PHD

Related elements in groups

Puttock, Richard

Award date:
2004

Awarding institution:
University of Bath

Related elements in groups

submitted by

Richard Puttock

for the degree of Ph.D.

of the

University of Bath

2004

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

Abstract

In this thesis we examine the ways in which elements in permutation groups may be related. The thesis is split into three parts.

In the first part of the thesis we examine those elements in S_n that have trivially intersecting cyclic groups but which nonetheless satisfy a word of length shorter than their order. We not only show that such elements exist but give constructions for related elements. We conclude this section by demonstrating some specific examples of nearly p-groups arising from looking at word lengths.

In the second part of the thesis we turn the problem on its head and look at expressing elements of S_n and A_n as products of cycles of a given length. We conclude that we can express any element in A_n as a product of two cycles of length $\frac{3n-3}{4}$ or longer.

In the third part of the thesis we extend our arguments relating to expressing elements as products of a given shape to look at the groups generated by two elements of a given shape. In particular we look at the groups generated by the n-cycle $(1, 2, \ldots, n)$ and a standard representative of each conjugacy class of S_n. By choosing our representative of the conjugacy class we are able to generate S_n or A_n in most cases.

Appendix A contains some early unrelated work on trying to recognize the Galois group of a polynomial based on the cycle shapes of elements of the Galois group.

Appendices B and C contain some notes on *Swirls*. We defined the swirl of an element when trying to solve word problems The swirl of a group element,g, is the right shift of each of the support of g under a given ordering of the set g acts on. We prove a number of interesting results concerning swirls but ultimately were not able to use them to help solve the word problems and their inclusion is as an interesting area where further investigation my yield results.

Throughout the development of this thesis the author has relied on the use of the computer algebra package GAP [8] as a way of gathering data and testing hypothesis. Without the use of this package the author doubts if he would have been able to develop the theory to the level seen and is indebted to the authors of the package for providing such a wonderful tool.

Acknowledgments

I would like to thank Dr Geoff Smith for supervising this work and showing extreme patience during the periods of my life where progress was slow. I would also like to thank HEFCE for providing financial support during my studies and allowing me the time to complete this thesis. Thanks must also go Dr Shekhar Nandy who started me on this path and assured me it only takes 3 years and to Dr John Thompson for constantly reminding me that I "wasn't " and to Mr Mario Ferelli who I plan to remind "is not". Finally my most sincere thanks must go to my partner Jill for her constant support and reminders that I should be studying rather than contemplating rivers, without her this thesis would almost certainly never have been completed.

I did not jump, I took a tiny little step and there conclusions were

Buffy the Vampire Slayer

Notation

We define the basic notation we will use throughout this thesis.

S_n	Symmetric group on n letters
A_n	Alternating group on n letters
M_{11}, M_{12}, M_{23}, M_{24}	The four Mathieu groups which are at least 4-transitive
g, h, x, y, z	Group elements
$C_G(g)$	The centralizer in G of g
p	Prime integer
$a, b, d, n, i, j, k, m, l, r$	Integers
ω	A word on two group elements
$o(g)$	The order of the group element g
c	A standard shape representative
c_i	A single cycle in a permutation
supp g	The support of the group element g
$Degree(G)$	The size of the support of the permutation group G

A word on pronouns

Throughout this thesis the author has adopted the use of the pronoun "we" rather than "I" to denote the joint journey taken by both the author and the reader.

Contents

Chapter 1

Definitions of related elements and basic existence results

1.1 Basic definitions

We begin with a basic definition.

Definition 1.1 (Related elements). Let G be a group, we say $g, h \in G$ are related if there is a non-trivial word ω on g, h (a product involving terms drawn from $\{g, h\}$) which is the identity. We say that g, h are non-trivially related if there exists such an ω and $\langle g \rangle \bigcap \langle h \rangle = 1$.

We hope that the terminology in Definition 1.1 will not cause confusion with the notions of *relator* and *relation.*

Our aim in the first part of this thesis is to show that there are non-trivially related elements in groups and ways of constructing both the elements and ω.

If we allow our elements to be trivially related, that is $\langle g \rangle \bigcap \langle h \rangle \neq 1$, then we may always find an ω. For example if $g^i = h^j$ and $o(g) = m$, then we may choose

$\omega = h^j g^{m-i}$. Therefore, this case is relatively uninteresting and we will not deal with it further.

Equally, if we allow the length of ω to be longer than $o(g), o(h)$, then again we may construct $\omega = g^i h^j$ where $o(g) = i$ and $o(h) = j$ and this case is again uninteresting.

Instead we shall concentrate on the situation where $o(g), o(h) > length(\omega)$. Of course we have no guarantee that suitable g, h, ω exist and proving this will be our first task.

We concentrate on the case where $G = S_n$ as his gives us the greatest flexibility in our choice of g and h.

1.2 Basic results

Our purpose in this section is to show that non-trivially related elements exist in S_n. In addition we will show that in some cases no non-trivially related elements exist. In this section we will concentrate on finding words of length les than m on $g, h \in S_n$ where $o(g), o(h) > m$

We begin this section by showing that for certain small n there are no non-trivially related elements.

Lemma 1.1. *Let $g, h \neq id$ be elements of S_n and let g have order $m \leq 4$. Then g and h cannot be non-trivially related.*

Proof. For g and h to be non-trivially related we need to find $\omega = 1$ of length less than m. We examine all possible cases and note that in each case we may reverse the roles of g and h.

For $m = 2$ there are no possible words of length 1.

For $m = 3$ the only possible word is $gh = id$ or alternatively $g = h^{-1}$ so $\langle g \rangle = \langle h \rangle$ so they are trivially related.

For $m = 4$ there are two options for ω. Firstly, ω may be of the form ghh or alternatively $g = h^{-2}$ so $\langle g \rangle \subseteq \langle h \rangle$ so they are trivially related. The other option is that $ghg = id$ but this similarly yields $h = g^{-2}$ and the same argument applies. □

We may also observe the following corollary.

Corollary 1.2. *For $n \leq 4$ there are no non-trivially related elements in S_n.*

1.3 Words of length 4

1.3.1 m-cycles

For $n \geq 5$ we can find non-trivially related elements in S_n. Lemma 1.3 gives a construction for elements in S_n that generate distinct cyclic subgroups.

Lemma 1.3. *Let $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ and let $g = (\alpha_1, \alpha_2, \ldots, \alpha_m) \in S_\Omega$ and also let $h = (\alpha_1, \ldots, \alpha_{j-1}, \alpha_m, \alpha_{m-1}, \ldots, \alpha_j) \in S_\Omega$ then for $2 < j < m$ the cyclic groups $\langle g \rangle$ and $\langle h \rangle$ intersect trivially.*

Proof. In order to prove this result we consider the action of the two cyclic groups on α_1 and α_j as a pair. For the cyclic groups to intersect at least one element of both groups each must be coincidental on these elements as a pair. We consider the image of α_j when the image of α_1 is α_i, $i \neq 1$. The following tables show the images under $\langle g \rangle$ and $\langle h \rangle$ respectively:

i	α_j
$2 \leq i \leq m-j+1$	$j+i-1$
$m-j+1 < i \leq m$	$j+i-(m+1)$

i	α_j
$2 \leq i \leq j-1$	$i-1$
$j \leq i \leq m-1$	$i+1$
m	$j-1$

There are 6 possible combinations namely:

$$\begin{aligned}
j+i-1 = i-1 &\Rightarrow j = 0 \\
j+i-1 = i+1 &\Rightarrow j = 2 \\
j+i-1 = j-1 &\Rightarrow i = 0 \\
j+i-(m+1) = i-1 &\Rightarrow j = m \\
j+i-(m+1) = i+1 &\Rightarrow j = m+2 \\
j+i-(m+1) = j-1 &\Rightarrow i = m
\end{aligned}$$

The only one of these combinations which is not precluded by our restrictions on j is where $i = m$. In this case we instead consider the image of α_2 when $i = m$, in $\langle g \rangle$ it is α_1 and in $\langle h \rangle$ it is α_{m-1}, these are distinct unless $m = 2$ which is precluded by our restrictions on m and the two cyclic groups intersect trivially. □

Lemma 1.3 gives elements of S_n that generate cyclic subgroups that have trivial intersection. If these elements are also related, then we have non-trivially related elements. As the next theorem shows where g is an m-cycle we can always find h, also an m-cycle, such that $(gh)^2 = id$.

Theorem 1.4. *For all $g \in S_n$, g an m-cycle, $m \geq 5$, there exists an h, also an m-cycle, such that $(gh)^2 = id$ and $\langle g \rangle \cap \langle h \rangle = id$.*

Proof. We attack this in two parts. Firstly we construct h given g and show that it has the required property. Secondly we use Lemma 1.3 to show that the two elements generate distinct cyclic subgroups of S_n.

We may assume that $g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots, \alpha_m)$, having fixed g we construct a suitable h. Let $h = (\alpha_1, \alpha_2, \alpha_3, \alpha_m, \alpha_{m-1}, \ldots, \alpha_4)$ so $gh = (\alpha_1, \alpha_3)(\alpha_2, \alpha_m)$. Thus gh has order 2 and ω has length 4 and we have demonstrated that the required h exists. Lemma 1.1 tells us that we cannot do better than this although alternative h will clearly exist.

Our chosen g and h have the form given in Lemma 1.3 with $j = 4$ so the cyclic groups are distinct and we are done. □

We note that if g is an m-cycle, then it will not be possible generate, h, also an m-cycle such that gh is a single transposition as a single transposition is an odd element and the product of two similarly shaped elements will always be even. Of course if we allow g to be an element other than an m-cycle, then it will sometimes be possible to generate an h such that gh is a single transposition.

1.3.2 Other elements of S_n

Where g is not an m-cycle can we do the same ? The obvious approach where g contains a suitable m-cycle is to form h by using the construction of Theorem 1.4 on the m-cycle and take the inverse of each of the other cycles. However, in such a construction there is no guarantee that the cyclic groups will intersect trivially. Clearly if g is of order m, then this will be the case as each element of the cyclic group will act non-trivially on the support of the m-cycle. However,

if g is of order k, then we cannot rely on this construction and must take a different approach. Again we have recourse to Lemma 1.3, we note from this that for cycles with support of size 4 or greater we can find a cycle with the same support such that when restricted to this support the cyclic groups intersect trivially. Furthermore, for transpositions we need not include any cycles acting on their support as they will disappear. Having dealt with transpositions and cycles of length 4 or more we need only consider 3-cycles, now if the 3-cycle in g is $(\alpha_1, \alpha_2, \alpha_3)$, then we may insert the transposition (α_1, α_2) into h, now restricting our attention to$\{\alpha_1, \alpha_2, \alpha_3\}$ we see the action of $gh = (\alpha_2, \alpha_3)$ hence $(gh)^2 = ()$. This naturally leads us to consider whether, for arbitrary g we can construct a h that is non-trivially related to g.

Clearly for arbitrary g we cannot create a word that is non-trivially related to g as by Lemma 1.1 elements of order 4 or less cannot be non-trivially related to any element. In addition, as 5 is prime the only elements of order 5 are the 5-cycles or products of 5-cycles so there is no scope for additional non-trivially related elements. For elements of order 6 or more then there are certainly non-trivially related elements where at least one of the elements is not an m-cycle of length greater than 5. Consider $g = (1,2,3)(4,5)$ and $h = (1,3,2,4,5)$ now $gh = (1,4)$ and g and h have orders 6 and 5 respectively so they are clearly related, in addition a little work shows the cyclic subgroups intersect trivially so the elements are non-trivially related. Theorem 1.5 generalises this argument.

Theorem 1.5. *Given $g \in S_n$ of order greater than 5, there exists $h \in S_n$, also of order greater than 5, such that $(gh)^2 = id$ and $\langle g \rangle \cap \langle h \rangle = id$*

Proof. If g contains an m-cycle, $m \geq 5$, then we can construct the required h. We do this by considering each cycle of g in turn. For cycles with length 4 or

greater we apply Theorem 1.4 and for transpositions we do nothing. For 3-cycles we insert a transposition with elements drawn from the support of the 3-cycle. As the support of each cycle of h is a subset of the support of a cycle of g we may consider the support of each cycle of g separately. It is clear that for each cycle of g_i of g that $\langle g_i \rangle \cap \langle h_i \rangle = \emptyset$ and we may extend to the full support.

If g does not contain any cycle of length 5 or more, then it must consist solely of 2,3, and 4-cycles. If g only contains one type of cycle, then g has order less than 5. Similarly if g only contains 2-cycles and 4-cycles, then it will have order 4. So g must have at least one of the following combinations of cycles a 2-cycle and a 3-cycle or a 3-cycle and a 4-cycle. The construction in both cases is similar, we construct a 5, or 6, cycle that joins each of the cycles together as a transposition while fixing the other elements, having generated the h we argue as in Lemma 1.3 that the cyclic groups intersect trivially.

When g contains both a 2-cycle and a 3-cycle we may assume, without loss of generality, that $g = (\alpha_1, \alpha_2, \alpha_3)(\alpha_4, \alpha_5)$ now form $h = (\alpha_1, \alpha_3, \alpha_2, \alpha_5, \alpha_4)$. Now $gh = (\alpha_1, \alpha_5)$ so g and h are clearly related. Now in the cyclic group generated by g the image of α_4 is either α_5 or α_4, $h^m(\alpha_4) = \alpha_5$ only when $m = 4$ and $h^4(\alpha_1) = \alpha_4$ an impossibility under the action of g so the cyclic groups are distinct.

Similarly when g contains both a 3-cycle and a 4-cycle we may assume, without loss of generality, that $g = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)(\alpha_5, \alpha_6, \alpha_7)$ and we now choose $h = (\alpha_1, \alpha_4, \alpha_3, \alpha_2, \alpha_5, \alpha_6)$. So, $gh = (\alpha_1, \alpha_5)(\alpha_6, \alpha_7)$ and the two elements are clearly related. Now $\langle h \rangle$ stabilises α_7 so the cyclic groups may only intersect when α_7 is stabilised. In $\langle g \rangle$ α_7 is only stabilised when α_5 and α_6 are also stabilised. The only element of $\langle h \rangle$ which stabilises all three elements is the identity thus $\langle h \rangle$ and $\langle g \rangle$ intersect trivially. $\square$

1.4 Words of length greater than 4

So far we have concentrated on proving that non-trivially related elements of groups exist by looking at the shortest possible non-trivially related words. However, it is worth considering whether, given g of order $m \geq 5$, it is possible to find a h for every $4 \leq l < m$ such that there exists an ω of length l. There are certain obvious cases that present themselves. Where g is an m-cycle and l is even then we can extend the proof of Theorem 1.4 so that $(gh)^{\frac{l}{2}} = id$.

