78k^k m!}{\varepsilon}\right)^3, k\left(1-\left(\frac{3}{3+\varepsilon}\right)^{\frac{1}{k-1}}\right)^{-1}, \sqrt{44m!}, (m!+1)\,m\right\}$. Let $n \in \mathbb{P}$ with $n \geq N \geq k \geq 3$. Consider $g \in S_n$ with $g^{m!(n-m)} = 1$, and let X be the cycle structure of g. Then $\mathcal{P} \coloneqq \{\operatorname{supp}(x) \cap \mathbb{P}_k \mid x \in X\} \setminus \{\varnothing\} \cup \{\{\sigma\} \mid \sigma \in \operatorname{fix}(g) \cap \mathbb{P}_k\}$ is a partition of $\mathbb{P}_k$ into non-empty sets. Let $s = |\mathcal{P}|$, and write $\mathcal{P} = \{P_1, P_2, \ldots, P_s\}$. For each $i \in \mathbb{P}_s$ there exists $a_i \in \mathbb{P}$ such that either $a_i \geq 2$ and $P_i = \operatorname{supp}(x_i) \cap \mathbb{P}_k$ for some cycle $x_i \in X$ of length a_i, or $a_i = |P_i| = 1$ and $P_i \subseteq \operatorname{fix}(g)$. Therefore g is among the

$$M^{a_1,a_2,\ldots,a_s}_{P_1,P_2,\ldots,P_s} \coloneqq \left(n - \sum_{j=1}^{s} a_j\right)! \prod_{i=1}^{s}\left(\binom{n-k-\sum_{j=1}^{i-1}(a_j-|P_j|)}{a_i-|P_i|}(a_i-1)!\right) \tag{3.4}$$

elements of S_n with the above property. More precisely, $M^{a_1,a_2,\ldots,a_s}_{P_1,P_2,\ldots,P_s}$ counts those $h \in S_n$ such that, for every $i \in \mathbb{P}_s$, if $a_i \geq 2$ then h contains an a_i-cycle x_i such that $P_i = \operatorname{supp}(x_i) \cap \mathbb{P}_k$, and otherwise (when $a_i = |P_i| = 1$) $P_i \subseteq \operatorname{fix}(h)$. To check this, compare the product terms in (3.4) with the first term in (3.3). If $i \in \mathbb{P}_s$ and $a_i \geq 2$, then the number of choices for $\operatorname{supp}(x_i)$ is restricted by the fact that all k elements of $\mathbb{P}_k$ are unavailable, so we need only choose $a_i - |P_i|$ of the remaining $n-k$ elements. However, $\sum_{j=1}^{i-1}(a_j - |P_j|)$ of these elements have been assigned to the preceding cycles. If $a_i = 1$, then $a_i - |P_i| = 0$ and the i^{th} product term in (3.4) is just 1, as required. The first term in (3.4) is the number of permutations of the remaining points of $\mathbb{P}_n$. Note that

$$\begin{aligned} M_{P_1,P_2,\ldots,P_s}^{a_1,a_2,\ldots,a_s} &= \left(n - \sum_{j=1}^{s} a_j\right)! \prod_{i=1}^{s} \left(\frac{\left(n-k-\sum_{j=1}^{i-1}(a_j - |P_j|)\right)!\,(a_i-1)!}{(a_i - |P_i|)!\left(n-k-\sum_{j=1}^{i}(a_j-|P_j|)\right)!} \right) \\ &= \left(n - \sum_{j=1}^{s} a_j\right)! \frac{(n-k)!}{\left(n-k-\sum_{j=1}^{s}(a_j-|P_j|)\right)!} \prod_{i=1}^{s} \frac{(a_i-1)!}{(a_i-|P_i|)!} \\ &= (n-k)! \prod_{i=1}^{s} \frac{(a_i-1)!}{(a_i-|P_i|)!} \leq (n-k)! \prod_{i=1}^{s} a_i^{|P_i|-1}. \end{aligned}$$