Theorem 1.6. *For all $g \in S_n$, g an m-cycle, $m \geq 5$, there exists an h also an m-cycle such that $(gh)^{\frac{l}{2}} = id$, for l even and $2 \leq l < m$ and $\langle g \rangle \cap \langle h \rangle = id$.*

Proof. The proof follows the same lines as Theorem 1.4 and again we assume that $g = (\alpha_1, \alpha_2, \ldots, \alpha_m)$. In this case we cannot assume a single construction for our m-cycle, instead we need different constructions when $\frac{l}{2}$ is odd or even these are given by:

$$h = \begin{cases} (\alpha_1, \alpha_2, \ldots, \alpha_{l-1}, \alpha_m, \alpha_{m-1}, \ldots, \alpha_l) & \frac{l}{2} \text{ even} \\ (\alpha_1, \alpha_2, \ldots, \alpha_{\frac{l}{2}-1}, \alpha_m, \alpha_{m-1}, \ldots, \alpha_{\frac{l}{2}}) & \frac{l}{2} \text{ odd} \end{cases}$$

Therefore gh gives rise to two $\frac{l}{2}$-cycles when $\frac{l}{2}$ is even and a single $\frac{l}{2}$-cycle when $\frac{l}{2}$ is odd. Thus $(gh)^{\frac{l}{2}} = id$ as required.

Again we can apply Lemma 1.3 to the chosen g and h to show that the two cyclic groups generated intersect trivially. □

In Theorem 1.5 we extended Theorem 1.4 to cover general elements of S_n. While it was possible to extend the construction for m-cycles easily when looking for a short word it is less clear how, in general, one would do this for arbitrary elements. For k even one could adopt the same construction as in the first part

of Theorem 1.5 ensuring only the support of the m-cycle is moved by $(gh)^2$. However, this does not help answer the general question of given $g \in S_n$ of order $m \geq 5$ and $4 \leq l < m$ can we always construct a h such that g and h are non-trivially related by a word ω of length l and there is no ω' of length less than l such that $\omega' = id$.

1.5 Words of arbitrary length

We can show that in general for $g \in S_n$ of order m and $4 \leq l < m$ we cannot find an ω of length l and h dependent on g and ω such that $\omega = id$ and the order of $h > l$ and $\langle g \rangle$ and $\langle h \rangle$ intersect trivially. The following theorem gives an example of this.

Theorem 1.7. *Let $g \in S_n$, of order greater than 5, then there does not exist an $h \in S_n$ also of order greater than 5 such that g and h are non-trivially related by a word of length 5.*

Proof. There are 32 possible words of length 5 on g and h, two of these words are

trivial as they consist solely of g's or h's. The remaining words are listed below:

ω	Case	ω	Case
$ggggh$	1	$hgggg$	1
$ggghg$	2	$hgggh$	2
$ggghh$	1	$hgghg$	3
$gghgg$	2	$hgghh$	2
$gghgh$	3	$hghgg$	3
$gghhg$	2	$hghgh$	4
$gghhh$	1	$hghhg$	4
$ghggg$	2	$hghhh$	2
$ghggh$	3	$hhggg$	1
$ghghg$	3	$hhggh$	2
$ghghh$	4	$hhghg$	4
$ghhgg$	2	$hhghh$	2
$ghhgh$	4	$hhhgg$	1
$ghhhg$	2	$hhhgh$	2
$ghhhh$	1	$hhhhg$	1

We deal with each word by an analysis of cases as given in the table above.

1. Where the word is of the form $g^i h^j = id$ or $h^j g^i = id$ then the cyclic groups intersect non-trivially as $g^i = h^{-j}$.

2. Where the ω is of the form $g^i h^j g^k = id$ then we may rearrange to get $h^j = g^{-(i+k)}$ and the two cyclic groups intersect non-trivially. The same argument applies if $\omega = h^i g^j h^k$.

3. As $\omega = id$ we may rearrange all of these words to be of the form $hghgg = id$. We can then look at this word in two different ways. Firstly:

$$hghgg = id \Rightarrow hghg = g^{-1} \tag{1.1}$$

Secondly we can see:

$$\begin{aligned} hghgg = id &\Rightarrow ghggh = id \\ &\Rightarrow hggh = g^{-1} \end{aligned} \tag{1.2}$$

Combining Equations 1.1 and 1.2 we can see that $hghg = hggh$ and by cancelling the leading hg that $hg = gh$ so g and h commute. Therefore we may write $\omega = h^2g^3$ and we have an equation of type 1.

4. As $\omega = id$ we may rearrange all of these words to be $ghghh = id$ so all are equivalent. We now see that the same argument as in case 3 applies by interchanging the roles of g by h.

□

Theorem 1.7 shows us that we cannot always generate words of a given length. However, it does not give us any information about whether this is possible for words of length other than 5. It may be that for ω of length 6, or more, given n sufficiently large $\exists g, h \in S_n$ that satisfy ω and $\langle g \rangle \cap \langle h \rangle = 1$.

Chapter 2

Words of Prime Length

In Chapter 1 we examined the existence of non-trivially related group elements. In Chapter 1 when forming words of length greater than 4 we utilised the fact that ω was of composite length, l, and constructed it by factorising l and forming a shorter word that had order dividing l. Of course where l is prime this approach will not work. Indeed, we have already showed that for $l = 5$ there are no non-trivially related elements. However, as the next section shows this is not the case for all primes.

2.1 Motivation

To motivate our discussion we consider a concrete example. Now suppose that $p = 11$, $g = (1,2,3)(6,7,8,9,10)$ and $h = (1,2,3,4,5)(6,8,7)$. Let $\omega = g^3hg^3hh^3$. A direct calculation reveals that $\omega = 1$ and it is easy to see that g, h are unrelated. However, let us elect not to perform that calculation but instead to proceed as follows. Consider both $g = g_1g_2$ and $h = h_1h_2$ as products of disjoint cycles with $g_1 = (1,2,3)$, $g_2 = (6,7,8,9,10)$, $h_1 = (1,2,3,4,5)$, and $h_2 = (6,8,7)$ we

can see that the supports enjoy the following inclusions: supp $g_1 \subseteq$ supp h_1 and supp $h_2 \subseteq$ supp g_2. Moreover, we have arranged our choice of g_1 so that g_1^3 is the identity and so commutes with h_1. Thus supp $g_1 \cap$ supp $\omega = \emptyset$.

We cannot apply the same arguments to the support of g_2. Observe that $h_2^3 = 1$ and that $g_2^3 h_2$ is a product of two disjoint 2-cycles, so supp $\omega \cap$ supp $g_2 = \emptyset$.

We conclude that supp $\omega = \emptyset$ so ω is the identity. A simple calculation shows the elements g, h are independent.

2.2 Results

2.2.1 Small Primes

Before we can proceed to the general case we address the issue of small primes where the construction outlined below does not work. Indeed, for $p = 2, 3, 5, 7$ we conjecture that there are no non-trivially related elements $g, h \in S_p$ where a word of length p on g, h is the identity. We showed in Lemma 1.1 that for $p < 5$ there are no elements that are non-trivially related by a word of length p. We then showed in Theorem 1.7 that the same is true for $p = 5$.

Theorem 1.7 does not extend to the case where $n = 7$ and we can see this via the following example provided by D Johnson. Let $n = 18$ and let

$$g = (1, 2, 3, 4, 5, 6, 7, 8, 9)(10, 11, 12, 13, 14, 15, 16, 17, 18)$$

now it is clear that g has order $9 > 7$. Now we choose x such that $x^2 = g^3$ so

$$x = (1, 2, 4, 5, 7, 8)(3, 10, 6, 13, 9, 16)(11, 12, 14, 15, 17, 18)$$

and we let

$$h = g^{-1}x^{-1} = (1,13,11,3)(2,8,5)(4,16,14,16)(7,10,17,9)(12,18,15)$$

Now, h has order $12 > 7$ as required and $\langle g \rangle \cap \langle h \rangle$ must have order 3 or 1. The only subgroup of $\langle h \rangle$ of order 3 is the one generated by h^4 so if the intersection has order 3 then $h^4 \in \langle g \rangle$, so $h^4 = g^3$ or g^6. But $(1)h^4 = 1$, while $(1)g^3 = 4$ and $(1)g^6 = 7$ and we deduce $\langle g \rangle \cap \langle h \rangle = 1$. Now if

$$\omega = g^4hgh = g^4g^{-1}x^{-1}gg^{-1}x^{-1} = g^3x^{-2} = 1$$

Therefore g and h satisfy a word of length 7 yet their cyclic groups intersect trivially and we are done. We have not been able to give a general construction although it seems likely that this is not an isolated example.

2.2.2 Preliminary Results

Before we can proceed to the general case we will need the following result concerning the intersection of the cyclic groups generated by cycles in S_n.

Lemma 2.1. *Let g and h be r and s-cycles (respectively) in S_n. If the greatest common divisor of r and s is 1, then the cyclic groups generated by g and h intersect trivially.*

Proof. We know by Lagrange's theorem that $\langle g \rangle \bigcap \langle h \rangle$ is a group of order dividing both r and s, but as r and s are coprime this group has order 1 so is trivial. □

2.2.3 The General Case

We may now move to the general case for $p > 7$ and show that we may always find $g, h \in S_p$ such that they satisfy a word of length p. The construction works in much the same way for all primes.

We begin the proof proper by arranging a structure for ω, g and h in similar vein to that used in Section 2.1. First, we suppose that p is odd and that there are natural numbers k and l such that $p = 2k + l + 2$. Now of course, except for small p there will be considerable choice in the selection of k, l, and we will take advantage of this flexibility at a later stage in the argument.

Consider the product $\omega = g^k h g^k h h^l$ so ω can be viewed as a word of length p. Moreover, by specifying the g and h we will arrange that the cyclic groups $\langle g \rangle$, $\langle h \rangle$ intersect trivially, that g, h both have order greater than p, and that $\omega = id$.

First we settle the structure of h. Let $h = h_1 h_2$ where h_1 and h_2 are disjoint cycles of lengths l and $l+2$ respectively. We now enforce a similar structure on g. Once again we want g to be a product of two disjoint cycles so $g = g_1 g_2$ and we want the order of g_2 to be k. Finally we settle the support of each cycle in g and h. Let the support of g_i be Γ_i and the support of h_i be H_i. Moreover, we want to ensure that $\Gamma_2 \subseteq H_2$, $H_1 \subseteq \Gamma_1$ and $\Gamma_1 \bigcap H_2 = \emptyset$. Therefore, we may consider the support of H_2 and Γ_1 independently.

When restricted to H_2, $g^k = id$ so commutes with h so supp $\omega \cap H_2 = \emptyset$. Next we want to arrange that $g^k h$ has order 2 and therefore that $g^k h g^k h = id$, finally our condition on h_1 ensures that $h^l = id$ and we are done.

We need a few results about greatest common divisors before we can proceed. We recall from our elementary algebra that if the integer d divides the integers a and b then d also divides $\lambda a + \mu b$ for all λ, μ also integers.

Lemma 2.2. *If n is an odd number greater than 2, then the greatest common divisor of n and $n+2$ is 1.*

Proof. The greatest common divisor must be odd and divide $(n+2)-n=2$. □

Lemma 2.3. *For p prime and $\frac{1}{2}(p-1)$ odd the greatest common divisor of $\frac{1}{4}(p+1)$ and $\frac{1}{2}(p-1)$ is 1.*

Proof. The greatest common divisor must divide

$$\frac{1}{2}(p+1-p+1)=1.$$

□

Lemma 2.4. *For p prime and $\frac{1}{2}(p-1)$ even the greatest common divisor of $\frac{1}{4}(p+3)$ and $\frac{1}{2}(p-3)$ is 1.*

Proof. Any common divisor of the given integers must divide two times the first minus the second i.e. 3. However, if the the greatest common divisor is 3, then 3 divides $\frac{1}{2}(p-3)$ so therefore must divide $p-3$ and in turn divide p. But, p is prime so $p=3$ and $\frac{1}{2}(p-1)=1$ which is not even so the greatest common divisor must be 1. □

Now if l is odd, then we can use Lemma 2.2 to show that h has order $l(l+2)$.

We now use our flexibility of choice for l to ensure it is odd. The value we choose for l depends on whether $\frac{1}{2}(p-1)$ is odd. If $\frac{1}{2}(p-1)$ is odd we let $l=\frac{1}{2}(p-5)$ and if it is even we let $l=\frac{1}{2}(p-7)$ ensuring l is odd, then $k=\frac{1}{4}(p+1)$ and $\frac{1}{4}(p+3)$ respectively.

Our choice of supports for the disjoint cycles in g, h ensures that we may consider whether $\langle g_i\rangle \bigcap \langle h_i\rangle = 1$ separately for each i. Firstly we consider $\langle g_2\rangle \bigcap \langle h_2\rangle$.

By Lemmas 2.3 and 2.4 we conclude that k and $l+2$ are co-prime. We may now use Lemma 2.1 to show the cyclic groups intersect trivially.

We use a similar approach for $\langle g_1 \rangle \bigcap \langle h_1 \rangle$. First we settle on an order for g_1. In choosing $o(g_1)$ we have two concerns: firstly we must ensure that $|\Gamma_1| + |H_2| \leq p$, and secondly $\langle g_1 \rangle \bigcap \langle h_1 \rangle = 1$. We choose an order for g_1 and deal with each of these concerns in turn. We choose $o(g_1) = l+2$. Now $|\Gamma_1| + |H_2| = 2(l+2) < p$ so our first concern is dealt with. Now we address whether the cyclic groups intersect trivially. We know by Lemma 2.2 that $l+2$ and l are co-prime so we may use Lemma 2.1 to show that $\langle g_1 \rangle \bigcap \langle h_1 \rangle = 1$.

The construction of ω also requires that $g_1^k h_1$ have order 2, but we have not shown this to be the case. We may use Lemmas 2.3 and 2.4 to show that $l+2$ and k are co-prime so g_1^k will also be an $(l+2)$-cycle. Now let $\Gamma_1 = \{\alpha_1 \dots \alpha_{l+2}\}$ and suppose $g_1^k = (\alpha_1, \alpha_2, \dots, \alpha_{l+2})$ we may choose $h_1 = (\alpha_1, \alpha_{l+1}, \dots, \alpha_3)$ and a direct calculation yields $g_1^k h_1 = (\alpha_1, \alpha_2)(\alpha_{l+1}, \alpha_{l+2})$. So we have a g_1 and h_1 with the required property. Moreover, by using Lemma 2.2 and Lemma 2.1 we can show the cyclic groups intersect trivially.