Define $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } m!\,(n-m)\}$. Since $\operatorname{supp}\left(g^{m!(n-m)}\right) = \operatorname{supp}(1) = \varnothing$, the length of each $x \in X$ divides $m!\,(n-m)$. Therefore $a_1, a_2, \ldots, a_s \in \Delta$, and the number of possibilities for $g \in S_n$ with $g^{m!(n-m)} = 1$ is less than

$$M := \sum (n-k)! \prod_{i=1}^{s} a_i^{|P_i|-1}, \tag{3.5}$$

where the sum is over all $s \in \mathbb{P}_k$, partitions $\{P_1, P_2, \ldots, P_s\}$ of $\mathbb{P}_k$ and $a_1, a_2, \ldots, a_s \in \Delta$. By Lemma 3.7.6 $\Delta \subseteq \mathbb{P}_{n-m}$, so by Lemma 3.7.5 the contribution made to (3.5) by $\{\mathbb{P}_k\}$ is

$$(n-k)! \sum_{i\in\Delta} i^{k-1} < (n-k)!\,(n-m)^{k-1}\left(1 + \frac{m!}{k-2}\right) \leq (n-k)! n^{k-1}\left(1 + \frac{m!}{k-2}\right).$$

Let $\mathcal{P}$ be another partition of $\mathbb{P}_k$, and write $\mathcal{P} = \{P_1, P_2, \ldots, P_s\}$ where $s := |\mathcal{P}| \in \mathbb{P}_k \setminus \{1\}$. By Lemma 3.7.2 $|\Delta| \leq d\,(m!\,(n-m)) \leq 24\sqrt[3]{m!\,(n-m)/315} \leq (44m!\,(n-m))^{\frac{1}{3}}$, so the number of sequences $a_1, a_2, \ldots, a_s \in \Delta$ is at most $(44m!\,(n-m))^{\frac{s}{3}}$. For such a sequence

$$\prod_{i=1}^{s} a_i^{|P_i|-1} \leq \prod_{i=1}^{s} n^{|P_i|-1} = n^{\sum_{i=1}^{s}(|P_i|-1)} = n^{k-s} = \frac{n^k}{n^s}.$$

Since $n^2 \geq 44m!$, the contribution made to (3.5) by $\mathcal{P}$ is at most $(n-k)!$ times

$$(44m!\,(n-m))^{\frac{s}{3}} \frac{n^k}{n^s} \leq \left(\frac{44m!n}{n^3}\right)^{\frac{s}{3}} n^k \leq \left(\frac{44m!}{n^2}\right)^{\frac{2}{3}} n^k < 13m!n^{k-\frac{4}{3}}.$$

As $\mathbb{P}_k$ is finite, there exists a function $f : \mathcal{P} \to \mathbb{P}_k$ such that $f(P) \in P$ for all $P \in \mathcal{P}$. If $i \in \mathbb{P}_k$ then there is a unique $P_i \in \mathcal{P}$ such that $i \in P_i$, so $i \mapsto f(P_i)$ is a well-defined mapping of $\mathbb{P}_k$ to itself. Define a relation $\sim$ on $\mathbb{P}_k \times \mathbb{P}_k$ by $i \sim j$ if and only if $f(P_i) = f(P_j)$. This clearly an equivalence relation and $\mathcal{P}$ is the corresponding set of equivalence classes. Every function mapping $\mathbb{P}_k$ to itself determines (in this way) a unique partition of $\mathbb{P}_k$, so the number of partitions of $\mathbb{P}_k$ is at most k^k, the number of functions mapping $\mathbb{P}_k$ to itself. It follows that

$$\begin{aligned} M &< (n-k)!\left(n^{k-1}\left(1+\frac{m!}{k-2}\right)+13k^k m!n^{k-\frac{4}{3}}\right) \\ &< (n-1)!\left(\frac{n}{n-k}\right)^{k-1}\left(1+\frac{m!}{k-2}+13k^k m!n^{-\frac{1}{3}}\right), \end{aligned}$$

where the second inequality follows from the fact that

$$(n-k)!n^{k-1} = (n-1)!\prod_{i=1}^{k-1}\frac{n}{n-i} < (n-1)!\prod_{i=1}^{k-1}\frac{n}{n-k} = (n-1)!\left(\frac{n}{n-k}\right)^{k-1}.$$