In order to ensure that $\Gamma_2 \subseteq H_2$ we require that $k < l+2$ but have not shown this to be the case. In addition we have not shown that the orders of g and h are greater than p. We address these for each choice of l in turn.

2.2.4 $l = \frac{1}{2}(p-5)$

In this case $k = \frac{1}{4}(p+1)$ and $k < l+2 \; \forall p > 3$.

All that remains is to show that g and h have order greater than p. Now we

have:

$$\begin{aligned} order(h) &= l(l+2) \\ &= \tfrac{1}{2}(p-5)(\tfrac{1}{2}(p-5)+2) \\ &= \tfrac{1}{4}(p-5)(p-1) \\ &= \tfrac{1}{4}(p^2-6p+5) \\ &> p \; \forall p > 9 \end{aligned}$$

As $l+2$ and k were co prime the order of g is $(l+2)k$ so

$$\begin{aligned} order(g) &= (l+2)k \\ &= \tfrac{1}{2}(p-1)\tfrac{1}{4}(p+1) \\ &= \tfrac{1}{8}(p-1)(p+1) \\ &= \tfrac{1}{8}(p^2-1) \\ &> p \; \forall p > 8 \end{aligned}$$

2.2.5 $l = \frac{1}{2}(p-7)$

Now $k = \frac{1}{4}(p+3)$ and $k < l+2 \; \forall p > 9$.

All that remains is to show that g and h have order greater than p. Now we have:

$$\begin{aligned} order(h) &= l(l+2) \\ &= \tfrac{1}{2}(p-7)(\tfrac{1}{2}(p-7)+2) \\ &= \tfrac{1}{4}(p-7)(p-3) \\ &= \tfrac{1}{4}(p^2-10p+21) \\ &> p \; \forall p > 12 \end{aligned}$$

As before:

$$\begin{aligned} order(g) &= (l+2)k \\ &= \tfrac{1}{2}(p-3)\tfrac{1}{4}(p+3) \\ &= \tfrac{1}{8}(p-3)(p+3) \\ &= \tfrac{1}{8}(p^2-9) \\ &> p \; \forall p > 9 \end{aligned}$$

We have already dealt with small p and the proof outlined above works for all $p > 12$ so we only need consider when $p = 11$. Now if $p = 11$, then $\frac{1}{2}(p-1)$ is odd so we are in the first case and we are done.

2.3 Conclusion

Putting all of the above together we obtain the following result.

Theorem 2.5. *Suppose that $p > 7$ is a prime number, then there exist $g, h \in S_p$ with $\langle g \rangle \bigcap \langle h \rangle = id$, $o(g), o(h) > p$ and there is a word ω of length p on g and h with $\omega = 1$.*

Chapter 3

Words of arbitrary length

In Chapter 2 we have shown that for p prime we can find $g, h \in S_p$ such that there is a word on g, h of length p which is the identity. In this chapter we demonstrate that in general we may do the same for any n.

3.1 n odd

We do this by considering the case for n prime and extending it to general n. In the first instance we note that in proving the case for n prime we have only required that n be odd and not divisible by 3. We restate the extended theorem 2.5.

Theorem 3.1. *Suppose that $n > 7$ is an odd number not divisible by 3, then there exist $g, h \in S_n$ with $\langle g \rangle \bigcap \langle h \rangle = id$, $o(g), o(h) > n$ and there is a word ω of length n on g and h with $\omega = 1$.*

Proof. We note that the proof of Theorem 2.5 only requires that n is odd and not divisible by 3. □

We now give a construction for n divisible by 3.

3.2 n divisible by 3

To motivate our discussion we consider a concrete example suppose that $n = 9$, $g = (1,4,5,2,3)(7,8,9)$ and $h = (1,2,3,4,5)(6,7,8)$. Let $\omega = g^2hg^2hg^2h$. A direct calculation reveals $\omega = 1$ and it is easy to see that the cyclic groups generated by g and h intersect trivially.

As before we first settle on a structure for ω. As for n prime we start by forming a repeating structure, in this case we use the fact that n is divisible by 3 and let $\omega = g^khg^khg^kh$ with $k = \frac{n}{3} - 1$. We now settle the structure of g and h as before where $g = g_1g_2$ and $h = h_1h_2$ as products of distinct cycles. However, this time we settle the structure more clearly. Firstly, we let $h = h_1h_2 = (1,2,\ldots,n-4)(n-3,n-2,n-1)$ and note that as n is divisible by 3 then the greatest common divisor of $n-4$ and 3 is 1, so h has order $3n - 12 > n\ \forall n > 6$.

Next we settle on the structure of g, we want g to consist of, g_1 a $(n-4)$-cycle with support of $\{1,2,\ldots,n-4\}$ and g_2 a 3-cycle with support $\{n-2,n-1,n\}$. We now consider how g_2 and h_2 interact. Clearly, whatever 3-cycle we choose for g_2 the cyclic groups will intersect trivially as they act on different supports. Now if k is a multiple of 3, then our choice of g_2 is irrelevant as $g_2^k = 1$ and $h_2^3 = 1$. If k is not a multiple of 3, then we choose g_2 so $g_2^k = (n-1,n-2,n)$ and we see that $g_2^kh_2 = (n-2,n,n-3)$ and in either case $\{n-3,\ldots,n\} \cap \text{supp}\ \omega = \emptyset$.

Next we need to ensure that if g_1 is a $(n-4)$-cycle, then g_1^k is still a $(n-4)$-cycle, we do this via the following lemma.

Lemma 3.2. *The greatest common divisor of* $n-4$ *and* $\frac{n}{3} - 1$ *is 1.*

Proof. Any common divisor must divide three times the second minus the first i.e. 1. □

We are therefore assured that our $(n-4)$-cycle remains an $(n-4)$-cycle so may choose g_1 so that $g_1^k = (1, n-4, n-5, \ldots, 5, 3, 4, 2)$ and we observe that $g_1^k h_1 = (3, 5, 4)$. Thus $\{1, 2, \ldots, n-4\} \cap \text{supp } \omega = \emptyset$. and we conclude supp $\omega = \emptyset$.

Given g_1 and g_1^k are both $(n-4)$-cycles we know $\langle g_1 \rangle = \langle g_1^k \rangle$. Therefore provided we can show $\langle g_1^k \rangle \cap \langle h_1 \rangle = 1$ we are done. We do this by considering the action of these groups on the pair $\{3, 4\}$. Under the action of h_1 if the image of 4 is m, then the image of 3 is $m-1$ for all m except 1 where the image is $n-4$. However, under the action of g_1^k if the image of 4 is m, then for $5 \leq m \leq n-5$ the image of 3 is $m+1$, this leaves only $m = 1, 2, 3,$ and $n-4$ where the images of 3 are $2, 4, 5,$ and 1 respectively whereas under the group generated by g_1^k they are $n-4, 1, 2, n-5$. Therefore these will only coincide if $n = 6$ and we have already ruled out this possibility and we have shown the cyclic groups intersect trivially. We note that we have not relied on n being odd and the proof works for any n divisible by 3 and we now conclude.

Theorem 3.3. *Suppose that $n > 6$ is divisible by 3, then there exist $g, h \in S_n$ with $\langle g \rangle \cap \langle h \rangle = id$, $o(g), o(h) > n$ and there is a word ω of length n on g and h with $\omega = 1$.*

Now Theorems 3.1 and 3.3 show that for odd $n > 7$ we may always find related elements in S_n that satisfy a word of length n. All that remains is to show that for suitably large n we may also do this for even n.

3.3 n even

As with n prime we consider a simple case for motivation. Suppose that $n = 10$, $g = (1, 2, 3, 4, 5)(6, 7, 8)$ and $h = (1, 2, 3, 4)(6, 8, 7)$. Let $\omega = g^4 h g^4 h$. A direct

calculation again reveals that $\omega = 1$ and it is easy to see that the cyclic groups generated by g and h intersect trivially.

Again we begin by settling our structure for ω and let $\omega = g^k h g^k h$ where $k = \frac{n}{2} - 1$. As before we settle the structure of g and h. Firstly we want g and h both to be products of two distinct cycles. We first settle the structure of g so that $g = (1, 2, \ldots, \frac{n}{2})(\frac{n}{2} + 1, \frac{n}{2} + 2, \ldots, n - 2)$, now g consists of an $\frac{n}{2}$-cycle and an $(\frac{n}{2} - 2)$-cycle. In both cases when raised to the $\frac{n}{2} - 1$ the cycles retain their original structure as in both cases the greatest common divisor is 1. Furthermore, the greatest common divisor of $\frac{n}{2}$ and $\frac{n}{2} - 2$ is at most 2 so g has order at least $\frac{n}{4}(\frac{n}{2} - 2) > n \; \forall n > 12$. For $n = 12$ $o(g) = 12$ and we note that this construction does not work in this case. For $n = 10$ the construction still holds as the greatest common divisor of 5 and 3 is 1 so $o(g) = 15 > 10$. However, for $n = 8$ this argument fails as the greatest common divisor is 2 and $o(g) = 4$.

We now consider $g^k = (1, \frac{n}{2}, \ldots, 2)(\frac{n}{2} + 1, \frac{n}{2} + 2, \ldots, n - 2)$. We now settle on our h in order to ensure that $g^k h$ results in disjoint transpositions. We do this by letting $h = (1, 2, \ldots, \frac{n}{2} - 1)(\frac{n}{2} + 1, n - 2, n - 3, \ldots, n, \frac{n}{2} + 2, n - 1)$ we have $g^k h = (1, \frac{n}{2})(\frac{n}{2} + 1, n - 1)(\frac{n}{2} + 2, n)$.

Now g_1 and h_1 are a $\frac{n}{2}$-cycle and a $(\frac{n}{2} - 1)$-cycle respectively and hence the greatest common divisor of their lengths is 1 and by Lemma 2.1 their cyclic groups intersect trivially. We observe that g_2 stabilises $n-1$ and n and the only element of $\langle h_2 \rangle$ that stabilises these elements is the identity and so $\langle g \rangle \cap \langle h \rangle = id$.

We need to ensure $o(h) > n$. Now h consists of an $\frac{n}{2}$-cycle and a $(\frac{n}{2} - 1)$-cycle, the lengths of these cycles are coprime and so h has order $\frac{n}{2}(\frac{n}{2} - 1) > n \; \forall n > 6$.

We have demonstrated a construction for all even $n > 12$, furthermore we have shown the construction works for $n = 10$. We note that for $n = 12$ we may use Theorem 3.3 as n is divisible by 3.

Finally, we turn our attention to the case where $n = 8$ we show that this is the case via a concrete example. Let $g = (1,2,3,4,5)(6,7,8)$ and let $h = (1,2,3,5)(4,7,6)$ so g and h have orders 15 and 12 respectively. We deduce that $\langle g \rangle \cap \langle h \rangle$ has order 3 or 1. Now if it has order 3 then, g^5 must be h^4 or h^8 but g^5 stabilises 4 yet h^4 and h^8 both move 4 and we conclude that the cyclic groups intersect trivially. All that remains is to show that g and h satisfy a word of length 8. Let $\omega = (g^2h^2)^2 = ((2,6)(4,5))^2 = 1$ and we are done.

Theorem 3.4. *Suppose that $n \geq 8$ is an even number, then there exist $g, h \in S_n$ with $\langle g \rangle \cap \langle h \rangle = id$, $o(g), o(h) > n$ and there is a word ω of length n on g and h with $\omega = 1$.*

3.4 Conclusion

We now draw together the results of the previous sections to obtain the following general result.

Theorem 3.5. *Suppose that $n \geq 8$, then there exist $g, h \in S_n$ with $\langle g \rangle \cap \langle h \rangle = id$, $o(g), o(h) > n$ and there is a word ω of length n on g and h with $\omega = 1$.*

Proof. The proof has been completed in three parts.

1. Theorem 3.1 gives us all n odd and not divisible by 3.
2. Theorem 3.3 gives us all n divisible by 3.
3. Theorem 3.4 gives us all the even n except $n = 12$.

□

We have already shown that of the remaining possibilities $n = 1, 2, 3$ and 5 are impossible as words of these lengths give rise to related elements. Furthermore for $n = 4$ and 6 all elements of S_n have order at most n. We now have a complete solution for all n except $n = 7$. However, a direct computation in GAP shows that no such g and h exist in S_7. While a direct computation does not constitute a proof it gives us reasonable confidence that one exists.

Chapter 4

Distribution of minimum length words

In this chapter we consider the distribution of the minimum length of a word, ω, on g and h, where g and h are n-cycles in S_n, such that $\omega = 1$ and $\langle g \rangle \cap \langle h \rangle = id$. Before we can attempt to calculate the distribution of word lengths we must address a few computational considerations.

In general for large n the problem will be computationally intractable as there are $(n-1)!$ n-cycles and hence $(n-1)!^2$ ordered pairs of n-cycles. Furthermore, for a given length of word, l, there are 2^l words. Therefore, if a given pair of elements have a minimum word of length l, then they will need to be tested in at least $\sum_{i=1}^{l-1} 2^i = 2^l - 2$ words before the minimum word is found.

4.1 Algorithms for reducing the search space

Clearly, if we are able to reduce the number of pairs of elements we need to test in each word, then we will gain a significant increase in efficiency of the algorithm.

In the first instance we note that we may, without loss of generality fix one of the cycles. To show this we use the following result:

Lemma 4.1. *Let $g, h \in S_n$ be n-cycles and let ω be a word on g and h such that $\omega = 1$. Then for $g' = (1, 2, \ldots, n)$ there exists h', also an n-cycle, such that $\omega' = 1$ where ω' is the word obtained by replacing g with g' and h with h' in ω.*

Proof. We first note that there exists $x \in S_n$ such that $g^x = (1, 2, \ldots, n) = g'$. Now let $h' = h^x$. Substituting g' and h' into ω' we can see $\omega' = x^{-1}\omega x = 1$. □

Given that we are able to fix one cycle without affecting the distribution of the lengths of words we reduce the problem of finding words for $(n-1)!^2$ pairs of elements by a factor of $(n-1)!$.