By the definitions of k and N

$$\frac{m!}{k-2}+\frac{13k^k m!}{n^{\frac{1}{3}}} \leq \frac{m!}{\frac{6m!}{\varepsilon}+2-2}+\frac{13k^k m!\varepsilon}{78k^k m!} = \frac{\varepsilon}{6}+\frac{\varepsilon}{6} = \frac{\varepsilon}{3},$$

and likewise $\left(\frac{n}{n-k}\right)^{k-1} \leq 1+\frac{\varepsilon}{3}$ because

$$\frac{n}{n-k} = \frac{1}{1-\frac{k}{n}} \leq \frac{1}{1-\left(1-\left(\frac{3}{3+\varepsilon}\right)^{\frac{1}{k-1}}\right)} = \left(\frac{3+\varepsilon}{3}\right)^{\frac{1}{k-1}} = \left(1+\frac{\varepsilon}{3}\right)^{\frac{1}{k-1}}.$$

Therefore

$$M < (n-1)!\left(1+\frac{\varepsilon}{3}\right)\left(1+\frac{\varepsilon}{3}\right) = (n-1)!\left(1+\frac{2\varepsilon}{3}+\frac{\varepsilon^2}{3^2}\right) < (n-1)!\,(1+\varepsilon).$$

□

This result effectively states that, for sufficiently large degrees, there is an arbitrarily high probability that a permutation which is 1 when raised to a certain power has a certain cycle structure. The following corollary formalises this idea. Unfortunately, the degrees required by this result are too high to be of practical use. However, the idea behind the proof can be used to obtain a reasonable bound for most degrees.

Corollary 3.7.9. Let $m \in \mathbb{N}$. For all $\varepsilon \in (0, \infty)$ there exists $N \in \mathbb{P}$ such that, for all $n \in \mathbb{P}$ with $n \geq N$ and $\frac{n}{2} > m$, the proportion of permutations $g \in S_n$ that contain a cycle of length $n - m$, among those for which $g^{m!(n-m)} = 1$, is greater than $1 - \varepsilon$.

Proof. Let $\varepsilon \in (0, \infty)$, and take N from Theorem 3.7.8. Also let $n \in \mathbb{P}$ with $n \geq N$ and $\frac{n}{2} > m$. Then the number of permutations $g \in S_n$ such that $g^{m!(n-m)} = 1$ is less than $(n-1)!\,(1+\varepsilon)$. By Lemma 2.4.1, the number that contain a cycle of length $n - m$ is $\frac{n!}{n-m}$. Let $g \in S_n$ be such a permutation. Then the other cycles contained in g each have length at most m, and hence $g^{m!(n-m)} = 1$. Therefore the proportion of such elements among those $g \in S_n$ with $g^{m!(n-m)} = 1$ is greater than

$$\frac{n!/\,(n-m)}{(n-1)!\,(1+\varepsilon)} = \frac{n}{n-m}\left(1 - \frac{\varepsilon}{1+\varepsilon}\right) > 1\left(1 - \frac{\varepsilon}{1}\right) = 1 - \varepsilon.$$

□

Corollary 3.7.10. Let $k, m \in \mathbb{P}$ be such that $2 \leq k \leq m$. For all $\varepsilon \in (0, \infty)$ there exists $N \in \mathbb{P}$ such that, for all $n \in \mathbb{P}$ with $n \geq N$ and $\frac{n}{2} > m$, the proportion of permutations $g \in S_n$ that are composed of (disjoint) cycles of length k and $n - m$, among those for which $g^{k(n-m)} = 1$, is greater than $\frac{1-\varepsilon}{m!}$.

Proof. Let $\varepsilon \in (0, \infty)$, and take N from Theorem 3.7.8. Also let $n \in \mathbb{P}$ with $n \geq N$ and $\frac{n}{2} > m$. Then the number of permutations $g \in S_n$ such that $g^{m!(n-m)} = 1$ is less than $(n-1)!\,(1+\varepsilon)$. If $g \in S_n$ and $g^{k(n-m)} = 1$, then $g^{m!(n-m)} = 1$ since $k \leq m$. So the number of such elements in S_n is also less than $(n-1)!\,(1+\varepsilon)$. By Lemma 3.7.7, the number of permutations $g \in S_n$ that are composed of cycles of length k and $n - m$ is $\frac{n!}{k(n-m)(m-k)!}$, and all of these clearly satisfy $g^{k(n-m)} = 1$. Therefore the proportion of such elements among those $g \in S_n$ with $g^{k(n-m)} = 1$ is greater than

$$\frac{n!/k\,(n-m)\,(m-k)!}{(n-1)!\,(1+\varepsilon)} = \frac{n}{(n-m)}\left(1 - \frac{\varepsilon}{1+\varepsilon}\right)\frac{1}{k\,(m-k)!} > \frac{1-\varepsilon}{m!}.$$

□

We now give more practical bounds for these proportions, by using ideas from the proof of Theorem 3.7.8. Our results are not valid for small degrees, so we first describe an algorithm which can be used to calculate these exactly.