We also note that that for all $z \in C_{S_n}(g)$ if $\omega =_G 1$ for g and h, then $\omega =_G 1$ for g and h^z. Therefore, if we consider the action of $C_{S_n}(g)$ by conjugation on the set of n-cycles, then we need only consider one representative from each orbit. If instead we only consider the action on the set of n-cycles whose cyclic groups intersect trivially with $\langle g \rangle$, then the calculation becomes trivial. We utilise the orbit counting lemma to determine the number of pairs we now need to test.

$$|Orbits| = \frac{1}{|C_{S_n}(g)|} \sum_{i \in C_{S_n}(g)} Fix(i)$$

We first turn our attention to $C_{S_n}(g)$. Now in S_n all n-cycles are conjugate and as previously noted there are $(n-1)!$ of them thus $|S_n : C_{S_n}(g)| = (n-1)!$. Hence, C_{S_n} has order n, furthermore $C_{S_n}(g) < \langle g \rangle$ which is also of has order n and so $C_{S_n}(g) = \langle g \rangle$. Now the construction means that for all but the identity every element moves every n-cycle as by removing elements whose cyclic groups intersect with that of g we have certainly removed all n-cycles that commute with

g and possibly some others. Now the equation reduces to

$$|Orbits| = \frac{Fix(id)}{|C_{S_n}(g)|} = \frac{\text{Number of } n\text{-cycles}}{n}$$

Therefore we make a saving of $|C_{S_n}(g)| = n$ on the number of pairs we need to test.

Having made these simple observations there are seem to be no further ways to reduce the number of pairs that need to be tested. Instead we turn our attention to the number of words that need to be considered for each pair.

4.2 Algorithms for reducing words

In calculating the minimum length of word required such that $\omega = 1$ we need to generate words into which g and h can be substituted. There are two considerations, the first is the number of words that need to be considered, the second is efficiency in calculating the words and making any reductions.

In order to reduce the number of words we make the following observations:

1. All words must contain at least one g and one h.

2. Any word of the form $g^i h^k$ may be ignored as these words imply that either the cyclic groups of g and h intersect non-trivially or that n divides both i and k.

3. If $\omega =_G 1$, then any cyclic permutation of ω will also equal 1.

These observations greatly help to reduce the search space. When considering the effect of each observation we must note the interactions between them for example Observations 3 and 1 taken together mean that we only need consider

words that start with a g and end with an h as any word containing a g and an h may be rotated to be of this form. Considering each observation independently we see that for words length l they save us a factor of 4, l words, and a factor of l respectively. Therefore at best we may assume there are $2^{l-2}/l$ words that we need consider. It is clear that this estimate of the savings is generous and we return to first principles for a more reasonable estimate. We know there are 2^l words of length l and rotations of these can be used to reduce this by a factor of up to l. Furthermore having considered the rotational reductions we need not consider the reduction to words of starting with a g or an h as this simply reduces the computational work. Furthermore there are $l+1$ words of the form $g^i h^{l-i}$ for $0 \leq i \leq l$ which together with their rotations may be removed. Therefore we have approximately $2^l/l - (l+1)$ words for any given l. Table 4.1 shows both the actual number of words and the estimate.

Table 4.1: Number of distinct words

l	Estimate	Actual
4	-1	1
5	1	2
6	4	7
7	11	12
8	23	27
9	47	50
10	92	97
15	2,169	2,176
20	52,408	52,467
25	1,342,151	1,342,158

4.3 Implementation

Having made these observations we turn our attention to the practical considerations of implementation of the algorithms. In order to implement the reduced word list we must generate each word, or ideally not generate words we do not want, and then check whether any cyclic permutation of it has already been included in the list of words or is one the form $g^i h^k$. The straightforward approach is to check each word and its cyclic permutations against the list of words. However, this is not practical as for even moderate n as we have to test inclusion for up to $n-1$ permutations of each of 2^{n-2} words in a list of words that can be up to $2^n/n-(n+2)$ long. Indeed, it seems that the natural constructions of lists of words generate an almost complete list of words early in the sequence with most of the words generated later being redundant.

In order to solve the problem of inclusion of a permutation of a word we consider how we represent our words. The most straightforward approach would be to hold these as strings of g's and h's. However, an alternative approach would be to consider each word as a list of 0's and 1's thus the word $gghgh$ would be $[0,0,1,0,1]$. There is a natural bijection between the set of words expressed as lists of 0's and 1's and the set $\{1 \ldots 2^n\}$ such that each word is the binary representation of the given integer. Indeed, we may set up the bijection to the set $\{1 \ldots 2^{n-2}\}$ by considering the first and last digits fixed as zero and one respectively. Already this approach gives a simple way to generate words in an ordered fashion and gives us the ability to exclude words of the form $g^i h^k$ merely by excluding from our set of integers those numbers consisting solely of 1's, namely $2^l - 1$ for $1 \leq l \leq n$.

The key advantage of the representation given above is the efficiency of check-

ing for inclusion of cyclic permutations of the current word in previously generated words. For each cyclic permutation of a word which starts with a zero and ends with a one instead of checking inclusion in the set of previous words we use the bijection merely to check that the integer representation of each permutation of the word is larger than that of the current word. This reduces the problem of inclusion for a given word from a large number of list comparisons to $n-2$ integer multiplications and an integer comparison.

We can further improve the efficiency of the algorithm by instead of using a single bijection ψ from the set of words to $\{1 \ldots 2^{n-2}\}$ we set up a family, ψ_i, of bijections. We construct ψ_i so that ψ_i is isomorphic to applying the permutation $(1, 2, \ldots, n)^i$ to the word and then applying ψ. We therefore no longer need calculate the cyclic permutations of each word, merely apply the relevant bijection. In considering how to generate the ψ_i it is useful to consider $(h)\psi$ as the cartesian product of the list $[0, 2^{(n-2)}, 2^{(n-3)}, \ldots, 1, 0]$ and h. Now, if we wish to generate ψ_i, then we may do this by taking a suitable permutation of $[0, 2^{(n-2)}, 2^{(n-3)}, \ldots, 1, 0]$, indeed the relevant permutation is $(1, 2, \ldots, n)^{-i}$, and then taking the cartesian product of this and the representation of the word. Thus applying each of the ψ_i is equivalent to taking the cartesian product of two lists and summing the result thus reducing the word reduction problem to $n(n-2)$ integer multiplications and n integer comparisons for each word.

While the reductions outlined above go some way to reducing the number of redundant words they by no means remove all such redundant words. For example, a word may contain the sequence g^n which will be identically one. Trapping and removing such words would be costly. However, their existence must be borne in mind when constructing the algorithms to test pairs of elements. Provided the algorithm tests words in ascending length, if $\omega = \omega_1 g^n \omega_2 = 1$, then

$\omega_1\omega_2 = 1$ and is shorter than ω so the algorithm will never test against such a word except where the result will not be 1. However, it is possible that in some cases the word $\omega_1\omega_2$ was not tested against as it was removed as a trivial word. However, we know the only words removed are of the form $g^i h^k$, provided we remove pairs of elements whose cyclic groups intersect non-trivially such words will only be the identity when n divides both i and k. Furthermore, we know the only sequences we can trivially remove are multiple of n powers of either g or h. In order for such a word not to have been removed it must contain at least hg as otherwise it ω would be of the form $g^i h^k$ which would be removed by standard reduction. The shortest trivial word containing a hg is $h^n g^n$. Therefore, the shortest word not currently removed that could cause spurious results is $g^n h^n g^n h^n$, a word of length $4n$.

4.4 Results

Even with the efficiencies outlined above for $n > 10$ it was not possible to calculate the distribution of minimum word lengths due to computational limitations.

Table 4.2 shows the distribution of length of shortest words for $4 \leq n \leq 10$.

There does not appear to be an obvious pattern to the longest minimum word length nor to the distribution of minimum word lengths. However, we can see that, at least for small n, the longest minimum word length appears to be increasing faster than n.

As previously noted there are no 7-cycles which satisfy a word of length 7 and do not satisfy a shorter word. Indeed we find no elements with minimum words length 11 or 13. However, we do find 36 pairs of elements that have a minimum word of length 17 for $n = 9$. For example, we may choose $g = (1, 2, \ldots, 9)$,

Table 4.2: Distribution of shortest words

Word length	n 4	5	6	7	8	9	10
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	5	12	35	80	315	1,120
5	0	0	0	0	0	0	0
6	4	10	36	161	536	2,088	8,920
7		0	0	0	0	0	0
8		5	54	231	1,120	5,220	23,800
9			0	91	0	2,520	0
10			6	119	880	2,250	19,310
11				0	0	0	0
12				77	1,384	14,679	92070
13					0	0	0
14					776	4,823	23,370
15					0	2,277	0
16					160	3,069	66,050
17					0	36	0
18					48	2,493	91,970
19						36	0
20						414	23,390
21						36	0
22						0	4,400
23						0	0
24						18	7,940
25							0
26							140

$h = (1,2,6,4,9,5,8,7,3)$ and $\omega = g^4(hg)^4gh^4 = 1$. Therefore it is possible to find pairs of n-cycles who have a minimum word of prime length. However, for the n tested there are no elements that have a minimum word of length 5, 7, 11, or 13 which leads to the following conjecture.

Conjecture 4.2. *Let p be a prime, $p < 17$, then there do not exist g, h both n-cycles in S_n whose cyclic groups intersect trivially such that the the shortest*

word they satisfy is of length p.

We note that for n even there are no elements that satisfy a word of odd length. Observe that the identity is an even permutation and an n-cycle for n even is an odd permutation, so an even number of n-cycles are required to maintain parity. We therefore need not consider any words of odd length when n is even a further saving, but only for even n.

We now consider the following example for $n = 5$. We let $g = (1, 2, 3, 4, 5)$ and let $h = (1, 3, 2, 5, 4)$ we now consider the shortest word that g and h satisfy. They do not satisfy the word *ghgh* and, as previously noted, they will only satisfy a word of length 5 if their cyclic groups intersect non-trivially, which they do not. Therefore the shortest word g and h may satisfy is of length 6, a little searching shows that they satisfy the word *gghggh*. However, we also see that they satisfy the words *ghghgh* and *ghhghh*. Thus the pair satisfy 3 of the 7 words of length 6. We conclude that not only may a given pair of elements not satisfy a unique shortest word but that they may satisfy a high proportion of the available words. Table 4.3 shows the number of minimum words for each of the 1,384 8-cycles that together with $(1, 2, \ldots, 8)$ have a minimum word of length 12. It also shows the same distribution for the 4,400 10-cycles that together with $(1, 2, \ldots, 10)$ have a minimum word of length 22.

While the vast majority of pairs of elements appear to satisfy a unique shortest word a significant number appear to satisfy more than one minimum length word.

Table 4.3: Distribution of the number of shortest words

Word count	Number of elements	
	$l = 12$ and $n = 8$	$l = 22$ and $n = 10$
1	928	3,600
2	368	700
3	72	80
4	8	20
5	0	0
6	8	0

Chapter 5

Prime power elements that do not generate p-groups

In this chapter we first look at the length of words where g and h both have prime power order, throughout this chapter p is a prime. This extends to a consideration of groups generated by two elements of prime power but which do not generate a Sylow p-subgroup of G. We begin by looking at such a p-group which is not Sylow p-subgroups of G. We consider the following two elements in S_6, we choose $g = (2,3)$ and $h = (1,5)(2,3)$ now every element of $\langle g, h \rangle$ has order 2, but $\langle g, h \rangle$ is not a Sylow 2-subgroup of S_6.

5.1 Preliminary results

We now turn our attention to the more interesting question. *Let G be a group now for $g, h \in G$ with g and h both of p power order, p prime, and $\langle g, h \rangle$ not a p-group what is the shortest word on g and h that does not have p power order ?*

We wish to begin by gathering some data with which to work by testing all

possible pairs of p-power elements in S_n that do not generate a p-group. Before we gather any data we make the following observations:

Lemma 5.1. *Let $g, h \in S_n$ and let x be the result of substituting g and h into ω, a word on two symbols. Then for $y \in S_n$ x^y is the result of substituting g^y and h^y into ω.*

Proof. The y^{-1} and y terms from successive substitutions will cancel leaving only the end terms □

Lemma 5.2. *Let $g, h, x \in S_n$ then if $\langle g, h \rangle$ is a p-group, then $\langle g^x, h^x \rangle$ is also a p-group*

Proof. Let $\gamma \in \langle g, h \rangle$ then $\gamma^x \in \langle g^x, h^x \rangle$ and as conjugate elements in S_n have the same shape we are done. □

Now Lemmas 5.1 and 5.2 tells us that we need only consider one g from each conjugacy class, as every conjugate of it will have a corresponding h. Unfortunately, we cannot apply the lemma twice to only consider one pair from each pair of conjugacy classes as we need the freedom in the choice of h. However, we should also ensure that we only test each pair once i.e. do not test substituting h and g if we have already tried g and h.

Having made the above observations we turn to calculating the distributions.

5.2 A nearly p-group

When $n = 8$ we can see that for $p = 7$ we sometimes need a word of length p in order to find a non-p-power element. In particular if we choose $g = (1, 2, 3, 4, 5, 6, 7)$ and $h = (1, 5, 4, 2, 8, 3, 6)$, then they first generate a non-p-power element in the

Table 5.1: Minimum word length for a non p-power element

		Word length					
n	p	2	3	4	5	6	7
3	2	3					
4	2	48					
4	3	12	12				
5	2	840	240	120			
5	3	120	60				
5	5	180	60				
6	2	21,720	5,760	1,440			
6	3	2,520	360				
6	5	6,480	2,880	720			
7	2	446,880	90,720	15,120			
7	3	49,140	10,080				
7	5	99,540	21,420	5,040			
7	7	194,040	60,480	2,520			
8	2	45,752,448	14,085,120	1,720,320	80,640		
8	3	667,800	83,160				
8	5	786,240	94,080	20,160			
8	7	12,035,520	3,911,040	584,640	0	0	40,320

word $\omega = g^6h = (1,7)(2,5)(3,8)(4,6)$. Indeed if we consider the group $G = \langle g, h \rangle$, then we see that it is a group of order 56 which has a normal subgroup, N, of order 8 consisting of involutions only. Furthermore the group is isomorphic to the semi-direct product of the normal subgroup and the cyclic group of order 7. The group has the property that every element that is not a member of the normal subgroup has order 7. Now suppose that $g' \in G$ but not in N, and that $\nu \in N$ but is not the identity. We put $h' = g'\nu$, now the natural homomorphism $G \to G/N$ sends both g' and h' to c, an element of order 7 in G/N. Now any positive word, ω on g', h' of length 6 or less will not map to 1 in G/N thus ω is not in N and therefore the element ω has order 7. Now g' and h' have the property that all words of length less than 7 have order 7. Now it is clear that G

is special group, indeed it is a Frobenius group and the Frobenius complement is N, a detailed description of Frobenius groups can be found in [12].

We now seek to generalise the argument given above for other primes. We do this by constructing a similar Frobenius group to that given above.

Theorem 5.3. *Let p be a prime then there exists a group G and elements $g, h \in G$ both of order p such that the shortest positive word on g and h that is not of order p is of length p.*

Before we start the proof of Theorem 5.3 we remind ourselves of some theory originally developed by Singer [13] which we will have recourse to during the proof.

Definition 5.1. A Singer cycle of a finite projective space $\Sigma_{n-1} = PG(n-1, q)$ is a collineation σ such that $\langle \sigma \rangle$ acts regularly on the points of Σ_{n-1}.

The upshot of the existence of Singer cycles is that we may use them to construct automorphisms of vector spaces where all bar one element of the vector space is moved. We now move on to prove Theorem 5.3.

Proof. Let N be a vector space of dimension d over $\mathbb{Z}_2$ and let s be a Singer cycle. The length of s is $2^d - 1$, now $\langle s \rangle$ is a group of order $2^d - 1$. Now if we choose d such that $2^d - 1 = pm$, then we are assured by Sylow's theorem that $\langle s \rangle$ has a subgroup of order p, let t be a generator of this subgroup. Clearly as the elements of $\langle t \rangle$ are in the Singer cycle every element of $\langle t \rangle$ except the identity will move all elements of N bar 1. Now Fermat's theorem tells us that if p is prime and a an integer, then $a^{p-1} \cong 1 \mod p$ so we may pick $d = p - 1$. Now we let $G = N \rtimes \langle t \rangle$ and suppose that $C_G(\langle t \rangle)$ is the centraliser of $\langle t \rangle$ in G. Certainly $\langle t \rangle$ is a subgroup of $C_G(\langle t \rangle)$. Now if ν is in the subgroup N of G corresponding to the original N

and $\nu \in C_G(\langle t \rangle)$, then $\nu^{-1}t\nu = t$ so $t^{-1}\nu t = \nu$, but t moves all of N but 1 so $\nu = 1$. Therefore $N \cap C_G(\langle t \rangle) = 1$. Now $|NC_G(\langle t \rangle)| \leq |G| = |N||\langle t \rangle|$, furthermore $|NC_G(\langle t \rangle)||N \cap C_G(\langle t \rangle)| = |N||C_G(\langle t \rangle)|$ so $|NC_G(\langle t \rangle)| = |N||C_G(\langle t \rangle)|$. Putting these together we get that $|N||C_G(\langle t \rangle)| \leq |N||\langle t \rangle|$. However, we know that $\langle t \rangle$ is a subgroup of $C_G(\langle t \rangle)$ so $\langle t \rangle = C_G(\langle t \rangle)$. Thus the number of elements conjugate to t is the index of $C_G(\langle t \rangle)$ in G, which in turn is $|N|$.

We now seek to show that different conjugates of s generate cyclic groups that intersect trivially. We do this by showing that for $x, y \in G$ if $\langle s^x \rangle$ intersects $\langle s^y \rangle$ non-trivially, then $s^x = s^y$. First suppose that $\langle s^x \rangle$ intersects $\langle s^y \rangle$ non-trivially, now we may conjugate by x^{-1}, if we let $z = yx^{-1}$, then we have $\langle s \rangle$ intersects $\langle s^z \rangle$ non-trivially. Now s and s^z are both of prime order so neither group has a proper subgroup so either $\langle s \rangle = \langle s^z \rangle$ or they intersect trivially.

Observe, we may express every element of G as a power of s times an element of N, thus we may assume that we are conjugating by an element of N rather than an element of G.

Therefore, we may write $z = s^k\nu$ for some integer k and $\nu \in N$ and $\nu \neq 1$ and we have $s^z = \nu^{-1}s\nu$. Now, if the groups coincide then some element of $\langle s \rangle$ must be equal to s^z. This means that $s^l = \nu^{-1}s\nu$ for some integer l, now $s^{l-1}\nu^{-1} = s^{-1}\nu^{-1}s$. Since s normalises N it follows that $s^{l-1}\nu^{-1}$ is in N and therefore s^{l-1} is in N. Now this forces $l - 1$ to be a multiple of p and therefore $s^l = s$ and hence $s = \nu^{-1}s\nu$ and so $\nu = 1$ contrary to our assumption and we are done.

Now we know that we can generate $|N|$ subgroups of G each of size p simply by taking the N conjugates of s and that each of these subgroups intersect trivially. Thus we have constructed $|N|(p-1)$ different elements of order p and together with N this exhausts G so we have shown that all elements not in N have order

p.

Now we use the natural homomorphism

$$\theta : G \to G/N \cong C_p$$

Let $g' \in G$ be of order p and let $h' = \nu g'$ for $\nu \in N$ and $\nu \neq 1$. Now if $(g')\theta = \overline{g'}$, then $(h')\theta = (\nu g')\theta = (\nu)\theta(g')\theta = \overline{g'}$. Now $\overline{g'}$ is of order p as $g' \notin N$ and the image is isomorphic to C_p. We let ω be a word length l on g' and h' and consider $(\omega)\theta$, as $(g')\theta = (h')\theta = \overline{g'}$ then $(\omega)\theta = \overline{g'}^l$. Thus ω is only the identity when p divides l. As the kernel of θ are the only elements of G whose order is not p we have shown that for g' and h' we need a word whose length divides p to generate an element whose order is not p. We now show that there is a word length p that is not the identity by considering $\omega = g'^p h'$, now if $\omega = 1$, then $g'^{-1}\nu g' = 1$ which is impossible as we insisted that ν was not the identity. □

Now the proportion of elements in G with p-power order is $(p-1)/p$, this raises the question is this the best we can do ? It turns out that it is close.

Theorem 5.4. *Let G be a finite group and p a prime. If $|G| = p^n q$ and p and q are co-prime then the proportion of p-power elements is at most $(p^n - 1)/p^n$*

Proof. Let P be a Sylow p-subgroup of of G. The number of Sylow p-subgroups of G is the index of the normalizer of P in G, this is at most q. Now every p-element of G is in a Sylow p-subgroup and there are at most q of these each with at most $p^n - 1$ p-power elements giving at most $p^n q - q$ p-elements and hence at least q non-p-power elements as required. □

Chapter 6

Expressing elements as products of elements of a given shape

In this chapter we look at expressing group elements as products of other group elements. In particular we look at expressing elements as pairs of other elements with a given cycle shape. In essence turning the word problems on their head. In particular we will look at expressing elements in A_n as the product of two l-cycles.

6.1 Previous work

Many results in this chapter are already known although the author arrived at the results independently and our methods often seem to be new or different. The classic reference in this area is Ore [10] who showed that every element in A_n was a commutator of an element in A_n for $n \geq 5$ (and so is a product of two elements with the same cycle shape). The results are included as they inform much of the work of later chapters which use techniques first developed during

this work.

Bertram [1] theorem 2 gives necessary and sufficient conditions on l such that the number of ways a permutation in A_n can be expressed as the product of two l-cycles is greater than zero. The conditions are a bound on the cycle length, l, and (happily) match those given in Theorem 6.26. Our approach is similar to that used by Bertram in that we form disjoint cycles of a given length and then join these together although our approach differs in that we generate a concrete cycle structure for each cycle length and give a concrete method for joining these cycles together. Bertram's work was extended by Boccara [3] to cover cycles of different lengths.

Other work by Walkup [15], Bertram and Wei [2], Stanley [14] and Cangelmi [6] have since given explicit formulae for the number of ways in which a permutation can be expressed as a product of two n-cycles. Walkup uses a recursive approach to solve this problem based on a set of transformations of a permutation. Bertram and Wei [2] develop a recursion that allows the explicit calculation of the number of ways a permutation may be expressed as a product of an n-cycle and an $(n-i)$-cycle. Finally, Cangelmi [6] has shown using combinatorial methods that the number of ways an n-cycle, n odd, can be expressed as a product of n-cycles is $\frac{2(n-1)!}{n+1}$, this method is then extended to cover other element of S_n.

As far as we are aware Theorem 6.13 is novel as are the results in section 6.7. Lemma 6.15 is a more explicit statement of a result implicit in Bertram [1].

6.2 Preliminary results

Before we can begin the work proper of this chapter we must first show what is not possible. We do this via the following lemma.

Lemma 6.1. *Let c be a cycle shape in S_n then there exists $g \in S_n$ such that g cannot be expressed as a product of two elements with cycle shape c*

Proof. We need only pick g as an odd element of S_n as the product of two even or two odd elements is always even. □

This tells us that we cannot express odd elements of S_n as a product of two similar shape elements. However, as every odd element may be expressed as an even element times a transposition we may deduce the following.

Lemma 6.2. *Let c be a cycle shape in A_n then if every element of A_n can be expressed as a product of two elements of shape c then every element of S_n can be expressed as a product of at most two elements of shape c and a transposition*

Proof. Even elements of S_n can be expressed as a product of two c shape elements by the hypothesis and all odd elements of S_n can be expressed as an even element multiplied by a single transposition □

6.3 Elements in A_p as products of p cycles

We motive ourselves via the following well known theorem.

Theorem 6.3. *For $n \geq 5$, n odd, A_n is generated by the n-cycles*

Proof. For $n \geq 5$ A_n is simple. Now the subgroup of A_n generated by the n-cycles is invariant under conjugation and hence is normal and non-trivial. But as A_n is simple it must be A_n. □

Of course the theorem is also true for $n = 3$ as it consists solely of the 3-cycles. Having shown that the p-cycles generate A_p we now turn our attention to the following related theorem.

Theorem 6.4. *Let $g \in A_p$ for p an odd prime then there exists x, y both p-cycles in A_p such that $g = xy$.*

Theorem 6.4 states that every element of A_p can be expressed as a product of two p-cycles. An alternative formation of Theorem 6.4 would be:

Theorem 6.5. *For p an odd prime let Π be the set of p-cycles in A_p. Then $A_p = \{p_1 p_2 | p_1, p_2 \in \Pi\}$.*

Before we can attempt to prove Theorem 6.4 we need a few preliminaries. The first observation is that we need not worry about showing that each element of A_p can be expressed as a product of two p-cycles merely that one representative of each conjugacy class can be expressed as a product of two p-cycles as, if this is true, then we simply need to conjugate the representative and x and y by a suitable element of A_p. However, while it is true that in S_p elements with the same cycle structure are conjugate this is not true in A_p, this need not worry us as we may conjugate by an element in S_p and be assured that the result will be within A_p. Therefore, we need not generate a representative of each conjugacy class merely an element with each cycle shape. We now deal with the trivial cases.

Lemma 6.6. *The identity element in A_p may be expressed as a product of two p-cycles*

Proof. Take a p-cycle and its inverse. □

Lemma 6.7. *A p-cycle in A_p may be expressed as the product of two p-cycles*

Proof. Let g be our p-cycle then g^2 and g^{-1} are p-cycles and $g^2g^{-1} = g$ □

We note that for Lemma 6.7 to be true we do not need p to be prime merely for it to be odd as this will ensure that g^2 has the same shape as g. We will have recourse to this more general version of Lemma 6.7 later.

With these preliminary cases now dealt with we turn to the more general case. First we fix on a standard shape representative for each cycle shape, for convenience we shall assume this to be the element achieved by filling the cycle shape by writing the elements in ascending order and the cycles in descending length order. For example if the shape were $(x, x, x, x)(x, x, x)$, then the standard shape representative would be $(1, 2, 3, 4)(5, 6, 7)$. We formalise this:

Definition 6.1 (Standard Shape Representative). Let $\Omega = \{1, 2, \ldots, n\}$ and $S = Sym(\Omega)$ then a standard shape representative,c, is an element of S such that the orbits of c have the form $(a, a+1, a+2, \ldots, a+b)$ and if $i < j$, then the orbit of i is at least as large as the orbit of j.

We note that our definition means that each conjugacy class in S_n will have a single standard shape representative. We also note that the definition applies equally in the alternating group but here two conjugacy classes may share the same standard shape representative. For many purposes we do not require that the cycle lengths are weakly decreasing although we will need this condition in Chapter 7. We note that in many cases we can alter the ordering of the cycles by conjugation in S_n. For example, $g = (1, 2, 3, 4)(5, 6, 7)(8, 9)$ is a standard shape representative in S_9 if we wanted to we could conjugate g by $h = (1, 4, 6, 2, 5)(3, 7)$ in order to move the 3-cycle to the front, we will use this flexibility later. The

notion of a standard shape representative is as far as the author is aware novel but is critical to the brevity of argument presented, without this notion the exposition would be significantly more complex.

Conjecture 6.8. *Let $p > 3$ be a prime and $g = (1, 2, \ldots, p)$ and let c be a standard shape representative excluding the identity and p-cycles. Then there exists $h \in < g >$ such that ch is a p-cycle*

On the face of it this seems a wholly unlikely conjecture. However, computation in GAP shows that the conjecture is true for $5 \leq p \leq 61$.

Conjecture 6.8 is true and a proof is given as Theorem 6.27. Observe that with a proof of Conjecture 6.8 we would be able to complete our proof of Theorem 6.4 via the observation that $chh^{-1} = c$ and is a product of two p-cycles as required. We elect not to prove Conjecture 6.8 now and instead use the following construction of a p-cycle.

Lemma 6.9. *If $c = c_1 c_2 \ldots c_n \in A_p$, for p prime such that:*

- *If c_i is an odd length cycle, then so is c_{i-1}.*
- *Each c_i is of the form $(j, j+1, j+2, \ldots, j+m)$.*
- *If j is the largest element of the support of c_i, then $j+1$ is in the support of c_{i+1} unless $i = n$ in which case it is in the stabiliser of c.*

We assume that the c_i are of length $l_i - l_{i-1}$ with $l_0 = 0$ and let

$$h = (1, 2, \ldots, l_1{-}1, l_1{+}1, l_1{+}2, \ldots, l_2{-}1, l_2{+}1, \ldots, l_n{-}1, l_1, l_2, \ldots, l_n, l_n{+}1, l_n{+}2, \ldots, p)$$

Then ch is a p-cycle.