Algorithm 13 $NumberOfPermutations\,(n,p)$.

```
$C := [1,1]$ ;

for $m := 2$ to $n$ do
    $N := 1$;
    $s := 1$;

    for $l := 2$ to $m$ do
        $s := s\,(m-l+2)$ ;

        if $l \mid p$ then
            $c := s$;
            for $i := 1$ to $m-l+1$ do
                $c := \frac{c(m-i-l+2)}{m-i+1}$;
                $N := N + cC_{m-i-l+2}$;
            end for;
        end if;
    end for;

    $Append(C, N)$;
end for;

return $C_{n+1}$;
```

Lemma 3.7.11. Given $n, p \in \mathbb{P}$, Algorithm 13 returns the number of permutations $g \in S_n$ which satisfy $g^p = 1$.

Proof. The algorithm constructs a list C such that, for each $m \in \mathbb{P}_n$, C_{m+1} is the number of permutations $g \in S_m$ which satisfy $g^p = 1$. Pass m of the outer loop aims to calculate C_{m+1}. Every permutation in S_m is composed of disjoint cycles, which can be ordered as described in Lemma 3.3.2. The outer loop initially sets N to 1, to count the identity permutation. It then adds to this, for each $l \in \mathbb{P}_m$, the number of permutations $g \in S_m$ which satisfy $g^p = 1$ and start with a cycle of length l. If $l = 1$ or l does not divide p there are no permutations with these properties. Otherwise, the number depends on the least element $i \in \mathbb{P}_n$ of the first cycle. This is clearly less than $m - l$. The variable s is continually updated to hold $\frac{m!}{(m-l+1)!}$, and similarly $c = \frac{(m-i)!}{(m-i-l+1)!}$ holds the number of sequences of length $l - 1$ in $\mathbb{P}_{m-i}$. Equivalently, c is the number of cycles of $x \in S_m$ of length l such that i is the least element of $\operatorname{supp}(x)$. Every permutation $g \in S_m$ which satisfies $g^p = 1$ and starts with such a cycle x consists of x composed with a permutation $h \in S_m|_{\{i,i+1,\ldots,m\}\setminus\operatorname{supp}(x)}$ such that $h^p = 1$. Conversely, every such composition gives a permutation $g \in S_m$ which satisfies $g^p = 1$ and starts with x. Since $|\{i, i+1, \ldots, m\} \setminus \operatorname{supp}(x)| = m - i - l + 1$, the count N is updated correctly on line 14. □

Lemma 3.7.12. Let $n \in \mathbb{P}$ and $m \in \mathbb{N}_2$ be such that $n \geq 5$ and $n - m$ is odd. The proportion of cycles of length $n - m$ among permutations $g \in S_n$ for which $g^{n-m} = 1$ is at least $\frac{2}{5}$.

Proof. Define $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } n - m\}$. Using (3.5) for the special case $k = 3$, the number of permutations $g \in S_n$ with $g^{n-m} = 1$ is less than

$$M \coloneqq \sum (n-3)! \prod_{i=1}^{s} a_i^{|P_i|-1},$$

where the sum is over all $s \in \mathbb{P}_3$, partitions $\{P_1, P_2, \ldots, P_s\}$ of $\mathbb{P}_3$ and $a_1, a_2, \ldots, a_s \in \Delta$. If $s = 3$ then there is only one partition of $\mathbb{P}_3$ of size s, namely $\{\{1\}, \{2\}, \{3\}\}$. The number of sequences $a_1, a_2, a_3 \in \Delta$ is at most $44(n-m) \leq 44n$, by Lemma 3.7.2. So the contribution made to M by this partition is at most $44(n-3)!n$, since the product terms are all raised to the power of 0. Each of the three partitions of size 2 contributes at most

$$(n-3)!D(n-m)\,d(n-m) < (n-3)!\frac{4+\log(n)}{2}n\sqrt[3]{44n} < 2n^{\frac{4}{3}}(n-3)!(4+\log(n))$$

to M, by Lemmas 3.7.2 and 3.7.3. The remaining partition $\{\mathbb{P}_3\}$ contributes less than

$$(n-3)!n^2\left(1+\frac{1}{2-1}\right) = 2n^2(n-3)!$$

to M, by Lemma 3.7.5. It follows that

$$M < (n-3)!\left(44n + 6n^{\frac{4}{3}}\left(4 + \log(n)\right) + 2n^2\right).$$