The construction in Lemma 6.9 is best shown by illustration. Let $c = (1,2,3,4,5)(6,7,8)$ and $p = 11$ then $h = (1,2,3,4,6,7,5,8,9,10,11)$ and $ch = (1,3,6,5,2,4,8,7,9,10,11)$. We initially assure ourselves that Lemma 6.9 is true by direct calculation in GAP.

Proof. We wish to consider the orbit of a given element in order to show it is of size p. First we consider the images of $l_i - 2$, $l_i - 1$ and l_i respectively under ch.

The image of $l_i - 2$ will be $l_i + 1$ except where $i = n$. When $i = n$ it will be l_1.

The image of $l_i - 1$ will be l_{i+1} except where $i = n$. When $i = n$ it will be $l_n + 1$.

The image of l_i will depend on the length of c_i. If c_i is a transposition, then it will go to $l_i + 1$ unless $i = n$, in which case it will go to $l_n + 1$. If c_i is not a transposition it will be $l_{i-1} + 2$.

For every other element, j, in each cycle its image will be $j + 2$. We also observe that if $l_n < p$, then for $l_n < j < p$ the image of j under ch is $j + 1$, the image of p is 1.

Now the image of 1 will traverse all of the odd elements, except the l_i, in the odd length cycles. If there are no even length cycles, then the image will then go to l_1 and then traverse the even elements of c_1 until $l_1 - 1$ whose image is l_2 and so on until c_n where the image of $l_n - 1$ will be $l_n + 1$. We now traverse the stabilizer of c until p where we return to 1 and we are done.

If c has some even length cycles, then these elements must come in pairs as c is even and even length cycles are odd. We consider each pair in turn. If c_i and c_{i+1} are the first such pair then the image will go to $l_{i-1} + 1$ and traverse the odd elements of c_i until it reaches $l_i - 1$ when it will go to l_{i+1} followed by $l_i + 2$ then traverse the even elements of c_{i+1} until the $l_{i+1} - 2$ it will then go to $l_{i+1} + 1$.

This will continue until c_n when the image will be l_i. The argument continues as above with the image traversing the remaining elements of the odd cycles until $l_{i-1}-1$ is reached. The image of this element will be l_i and its image in turn will be $l_{i-1}+2$ and the even elements of c_i will be traversed until l_i-2 whose image will be l_i+1 the odd elements of c_{i+1} will be traversed until $l_{i+1}-1$. If $i+1=n$, then its image will be l_n+1 if not, then it will be the $l_{i+1}+1$ and the pattern continues.

The argument above follows even where c contains transpositions but this is far from clear so is set out in more detail below.

If c contains an even number of transpositions, then the image goes to the first point of the first transposition followed by the second point of the second transposition and then the first element of the next pair. When we arrive back at the pair we will go first to the second element of the first transposition then the first element of the second. We then go to the second element of the first of the next pair or the first point stabilized by c.

If c contains an odd number of transpositions, then we must deal with the case where there is an even length cycle of length greater than two and a transposition in a pair. Let c_i be the even length cycle and c_{i+1} the transposition. The image goes to the $l_{i-1}+1$ and traverses all of the odd elements followed by l_i+2 and then l_i+3. When we arrive back at the pair we will go first to l_i then the even elements of c_i until l_i-2 when we go l_i+1. We then go to $l_{i+1}+2$ if c_{i+1} is not the last cycle or l_n+1 if it is. □

Now Lemma 6.9 appears to be extremely restrictive in its application as it places specific requirements on the support of c as well the ordering of the support of each cycle and the ordering of the cycles. However, we note that if c' is any

element in A_p with the same cycle decomposition as c then there exists an $x \in S_p$ such that $c' = c^x$, furthermore $(ch)^x = c^x h^x = c' h^x$ will be a p-cycle and h^x will be a p-cycle in A_p. We can use this observation to generalise Lemma 6.9 to cover any element of A_p.

Lemma 6.10. *If $c \in A_p$, then there exists a a p-cycle $h \in A_p$ such that ch is a p-cycle.*

Having completed the proof of Lemma 6.10 we are now in a position to be able to prove Theorem 6.4

Proof of Theorem 6.4. First we use Lemmas 6.6 and 6.7 to dispose of the trivial cases. Now we turn to the non-trivial cases. For $p = 3$ the conjecture is manifestly true. Now for $p > 3$, we can use Lemma 6.10 to find a p-cycle, h, such that ch is a p-cycle. Now h^{-1} is also a p-cycle and $(ch)h^{-1} = c$ as required. □

We now note that we have not relied on p being prime in the proof of Theorem 6.4 merely that the p-cycles are in A_p. Furthermore, we have already noted that Lemma 6.7 applies when p is odd so we may deduce the following corollary.

Corollary 6.11. *Let $g \in A_n$ for n odd then there exists x, y both n-cycles in A_n such that $g = xy$*

We already know from Lemma 6.1 that we cannot express every element of S_n as a product of two n-cycles. Therefore, the best we can do is express every element in S_n, n odd, as the product of two n-cycles and a transposition.

6.4 A_n as a product of $(n-1)$-cycles for n even

Having shown that we can express every element of A_n as a product of n-cycles for n odd we now turn our attention to n even. For n even the n-cycles are odd

permutations and hence are not in A_n. Instead we turn our attention to the $(n-1)$-cycles. First we observe that for elements of A_n with non-trivial stabiliser we may consider them as elements of A_{n-1} and apply Corollary 6.11. This means we need only consider those elements of A_n that have no fixed points. We now examine the proof of Theorem 6.10 and note that we have not required that n be odd, this requirement came in order to allow the n-cycles to be included in A_n. Now if there exists $h' \in S_n$ such that ghh' is an $(n-1)$-cycle and $h'^{-1}h^{-1}$ is also an $(n-1)$-cycle, then we would be done. The obvious choice for h' is the transposition consisting of the first and last elements of gh, unfortunately $h'^{-1}h^{-1}$ may not be an $(n-1)$-cycle. Direct computation in GAP shows it is not sufficient for h' to be a single transposition . However, a 4-cycle is sufficient, we construct the required 4-cycle as follows let $h' = (1, n, a, b)$ where a is the element preceding n in the cycle gh and b is the element preceding 1 in the cycle gh.

Theorem 6.12. *Let $g \in A_n$ for $n \geq 4$ even then there exists x, y both $(n-1)$-cycles in A_n such that $g = xy$*

Proof. We first use Theorem 6.4 to dispose of the elements which stabilise at least one point as these may be considered elements of A_{n-1}.

We now turn our attention to the elements with no fixed points. Again we construct h as in Theorem 6.4. We then construct $z = (1, n, a, b)$ where a is the element preceding n in the cycle gh and b is the element preceding 1 in the cycle gh. Now we consider the following construction $ghzz^{-1}h^{-1} = g$, it is clear that the product ghz and $z^{-1}h^{-1}$ has the required cycle structure. However, we still need to prove that z is well defined and that ghz and $z^{-1}h^{-1}$ are both $(n-1)$-cycles.

First we show that z is always a cycle, this will only not be the case if $a = b$,

$a = 1, n$, or $b = 1, n$. We deal with the case $a = b$ by observing that b precedes 1 and a precedes n so they cannot be equal unless $n = 1$ which is absurd. Equally a cannot be n as it precedes it and b cannot be 1 as it precedes it. This leaves only the cases where $a = 1$ or $b = n$. We observe from the proof of Theorem 6.4 that if there are no even length cycles, then the orbit of 1 in gh will traverse the final element of the final cycle i.e. n before traversing the even position elements and so $b \neq n$. However, if there are some even length cycles, then n will be covered as the orbit first passes the last even cycle and again $b \neq n$. As before we consider which element precedes n in gh using the proof of Theorem 6.4, the pre-image of n will be the penultimate element of the penultimate cycle which can only be 1 if $g = (1,2)(3,4)$ so $a \neq 1$ for $n > 4$.

Next we consider ghz, now gh is an n-cycle. As $(a)gh = n$ and $(n)z = a$, a is fixed by ghz so the support is at most size $n - 1$. We still need to show that ghz is an $(n-1)$-cycle. We consider the orbit of 1 and we see that it continues as in gh until it reaches the element preceding a, the image of this will be b whose image will in turn be n (the element after a) and the cycle will continue as in gh from n, so we are assured that ghz is a single cycle and the only point stabilised by ghz is a so it has support size $n - 1$ as required.

Finally we consider $z^{-1}h^{-1}$, now $z^{-1} = (1, b, a, n)$. As h is an n-cycle our construction ensures that $(1)h^{-1} = n$ and $(n)z^{-1} = 1$ so n is fixed by $z^{-1}h^{-1}$. First we look at what order $1, n, a, b$ appear in the orbit of 1 under h^{-1}. Consider $(n-1)gh$, now $(n-1)g = n$ as we have insisted that the support of g is of size n and each cycle lists elements in ascending order. Equally, as g has no fixed points the construction of h yields that $(n)h = 1$ so $(n-1)gh = 1$ and therefore $b = n-1$, in h^{-1} this will be the first element after the last element of each cycle is covered. Now, a precedes n in gh so will be the penultimate element of the penultimate

cycle of g, thus in h^{-1} it will follow b. So $h^{-1} = (1, n, \ldots, b, \ldots, a, \ldots)$

Consider the orbit of 1 under $z^{-1}h^{-1}$. First the orbit will go to the image of b under h^{-1}, it will then continue as in h^{-1} until it hits a. In the case it hits a it will then go to the third element of h^{-1} and continue until it hits b whose image will be $(x)h^{-1}$ and the cycle will now continue back to 1.

We have now completed the proof for $n > 4$, to prove the result for $n = 4$ we simply observe that $(1,2,3)(1,2,4) = (1,4)(2,3)$ which is the only other cycle shape in A_4. □

6.5 Other spanning elements

Having covered the longest cycles in A_n we next consider whether we can use the same treatment on pairs of elements whose support is n. We first attack this via direct computation in GAP. We quickly discover that if c is an element shape in A_n with support n, then we cannot always express $g = c_1c_2$ for $g, c_1, c_2 \in A_n$ and c_1, c_2 of shape c. First we demonstrate this by example, let $n = 4$, the only elements with no fixed points are of the form $(\alpha, \beta)(\gamma, \delta)$, of which there are 3 such elements, these, together with the identity, form a group of size 4. Therefore, not all elements of A_n can be expressed as a product of these cycles.

A similar effect can be seen for larger groups. Table 6.1 shows the spanning cycle shapes where not all elements of A_n can be expressed as a product of two elements with the given cycle shape.

Theorem 6.13. *Let n be even and Ω be of size n, and let Π be the set of elements in S_Ω composed of precisely $n/2$ disjoint transpositions then only elements with an even number of each cycle shape may be expressed as a product of two elements of Π. Moreover, for each transposition only one point will appear in each cycle.*

Table 6.1: Non-generating spanning shapes in A_n

n	Bad cycle shapes
4	(1,2)(3,4)
5	None
6	(1,2,3)(4,5,6)
7	None
8	(1,2)(3,4)(5,6)(7,8)
9	(1,2,3)(4,5,6)(7,8,9)
10	None
11	None
12	(1,2)(3,4)(5,6)(7,8)(9,10)(11,12) and (1,2,3)(4,5,6)(7,8,9)(10,11,12)

Proof. Consider $g, h \in \Pi$. We observe that if we can partition the support such that each transposition in g, h only moves elements in one subset, then we may consider each subset in the partition separately. There exists a partition of Ω such that each subset is of minimal size. Each subset will be of even size, the subsets of size two are trivial as they imply g and h contain the same transposition resulting in two cycles of length 1.

Let $\overline{\Omega}$ be a subset in the minimal partition of Ω for g and h and let g', h' be g, h restricted to $\overline{\Omega}$.

We proceed by induction on k, the size of $\overline{\Omega}$. Assume that we may pick $\overline{\Omega}_m$ of size $2m < k$ and g_m, h_m such that:

1. g_m is identical to g' restricted to $\overline{\Omega}_m$.

2. h_m contains at most one transposition not in h' and acts identically to h' on the rest of $\overline{\Omega}_m$.

3. g_m and h_m satisfy the theorem.

We are assured that we may pick g_2 and h_2 that satisfy conditions 1 and 2 as we may pick any transposition in h' and the two transpositions in g' whose

support intersects our chosen transposition in h' non-trivially. We then complete h_2 with a transposition drawn from the remainder of $\overline{\Omega}_2$. Now there are six possible ordered pairs of transpositions with support size 4 and direct calculation shows:

$$\begin{aligned}
(\omega_1,\omega_2)(\omega_3,\omega_4).(\omega_1,\omega_3)(\omega_2,\omega_4) &= (\omega_1,\omega_3)(\omega_2,\omega_4).(\omega_1,\omega_2)(\omega_3,\omega_4) \\
&= (\omega_1,\omega_4)(\omega_2,\omega_3) \\
(\omega_1,\omega_2)(\omega_3,\omega_4).(\omega_1,\omega_4)(\omega_2,\omega_3) &= (\omega_1,\omega_4)(\omega_2,\omega_3).(\omega_1,\omega_2)(\omega_3,\omega_4) \\
&= (\omega_1,\omega_3)(\omega_2,\omega_4) \\
(\omega_1,\omega_3)(\omega_2,\omega_4).(\omega_1,\omega_4)(\omega_2,\omega_3) &= (\omega_1,\omega_4)(\omega_2,\omega_3).(\omega_1,\omega_3)(\omega_2,\omega_4) \\
&= (\omega_1,\omega_2)(\omega_3,\omega_4)
\end{aligned}$$

Thus we are assured the theorem is true for $k = 4$ and furthermore where $k > 4$ we may pick a subset of size 4 that satisfies our induction hypothesis.

Now for $k > 4$ let (a, b) be the transposition in h_m which is not in h' and let $(a)h' = \alpha$ and $(b)h' = \beta$. Now we are assured that $\alpha, \beta \notin \overline{\Omega}_m$ or h_m would differ from h' in more than one place. Now assume $(a)g' = \gamma$, now $\gamma \notin \overline{\Omega}_m$ as we have insisted that $g_m =_{\overline{\Omega}_m} g'$. Let $g_{m+1} = g_m(\alpha, \gamma)$ so g_{m+1} satisfies condition 1.

Now $(\gamma)h' \notin \overline{\Omega}_m$ or h_m would differ from h' by more than one transposition. Let $h_{m+1} = h_m(b, \alpha)(b, a)(b, \gamma)$. Now $(a, b)(b, \alpha)(b, a)(b, \gamma) = (a, \alpha)(b, \gamma)$ so h_{m+1} satisfies condition 2.

Now condition 3 assures us that in $g_m h_m$ a and b are in different cycles as they are in the same transposition in h_m. Now

$$\begin{aligned} g_{m+1}h_{m+1} &= g_m(\alpha,\gamma)h_m(b,\alpha)(b,a)(b,\gamma) \\ &= g_m h_m(\alpha,\gamma)(b,\alpha)(b,a)(b,\gamma) \\ &= g_m h_m(\alpha,b)(a,\gamma) \end{aligned}$$

Now the effect of multiplying $g_m h_m$ by $(\alpha,b)(a,\gamma)$ will be to insert an α into the cycle containing b and a γ into the cycle containing a. Therefore, each cycle will increase in length by one. Furthermore, α and γ are in different cycles as are a and α, and b and γ and g_{m+1}, h_{m+1} satisfy condition 3. Finally we observe that when $2m = |\overline{\Omega}|$ the construction works with $\gamma = \beta$ and we are done. □

Theorem 6.14. *Let $n > 2$ be even and let Π be the set of elements in A_n composed of precisely $n/2$ disjoint transpositions then there exist elements of A_n which cannot be expressed as product of two elements from Π.*

Proof. We may either deploy Theorem 6.13 and observe that there are elements in A_n whose cycle structure is not symmetrical.

Alternatively we may employ the following argument

First we observe that there are $\frac{n!}{2}$ elements in A_n, now if Π has size S, then there are at most S^2 distinct elements generated by pairs of elements of Π.

Now $S = \frac{n!}{2^{\frac{n}{2}}\frac{n}{2}!}$ so $S^2 = \frac{n!^2}{2^n \frac{n}{2}!^2}$ we need only show that $2^{n-1}(\frac{n}{2}!)^2 > n!$ and we are done.

It is clear that this is true for $n \leq 4$. We proceed by using induction, we know the result is true for $n \leq 4$ and we assume it is true for $n = m$ and proceed to

show it follows for $n = m + 4$.

$$\begin{aligned}
2^{m+4-1}\left(\frac{m+4}{2}!\right)^2 &= 2^4 2^{m-1}\left(\frac{m+4}{2}\right)^2\left(\frac{m+2}{2}\right)^2\left(\frac{m}{2}!\right)^2 \\
&= (m+4)^2(m+2)^2 2^{m-1}\left(\frac{m}{2}!\right)^2 \\
&\geq (m+4)^2(m+2)^2 m! \\
&> (m+4)(m+3)(m+2)(m+1)m! \\
&= (m+4)!
\end{aligned}$$

So $2^{n-1}(\frac{n}{2}!)^2 > n!$ as required and we are done. □

6.6 Other elements with large support

We now observe that we need not necessarily insist that the elements have support size n or even $n-1$. However, we note that we must place some constraints on the size of the support namely that it must have size greater than $\frac{n}{2}$ as if the support is smaller than this it would not be possible to generate an element with no fixed points. Equally we require the number of elements with the given shape to be greater than $\sqrt{\frac{n!}{2}}$ or there will be insufficient pairs to generate $\frac{n!}{2}$ distinct elements.

Looking at these constraints only we can relatively quickly establish the number of element shapes which have a support greater than $n/2$ but where there are insufficient elements of the given shape. The number of such bad shapes is given in Table 6.2.

Looking back to Table 6.1 we can see that there are 2 elements shapes with

Table 6.2: Element shapes with large support that cannot generate A_n

n	Total big shapes	Bad shapes
4	2	1
5	3	0
6	4	0
7	6	0
8	9	1
9	13	0
10	18	0
11	25	0
12	34	1
13	46	0
14	61	0
15	82	1
16	106	1
17	139	0
18	179	0
19	232	0
20	295	1
21	378	1
22	476	1
23	603	1
24	753	1
25	945	1
26	1,172	1
27	1,460	1
28	1,798	3
29	2,222	2
30	2,721	1

no fixed points where not every element of A_{12} can be expressed as a pair of elements of the given shape yet our estimate says there is only one. It is clear that our naive estimate is not sufficient.

We note that while there are over 1,400 times more pairs of 7-cycles in A_{11} than there are elements in A_{11} it is still not possible to express every element as a product of two 7-cycles. It fails for the single conjugacy class contain-

ing $(1,2,3)(4,5)(6,7)(8,9)(10,11)$. The same applies for 5-cycles in A_9 where the conjugacy classes containing the following elements $\{(1,2)(3,4)(5,6)(7,8)$, $(1,2,3)(4,5,6)(7,8,9), (1,2,3,4)(5,6,7)(8,9), (1,2,3,4,5)(6,7)(8,9)\}$.

6.6.1 $(n-2)$-cycles for n odd

Despite showing that there are element shapes with large support where we cannot express every element of A_n as a product of two elements of the given shape there is some hope that we may be able to do so for some shapes. We turn our attention to the $(n-2)$-cycles in A_n where n is odd. Firstly we observe, that for those elements where the size of the support is less than $n-1$ we can simply use the construction of Theorem 6.4 on the smaller support. This leaves the problem of elements whose support has more than $n-2$ elements. We remind ourselves of the basic construction of Theorem 6.4, if $g \in A_n$ then we try to find h such that gh is a n-cycle then gh and h^{-1} are the required n-cycles.

Before we can show that every element in A_n, for n odd, can be expressed as two $(n-2)$-cycles we need the following preliminary result.

Lemma 6.15. *Let $g \in A_n$ with $g = g_1 g_2$ where $g_1, g_2 \in S_n$ have disjoint support. Then if there exists $h_1, h_2 \in S_n$ such that*

- *$Supp(h_i) \subseteq Supp(g_i)$ $i \in \{1,2\}$*
- *h_i is a single cycle*
- *$g_i h_i = c_i$ is a cycle length k_i and $Supp(h_i) \cap Supp(c_i) \neq \emptyset$*

Then there exists h a single cycle such that gh is a single cycle, c, of length $k_1 + k_2$. Moreover h has length equal to the sum of the lengths of h_1 and h_2.

Proof. By design $g_1h_1g_2h_2 = c_1c_2$ and since the support of h_1 is disjoint from g_2 we may change their order so $g_1g_2h_1h_2 = gh_1h_2 = c_1c_2$. Now we choose a transposition $t = (t_1, t_2)$ such that it consists of an element from $Supp(h_1) \cap Supp(c_1)$ and one from $Supp(h_2) \cap Supp(c_2)$. We observe that post multiplying h_1h_2 by t will have the effect of joining h_1 and h_2 (see Figure 6-1), similarly it will join c_1 and c_2. Now we let $h = h_1h_2t$ which is a single cycle then $c = c_1c_2t$ a cycle of length $k_1 + k_2$ as required. We note that h has length equal to the sum of the lengths of h_1 and h_2

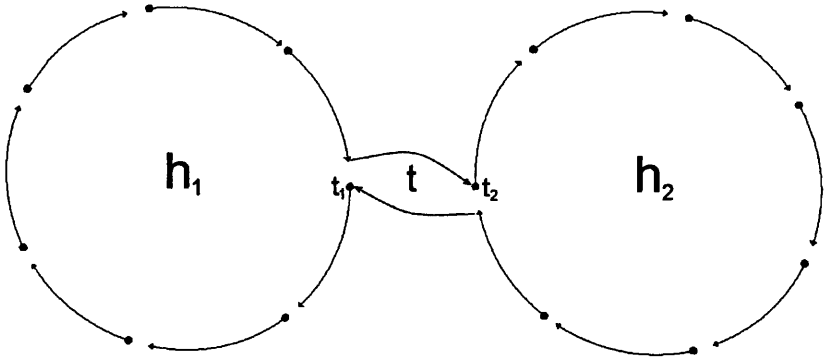

Figure 6-1: Joining cycles with a transposition

□

Lemma 6.15 is important as it allows us to break the problem of finding cycles into smaller problems. Essentially with Lemma 6.15 in our arsenal we can find a suitable cycle for each cycle in g and then stitch them together to form the required cycle.

We first note that for $n = 3$ an $(n-2)$-cycle would be a cycle of length 1 so we will need to insist that $n > 3$.

Theorem 6.16. *For $g \in A_n$, $n > 3$ odd, there exist $x, y \in A_n$ both $(n-2)$-cycles such that $g = xy$*

Proof. As before we observe that treating the elements of A_n as elements of S_n we need only generate one member of each conjugacy class in S_n as we may obtain all other members of the conjugacy class by conjugation in S_n. Furthermore, we note that if the size of the support of g is less than $n-1$ then we can use the construction of Theorem 6.4 treating g as if it were in A_{n-2}. Equally, we note that for elements whose support is of size $n-1$ their support is of even size and we may consider these as elements of A_{n-1} and we may apply Theorem 6.12 as our cycles are one shorter than $n-1$ as required in that theorem.

This leaves us only the cases where the support has size n. The general construction is similar to that used in Theorem 6.4, in that we attempt to construct h, a cycle of the required length, such that gh is a cycle of the same length. We also have recourse to the detailed construction used in Theorem 6.4 and the general approach is the same in all cases. Now let g have support size n, we want h to be an $(n-2)$-cycle. Now we split g so that $g = g_1 g_2$ where g_1 and g_2 have disjoint support. We use all but 2 of the support of g_1 to form the cycle h_1 and all of the support of g_2 to form the cycle h_2, thus the length of h_1 plus the length of h_2 is $n-2$. It may be that g is a single cycle in which case we cannot split g as described, in this case we simply take $g_2 = h_2 = ()$. We note that we may always allow $g_2 = h_2 = ()$.

We now further restrict our choice of h_1 and h_2 such that $g_1 h_1$ and $g_2 h_2$ are both single cycles whose supports have non trivial intersection with the supports of h_1 and h_2 respectively. We may then deploy Lemma 6.15 to show that we can use h_1 and h_2 to form a single cycle h of length $n-2$ such that gh is a single cycle also of length $n-2$. Clearly where $g_2 = id$ we may omit this step.

First we deal with h_2. Provided $h_2 \neq ()$ we use the construction of Theorem 6.4. We note that in proving Theorem 6.4 we did not use the fact that p

was odd except to ensure that p-cycles existed in A_p. In order to allow ourselves greater choice of h_2 we relax this restriction and instead work in the symmetric group on the support of g_2 as the application of Lemma 6.15 will ensure we end up in A_n. However, the proof of Theorem 6.4 did rely on the fact that the shape contained an even number of even cycles. We note that g_2 will satisfy this condition provided g_1 contains odd cycles only or an even number of even length cycles, we will ensure this happens in all cases.

We now address our choice of g_1 and hence h_1 this will depend on the structure of g.

First we note that g must contain a cycle of odd length as n is odd. We have four cases:

1. g contains an odd cycle of length greater than 5
2. g contains a 5-cycle
3. g contains a 3-cycle
   (a) g contains 3 3-cycles
   (b) g contains only one 3-cycle

We give a separate construction for each case assuming in each case that the conditions of the previous cases are not met:

1. Assume the long odd cycle is $(1, 2, \ldots, k)$ and let g_1 be this cycle. Now we let $h_1 = (1, 2, \ldots, k-5, k-1, k-2, k-3)$ which gives

$$g_1 h_1 = (1, 3, \ldots, k-6, k-1, k, 2, 4, \ldots, k-5, k-4)$$

   Thus $g_1 h_1$ has support size $k-2$ as required.

2. Assume the 5-cycle is $(1,2,3,4,5)$ and let g_1 be this cycle. Now let $h_1 = (1,5,4)$ now $g_1h_1 = (1,2,3)$ which has support size 3 as required.

3. We note that if g contains a 3-cycle it must contain at least one other cycle as we have insisted that $n > 3$. Furthermore if g contains another 3-cycle then g must contain at least two other cycles as a single odd cycle would give g an even size support and we insisted n was odd equally even cycles must come in pairs. Therefore there are two sub-cases, the first where g contains at least 3 3-cycles, the second where g contains one 3-cycle and at least two even length cycles.

   (a) Assume the 3 3-cycles are $(1,2,3)(4,5,6)(7,8,9)$ and let g_1 be these cycles. Now let $h_1 = (1,3,2,4,5,6,7)$ now $g_1h_1 = (1,4,6,5,7,8,9)$ a 7-cycle as required.

   (b) If none of the previous conditions are met, then every cycle in g bar the 3-cycle is of even length. Now if there are two cycles which are not transpositions with lengths k_1 and k_2 respectively then we may assume

$$g_1 = (1,2,3)(4,5,\ldots,k_1+3)(k_1+4,k_1+5,\ldots,k_1+k_2)$$

   Now let

$$h_1 = (1,3,2,4,\ldots,k_1+3-2,k_1+3,k_1+4,\ldots,k_1+k_2+3-2,k_1+k_2+3),$$

   So colloquially h_1 is the inverse of the 3-cycle followed by the support of each of the even length cycles but omitting the penultimate element in

each case. Therefore, it is clear h_1 has length k_1+k_2+1. Now we turn our attention to g_1h_1. First we note that $(2)g_1h_1 = 2$ and $(3)g_1h_1 = 3$ so g_1h_1 has support at most $k_1 + k_2 + 1$. We now consider the orbit of 1, the orbit begins $1, 4, 6$ it then traverses the even elements of the first even cycle, excluding $k_1 + 2$, followed by $k_1 + 3$ and the traverses the odd elements of the first even cycle followed by $k_1 + 2$ and then repeats this pattern on the support of the second even cycle before returning to 1 and we conclude g_1h_1 is of length $k_1 + k_2 + 1$. This is best illustrated by the following concrete example let

$$g_1 = (1, 2, 3)(4, 5, 6, 7, 8, 9)(10, 11, 12, 13)$$

and then

$$h_1 = (1, 3, 2, 4, 5, 6, 7, 9, 10, 11, 13)$$

so

$$g_1h_1 = (1, 4, 6, 9, 5, 7, 8, 10, 13, 11, 12).$$

We note that if we are forced to use a single transposition the same construction works. If g consists of a single 3-cycle and transpositions only then we may assume $g_1 = (1, 2, 3)(4, 5)(6, 7)$ and let $h_1 = (1, 3, 2, 4, 6)$ now $g_1h_1 = (1, 4, 5, 6, 7)$

We have now given a construction for all possible elements of A_n and we are done. □

While Theorem 6.16 is interesting in its own right we are forced to ask are $n-2$ cycles the shortest cycles that may be used in this way or are there other i such that every element of A_n can be expressed as the product of two $n-i$ cycles.