Define a function $f : (2, \infty) \to \mathbb{R}$ by

$$f(x) = \frac{44x + 6x^{\frac{4}{3}}\left(4 + \log(x)\right) + 2x^2}{(x-1)(x-2)}$$

for all $x \in (2, \infty)$. It can be shown, via the Mean Value Theorem, that f is decreasing on $[5000, \infty)$. Hence by Lemma 3.7.7, if $n > 5000$ the proportion of cycles of length $n - m$ among permutations $g \in S_n$ for which $g^{n-m} = 1$ is at least

$$\frac{n!}{M(n-m)\,m!} > \frac{n!}{(n-1)!f(n)(n-m)} \geq \frac{n}{f(5000)(n-m)} \geq f(5000)^{-1} > \frac{2}{5}.$$

An exact calculation of this proportion using Algorithm 13 shows that for $5 \leq n \leq 5000$ the minimum occurs when $n = 9$. This proportion, namely $\frac{4480}{5121}$, is larger than $\frac{2}{5}$. □

Lemma 3.7.13. Let $n \in \mathbb{P}$ and $m \in \mathbb{P}_n$ be such that $n \geq 5$ and $3 \leq m \leq 6$ as small as possible such that $n - m$ is not divisible by 2 or 3. The proportion of permutations $g \in S_n$ that are composed of (disjoint) cycles of length 3 and $n - m$, among those for which $g^{3(n-m)} = 1$, is at least $\frac{1}{100}$.

Proof. First, suppose that $n \geq 24$. Define $\Delta = \{i \in \mathbb{P}_n \mid i \text{ divides } 3(n-m)\}$. Using (3.5) for the special case $k = 3$, the number of permutations $g \in S_n$ with $g^{3(n-m)} = 1$ is less than

$$M := \sum (n-3)! \prod_{i=1}^{s} a_i^{|P_i|-1},$$

where the sum is over all $s \in \mathbb{P}_3$, partitions $\{P_1, P_2, \ldots, P_s\}$ of $\mathbb{P}_3$ and $a_1, a_2, \ldots, a_s \in \Delta$. If $s = 3$ then there is only one partition of $\mathbb{P}_3$ of size s, namely $\{\{1\}, \{2\}, \{3\}\}$. Since $n - m$ is not divisible by 2 or 3, the number of sequences $a_1, a_2, a_3 \in \Delta$ is at most $352(n-m) \leq 352n$, by Lemma 3.7.4. So the contribution made to M by this partition is at most $352(n-3)!n$. As $n - m \geq n - 6 \geq 18$, Lemma 3.7.6 implies that $\Delta \subseteq \mathbb{P}_{n-m}$. Hence by Lemma 3.7.4, the three partitions of size 2 contribute at most

$$\begin{aligned} 3d(n-m)(n-3)!\sum_{i\in\Delta} i &< 3\sqrt[3]{352n}\,(n-3)!\frac{4+6+4\left(\log(n-m) - 2\log(3)\right)}{2}(n-m) \\ &< \sqrt[3]{9504n}\,(n-3)!\left(5 - 4\log(3) + 2\log(n)\right)n \\ &< 22n^{\frac{4}{3}}(n-3)!\left(1 + 2\log(n)\right) \end{aligned}$$

to M. The remaining partition $\{\mathbb{P}_3\}$ contributes less than

$$(n-3)!\,(n-m)^2\left(1+\frac{3}{2-1}\right) < 4n^2\,(n-3)!$$

to M, by Lemmas 3.7.6 and 3.7.5. It follows that

$$M < (n-3)!\left(352n + 22n^{\frac{4}{3}}\,(1+2\log(n)) + 4n^2\right).$$

Define a function $f : (2,\infty) \to \mathbb{R}$ by

$$f(x) = \frac{352x + 22x^{\frac{4}{3}}\,(1+2\log(x)) + 4x^2}{(x-1)\,(x-2)}$$

for all $x \in (2,\infty)$. It can be shown, via the Mean Value Theorem, that f is decreasing on $[5000,\infty)$. Hence by Lemma 3.7.7, if $n > 5000$ the proportion of permutations $g \in S_n$ that are composed of cycles of length 3 and $n-m$, among those for which $g^{3(n-m)} = 1$, is at least

$$\frac{n!}{3M\,(n-m)\,(m-3)!} > \frac{n!}{3\,(n-1)!f(n)\,(n-m)\,3!} > \frac{f(5000)^{-1}}{18} > \frac{1}{100}.$$

An exact calculation of this proportion using Algorithm 13 shows that for $5 \le n \le 5000$ the minimum occurs when $n = 31$. This proportion, namely

$$\frac{891228765715570221907968}{6021030439189582986154675},$$

is larger than $\frac{1}{100}$. □

Lemma 3.7.14. Let G be a group isomorphic to A_n or S_n for some $n \in \mathbb{P}$ with $n \ge 5$. Given n and a process R for generating random elements of G, Algorithm 14 returns alternating n-generators within G with probability at least $\frac{1}{400}$.

Proof. It is clear that k and m are initialised to satisfy the requirements for m in Lemmas 3.7.12 and 3.7.13 respectively. By Lemma 3.7.7, the proportion of cycles of length $n-k$ in S_n, thus A_n, is at least $\frac{1}{n}$. In particular, the proportion of elements $g \in G$ which satisfy $g^{n-k} = 1$ is at least $\frac{1}{n}$. It follows that the probability that the algorithm fails to find such an element is at most $\left(1-\frac{1}{n}\right)^{2n}$. Similarly, the proportion of elements $g \in G$ which satisfy $g^{3(n-m)} = 1$ is at least $\frac{1}{18n}$, and the probability that the algorithm

Algorithm 14 *FindAltGenerators* (R, n) .

```
$k := 1 - (n \bmod 2)$;
$m := n \bmod 6$;

if $m \leq 1$ then
    $m := m + 5$;
else if $m \leq 3$ then
    $m := m + 1$;
else
    $m := m - 1$;
end if;

$a := 1$;
$c := 1$;

for $r := 1$ to $2n$ do
    $g := Random(R)$;
    if $g^{n-k} = 1$ then
        $a := g$;
        break;
    end if;
end for;

for $r := 1$ to $36n$ do
    $g := Random(R)$;
    if $g^{3(n-m)} = 1$ then
        $c := g$;
        break;
    end if;
end for;
```

Algorithm 14 $FindAltGenerators\,(R, n)$ (continued).

```
$b := c^{n-m}$;

if $IsOdd\,(n)$ then
    $s, t := FindOddGenerators\,(R, n, a, b)$;
    if $CheckOddGenerators\,(n, s, t)$ then
        return $s, t$;
    end if;
else
    $s, t := FindEvenGenerators\,(R, n, a, b)$;
    if $CheckEvenGenerators\,(n, s, t)$ then
        return $s, t$;
    end if;
end if;

return $1, 1$;
```

fails to find such an element is at most $\left(1 - \frac{1}{18n}\right)^{36n}$. Both of these probabilities are bounded above by $e^{-2} < \frac{1}{7}$, so the chance that both succeed is at least $\left(\frac{6}{7}\right)^2$. When this occurs, the probability that a is a cycle of length $n-k$ is at least $\frac{2}{5}$ by Lemma 3.7.12. Moreover, Lemma 3.7.13 implies that the probability that c is composed of cycles of length 3 and $n-m$ is at least $\frac{1}{100}$. When these conditions all hold, the chance that the appropriate choice of Algorithm 11 or 12 succeeds is at least $1 - e^{-2} > \frac{6}{7}$. Therefore, the probability that the algorithm succeeds is at least $\left(\frac{6}{7}\right)^3 \frac{2}{500} \geq \frac{1}{400}$. □

Theorem 3.7.15. Given a finitely-generated group G, a constant $\varepsilon \in (0,1)$, and $n \in \mathbb{N}$ with $n \geq 11$, Algorithm 15 determines whether $G \simeq A_n$ or $G \simeq S_n$ with probability at least $1 - \varepsilon$. If it determines that $G \simeq A_n$, via some isomorphism $\theta : G \to A_n$, the algorithm returns functions to compute θ and θ^{-1}. Likewise, if the algorithm finds that $G \simeq S_n$, via some isomorphism $\theta : G \to S_n$, it returns functions to compute θ and θ^{-1}.

Proof. Suppose that G is isomorphic to A_n or S_n. The probability that none of $c \in \mathbb{P}$ calls to Algorithm 14 succeed is $\left(\frac{399}{400}\right)^c$, which is less than ε provided that $\log_{\frac{399}{400}}(\varepsilon) < c$.

Algorithm 15 *ConstructiveRecognition* (G, n, ε) .

```
$s \coloneqq 1$;
$t \coloneqq 1$;

$R \coloneqq RandomProcess\,(G)$ ;
$c \coloneqq \left\lceil \log_{\frac{399}{400}} (\varepsilon) \right\rceil$ ;

while $s = 1$ or $t = 1$ do
    $s, t \coloneqq FindAltGenerators\,(R, n)$ ;
    $c \coloneqq c - 1$;
    if $c \leq 0$ then
        return false;
    end if;
end while

$E \coloneqq \left[ \begin{cases} t, & \textbf{if } j = 0 \\ \left(E_j^s\right)^{2-(n \bmod 2)}, & \textbf{otherwise} \end{cases} \middle| \; j \in [0, \ldots, 8] \right]$ ;
$X \coloneqq DomainCover\,(n, s, t, E)$ ;

$o \coloneqq$ false;
for $g \in Generators\,(G)$ do
    $b \coloneqq Sym\,(n)!ElementToPermutation\,(n, s, t, E, X, g)$ ;
    on failure: return false;

    if not $o$ and $IsOdd\,(b)$ then
        $o \coloneqq$ true;
        $c \coloneqq (1\ 2)\,b$;
        $h \coloneqq EvenPermutationToElement(n, s, t, c)$;

        $t' \coloneqq hg^{-1}$;
        $s' \coloneqq (t')^{(n+1) \bmod 2}\,st$;
    end if;
```

Algorithm 15 *ConstructiveRecognition* (G, n, ε) (continued).

```
    if $o$ then
        $h := PermutationToElement(n, s', t', b)$;
    else
        $h := EvenPermutationToElement(n, s, t, b)$;
    end if;

    if $h \neq g$ then
        return false;
    end if;
end for;

if $o$ then
    $\theta : g \mapsto Sym\,(n)!ElementToPermutation\,(n, s, t, E, X, g)\,$;
    $\phi : b \mapsto PermutationToElement(n, s', t', b)$;
    return true, $o, \theta, \phi$;
else
    $\theta : g \mapsto Alt(n)!ElementToPermutation\,(n, s, t, E, X, g)\,$;
    $\phi : b \mapsto EvenPermutationToElement(n, s, t, b)$;
    return true, $o, \theta, \phi$;
end if;
```

If one does, it returns alternating n-generators s and t within G, which induce a monomorphism $\theta : G \to S_n$. It is easy to check that the list E gives the initial 9 elements of $\langle s, t \rangle$. The next step constructs g^θ for each generator $g \in G$, and if one of these permutations is odd the algorithm computes symmetric n-generators s' and t' within G. When this occurs $G \simeq S_n$, and the correct algorithms to compute θ and θ^{-1} are returned. Otherwise $G \leq \langle s, t \rangle$, so $G \simeq A_n$ and the corresponding algorithms are returned correctly.

Conversely, if G is not isomorphic to A_n or S_n then the algorithm cannot possibly succeed, since the test on line 37 requires that each generator of G lies in $\langle s, t \rangle$ or $\langle s', t' \rangle$ for some alternating (symmetric) n-generators s and t (s' and t') within G. □

Algorithm 15 only works for degrees at least 11, but it is easily modified to account for those between 5 and 10, by replacing calls to Algorithm 9 with calls to Algorithm 10, removing the call to Algorithm 6, and only computing the initial 3 elements of $\langle s, t \rangle$.

3.8 Performance

The algorithms we have described have the same asymptotic performance as the corresponding ones described in [6]. However, their actual running time can vary substantially depending on the care taken to implement them. We have prepared an implementation for the Magma computer algebra system [10]. This implementation, available at [11], works for groups of degree at least 5. The algorithms employed are essentially the same as those described in this chapter, but have been optimised substantially (trading readability for speed). Moreover, the implementation of Algorithm 15 produces two additional functions. The first of these takes an element of the black-box group G and returns it as a word in the generators of G; the second takes a word in the generators of G and returns the corresponding element.

We have compared the performance of our implementation with that of the built-in Magma function `RecogniseAlternatingOrSymmetric` [12, p. 1818]. Our implementations of Algorithms 15 and 9 tend to be faster than their built-in equivalents, although Algorithms 4 and 5 seem to take slightly longer to complete. The latter algorithms are much faster than the others, so their performance is not as important. Our implementation of Algorithm 9 does less than the built-in equivalent, which is able to test for membership in the black-box group G. However, extending it would only require one call to Algorithm 4 or 5, and one equality test within G, the running times of which are far smaller than that of Algorithm 9 itself.

Listed below are the average running times (in seconds) we obtained by running each algorithm three times on a variety of input groups, and randomly generated elements of these groups. The same random elements were used as input to each implementation of Algorithm 9, although different elements were used for each of the three repeated tests; the resulting permutations were passed back to the appropriate implementation of Algorithm 4 or 5. This process was automated, and the program we used to perform it can be found at [13]. We used Magma version 2.18-8 on a computer with an AMD Opteron 880 processor clocked at 2.4 GHz.

		Algorithm			Built-in equivalent		
Input group	Parent	15	9	4/5	15	9	4/5
A_{100}	S_{100}	0.10	0.04	0.01	0.80	0.21	0.00
A_{101}	S_{101}	0.08	0.04	0.01	0.82	0.22	0.00
S_{100}	S_{100}	0.10	0.04	0.00	0.81	0.21	0.01
S_{101}	S_{101}	0.08	0.04	0.00	0.83	0.22	0.00
A_{100}	$\mathrm{GL}\,(99,3)$	1.52	0.52	0.06	2.83	0.81	0.03
A_{101}	$\mathrm{GL}\,(100,3)$	1.56	0.51	0.07	2.70	0.91	0.03
S_{100}	$\mathrm{GL}\,(99,3)$	2.53	0.51	0.04	5.60	0.80	0.02
S_{101}	$\mathrm{GL}\,(100,3)$	2.17	0.51	0.03	2.74	0.88	0.04
A_{100}	$\mathrm{GL}\,(99,37)$	75.26	47.78	2.64	104.47	48.18	1.38
A_{101}	$\mathrm{GL}\,(100,37)$	50.65	33.00	1.33	65.46	34.14	0.93
S_{100}	$\mathrm{GL}\,(99,37)$	79.34	47.49	1.15	110.62	48.23	1.52
S_{101}	$\mathrm{GL}\,(100,37)$	80.65	37.96	0.99	90.14	41.85	1.23

References

[1] Seress Á. *Permutation group algorithms.* Cambridge: Cambridge University Press; 2003.

[2] Dixon JD, Mortimer B. *Permutation groups.* New York: Springer-Verlag; 1996.

[3] Jordan C. Théorèmes sur les groupes primitifs. *Journal de Mathématiques Pures et Appliquées* 1871; 16: 383-408.

[4] Dixon JD. *Errata for Dixon and Mortimer "PERMUTATION GROUPS".*
`http://people.math.carleton.ca/~jdixon/Errata.pdf`
(accessed 28 September 2012).

[5] Wielandt H. *Finite permutation groups.* New York-London: Academic Press; 1964.

[6] Beals R, Leedham-Green CR, Niemeyer AC, Praeger CR, Seress Á. A black-box group algorithm for recognizing finite symmetric and alternating groups, I. *Transactions of the American Mathematical Society* 2003; 355(5): 2097-2113.

[7] Carmichael RD. Abstract definitions of the symmetric and alternating groups and certain other permutation groups. *Quarterly Journal of Pure and Applied Mathematics* 1922; 49: 226-283.

[8] Coxeter HSM, Moser WOJ. *Generators and relations for discrete groups.* Berlin-Göttingen-Heidelberg: Springer-Verlag; 1957.

[9] Tao T. *The divisor bound.*
`http://terrytao.wordpress.com/2008/09/23/the-divisor-bound/`
(accessed 4 October 2012).

[10] Bosma W, Cannon J, Playoust C. The Magma algebra system. I. The user language. *Journal of Symbolic Computation* 1997; 24: 235-265.

[11] `http://www.math.auckland.ac.nz/~obrien/cr.m`

[12] Bosma W, Cannon J, Fieker C, Steel A (eds.). *Handbook of Magma functions*, Edition 2.18. Sydney; 2011.

[13] `http://www.math.auckland.ac.nz/~obrien/test.m`