We look back to the proof of Theorem 6.16 and see that there does not appear to be any reason why a similar approach could not be adopted for larger i assuming sufficiently large n. Indeed, we note that Theorem 6.16 effectively contains an induction step for all elements whose support is of size $n-1$ or smaller. While it is clear that for large i the number of cases may become unwieldy there is certainly scope for extending this sort of construction a little further and we turn our attention to the case where $i = 3$.

6.6.2 $(n-3)$-cycles for n even

Before we may start we observe that for even n less than 8, $n - 3 \leq \frac{n}{2}$, therefore $(n-3)$-cycles will not be able to generate elements whose support is of size n and we shall not consider such small n. Now we may proceed with the general case where n is sufficiently large.

Theorem 6.17. *For $g \in A_n$, $n \geq 10$ even, then there exist $x, y \in A_n$ both $(n-3)$-cycles such that $g = xy$*

Proof. As before we note that for elements whose support is smaller than $n-2$ we may simply treat them as elements of A_{n-2} and apply Theorem 6.12. Again we are left with elements whose support is of size $n-1$ or n.

We now use Theorem 6.16 as a guide and start with the case where the support has size $n-1$. We note that in this case the elements can be considered as elements of A_{n-1}, now $n-1$ is odd and an $(n-3)$-cycle has support two smaller than $n-1$ and we may apply the case where the support has size n of Theorem 6.16 directly.

This leaves only the case where elements have support size n. We have six cases, in each case we give a construction that takes takes a support of size k and

gives a cycle of length $k-3$, we then use the construction of Theorem 6.4 on the remaining support using Lemma 6.15 to get a single cycle. We note that as in corollary 6.11 that the construction works for all odd n.

1. g has an odd cycle of length greater than 5.
2. g contains a 5-cycle.
3. g contains a 3-cycle.
   (a) g contains at least 3 3-cycles.
   (b) g contains two 3-cycles.
4. g contains two even cycles of length greater than 2.
5. g contains only one even cycle of length greater than 2.
6. g consists solely of transpositions.

We provide a construction in each case assuming in each case that the conditions of the previous cases are not met:

1. Assume the long odd cycle is $(1,2,\ldots,k)$ and let g_1 be this cycle now let $h_1 = (1,2,\ldots,k-3,k-4,k-5,k-6)$ now

$$g_1h_1 = (1,3,\ldots,k-3,k-2,k-1,k,2,4,\ldots,k-7).$$

   g_1h_1 has support $k-3$ as required. We may also apply Theorem 6.4 to g_2, h_2 as there are an odd number of elements.

2. Assume the 5-cycle is $(1,2,3,4,5)$ and let g_{1_1} be this cycle. Now as n is even g must contain at least one other odd length cycle $(6,7,\ldots,k+5)$ let this be

g_{1_2}. Now we choose $h_{1_1} = (3,2,1)$ so that $g_{1_1}h_{1_1} = (3,4,5)$ which has length 3. Now g must contain another odd length cycle and it must be length 3 or 5, if it is length 3 we may assume $g_{1_2} = (6,7,8)$ and then $h_{1_2} = (7,6)$ giving $g_{1_2}h_{1_2} = (7,8)$. If the other odd cycle is length 5 we may assume $g_{1_2} = (6,7,8,9,10)$ and then $h_{1_2} = (6,7,9,8)$ giving $g_{1_2}h_{1_2} = (6,9,10,7)$. In both cases the size of the support of the cycle is one less than the size of the support of g_{1_2} as required. We now use Lemma 6.15 to join the results.

3. g contains a 3-cycle assume this is $(1,2,3)$ and let g_1 be this cycle, we now consider two different cases depending on if g contains two other 3-cycles.

   (a) We may assume the 3-cycles are $(1,2,3)(4,5,6)(7,8,9)$ and let g_1 be these cycles. Now we let $h_1 = (3,2,6,5,9,8)$ now $g_1h_1 = (1,6,4,9,7,3)$ which is of length 6 as required.

   (b) Now g must contain exactly 2 3-cycles as it has an even size support, assume the second is $(4,5,6)$. First we deal with the case where g has only transpositions $(7,8)(9,10)$ say. Now we let $h_1 = (3,2,6,5,8,7,9)$ giving $g_1h_1 = (1,6,4,8,9,10,3)$ which has length 7 as required. Now if g contains only one even length cycle which is not a transposition, then we may assume $g_1 = (1,2,3)(4,5)(6,7,\ldots,k+5)$ then we let

$$h_1 = (2,1,4,6,7,\ldots,k+1,k+4,k+3,k+2)$$

   giving

$$g_1h_1 = (2,3,4,5,6,8,\ldots,k,k+4,k+5,7,9,\ldots,k+1).$$

Thus g_1h_1 has length $k+2$ as required.

4. We may assume that the non transpositions are

$$(1,2,\ldots,k_1)(k_1+1,k_1+2,\ldots,k_1+k_2)$$

we let this be g_1. Now we choose

$$\begin{aligned} h_1 \;=\; & (1,2,\ldots,k_1-4,k_1-2,k_1-3,k_1+1,\\ & k_1+2,\ldots,k_1+k_2-4,k_1+k_2-1,k_1+k_2-2,k_1+k_2-3) \end{aligned}$$

which gives

$$\begin{aligned} g_1h_1 \;=\; & (1,3,\ldots,k_1-5,k_1-2,k_1-1,k_1,2,4,\ldots,k_1-4,\\ & k_1+1,k_1+3,\ldots,k_1+k_2-5,k_1+k_2-1,k_1+k_2,\\ & k_1+2,k_1+4,\ldots,k_1+k_2-4) \end{aligned}$$

Thus g_1h_1 has length k_1+k_2-3 as required. It is not clear this construction works when the cycles are 4-cycles but it does, the required $h_1=(2,1,7,6,5)$.

We now deal with the case where g_1 has a single transposition. Now $k \geq 8$ as $n \geq 10$. Let

$$g_1=(1,2,\ldots,k)(k+1,k+2)$$

now let

$$h_1=(1,2,\ldots,k-6,k-1,k-2,k-3,k+1,k+2)$$

which has length $k-1$ as required. Now

$$g_1h_1 = (1,3,5,\ldots,k-7,k-1,k,2,4\ldots,k-6,k-5,k-4,k+1)$$

Thus g_1h_1 has length $k-1$ as required.

5. We may assume that the non-transposition is $(1,2,\ldots,k)$. Let

$$g_1 = (1,2,\ldots,k)(k+1,k+2)(k+3,k+4)(k+5,k+6)$$

now let

$$h_1 = (1,2,\ldots,k-4,k-1,k-2,k-3,k+1,k+4,k+3,k+5).$$

This gives

$$g_1h_1 = (1,3,\ldots,k-5,k-1,k,2,4,\ldots,k-4,k+1,k+2,k+4,k+5,k+6)$$

Thus g_1h_1 has length $k+3$ as required. Again it is not clear this construction work where $k=4$ so we give the special case, the required $h_1 = (3,2,1,4,7,6,9)$.

6. We may assume that the transpositions are $(1,2)(3,4)\ldots(11,12)$ and let g_1 be these transpositions. Now we choose $h_1 = (2,1,3,6,5,7,10,9,11)$ which gives $g_1h_1 = (2,3,4,6,7,8,10,11,12)$ which has length 9 as required.

We note that case 6 can only occur when n is divisible by 4 so we need not worry about this case when $n = 10$.

□

6.6.3 $n - i$ cycles

We see from the proofs of Theorems 6.16 and 6.17 that in each case we need only consider elements whose support is of size n. However, it is also clear that the number of special cases will increase as the length of the cycles used decreases. However, it is also clear that at each point we use similar constructions for example, where we have two transpositions, $(\alpha_1, \alpha_2)(\alpha_3, \alpha_4)$ then multiplying by the 3-cycle $(\alpha_1, \alpha_3, \alpha_2)$ will produce another 3-cycle. Now if we could build an arsenal of such constructions such that took a set of cycles with support size k and produced a single k-cycle such that the result was also a k-cycle, then if we partitioned the support of g, then we could use a standard construction on each partition and then repeatedly apply Lemma 6.15 to join all of these cycles together. We start by setting out a few preliminary results.

Lemma 6.18. *Let $c \in S_n$ be a cycle of even length then there do not exist cycles $c_1, c_2 \in S_n$ both of length k such that $cc_1 = c_2$*

Proof. We observe that c is an odd element. If k is even, then c_1 is an odd cycle and the product of two odd cycles is even so cannot be an even length cycle. Equally if k is of odd length, then cc_1 will be an odd cycle so c_2 will have even length. □

Lemma 6.18 tells us that we must always consider even length cycles in pairs so that we may use a single cycle length.

We now gather some of the constructions used so far.

Lemma 6.19. *Let $g = (\alpha_1, \alpha_2)(\alpha_3, \alpha_4)$ be transpositions then there exists h, a 3-cycle, such that gh is a 3-cycle whose support is a subset of $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$*

Proof. Let $h = (\alpha_1, \alpha_3, \alpha_2)$ □

Having dealt with transpositions we now turn our attention to other pairs of even length cycles. We give two constructions that we will use in tandem.

Lemma 6.20. *Let c be a cycle of length k, k even, then there exists a cycle c' of length k' such that cc' is a cycle of length $k'+1$ for all $\frac{k}{2} \leq k' \leq k-1$*

Proof. Assume $c = (1, 2, \ldots, k)$. Let

$$c' = (1, 2, \ldots, 2k' - k, k', k' - 1, \ldots, 2k' - k + 1)$$

c' is of length k' as required. Now

$$cc' = (1, 3, \ldots, 2k' - k - 1, k', k' + 1, \ldots, k, 2, 4, \ldots, 2k' - 2).$$

Thus cc' has $k'+1$ elements as required. □

We note that in the construction of Lemma 6.20 k' is in the support of c' and cc' so the cycles are amenable to the application of Lemma 6.15.

Lemma 6.21. *Let c be a cycle of length k, k even, then there exists a cycle c' of length k' such that cc' is a cycle of length $k'-1$ for all $\frac{k}{2}+1 \leq k' \leq k$*

Proof. Assume $c = (1, 2, \ldots, k)$. Let

$$c' = (1, 2, \ldots, 2k' - k - 2, k', k' - 1, \ldots, 2k' - k - 1)$$

c' is of length k' as required. Now

$$cc' = (1, 3, \ldots, 2k' - k - 3, k', k' + 1, \ldots, k, 2, 4, \ldots, 2k' - k - 2)$$

Thus cc' has $k'-1$ elements as required. □

As before we note that k' is in the support of c' and cc'.

As already noted with even cycles it is not possible to multiply by a given length cycle and obtain a cycle of the same given length. However, the last two lemmas have shown a way of multiplying by a cycle of a given length and obtaining a cycle either one shorter or one longer than the given length. As even cycles always come in pairs in A_n we may take a pair of even cycles and apply Lemma 6.20 to one and Lemma 6.21 to the other. We then note that the supports of c' and cc' have non-trivial intersection in all cases so we may then apply Lemma 6.15 to join our cycles. We formalise this via the following result.

Lemma 6.22. *Let c_1, c_2 be disjoint cycles of even lengths , $k_1, k_2 > 2$ respectively, then there exists a cycle c' of length k' such that c_1c_2c' is a cycle of length k' for $\frac{k_1+k_2}{2} + 1 \leq k' \leq k_1 + k_2$*

Proof. For the case where $k' < k_1 + k_2$ we use Lemmas 6.20 and 6.21 and observe that we may apply one construction to c_1 and the other to c_2. We may then apply Lemma 6.15 in order to form the required cycles. Where $k' = k_1 + k_2$ we observe that if $c_1 = (1, 2, \ldots, k_1)$ and $c_2 = (k_1 + 1, k_1 + 2, \ldots, k_1 + k_2)$ then $c' = (1, 2, \ldots, k_1 - 1, k_1 + 1, k_1 + 2, \ldots, k_1, k_2)$ will suffice. □

Before moving on to cycles of odd length we need to address the case where there is an even cycle of length greater than 2 and a transposition. We note that if in Lemma 6.22 we apply Lemma 6.21 to the longer cycle and use a single element of the transposition as the cycle to join to, then we are done, the same limits apply.

We now turn our attention to cycles of odd length.

Lemma 6.23. *Let c be a cycle of length k, k odd, then there exists a cycle c' of length k' such that cc' is a cycle of length k' for $\frac{k+1}{2} \leq k' \leq k$*

Proof. Assume $c = (1, 2, \ldots, k)$ and let

$$c' = (1, 2, \ldots, 2k' - k - 1, k', k' - 1, \ldots, 2k' - k).$$

Now c' has length k' as required. We now calculate

$$cc' = (1, 3, \ldots, 2k' - k - 2, k', k' + 1), \ldots, k, 2, 4, \ldots, 2k' - k - 1)$$

which again has length k' as required. We note that the the supports of cc' and c have non-trivial intersection. □

We are now in a position to show constructions for arbitrary cycle lengths. However, while the combination of constructions used relies on the element being in A_n as we require even length cycles to come in pairs we are not assured that the single cycle is in A_n, as the constructions given allow us to generate cycles of even length which are not in A_n. If we further insist that the resulting cycle is of odd length then Lemmas 6.19, 6.22 and 6.23 together with Lemma 6.15 allow us to calculate an estimate of the shortest cycle that a given element, g, of A_n may be expressed as the product of two of. If we also observe that our constructions allow us to use any cycle between the shortest cycle for g and the size of its support, then we need now only observe that we can extend this cycle to any other odd length, k less than n, by joining it with any cycle length $k - |Supp(g)|$ whose support is drawn from the stabiliser of g. Therefore, in order to determine an estimate of the shortest cycle length, l, such that every element of A_n may be expressed as the product of two l-cycles we need only find the longest value of l required for any element of A_n as we can extend all shorter cycles to this length.

Of course, we could reason about each group in turn as in Theorems 6.16

and 6.17. However, we observe that we can reason about the shortest cycle based solely on the shape of the element. GAP allows calculation of the conjugacy classes of a group and will return the cycle shape of a representative it is then trivial to determine the shortest cycle length. Table 6.3 shows our estimate of the minimum value of l such that every element of A_n may be expressed as the product of two l-cycles for various n.

We observe that for those groups tested we may express our estimate of the shortest cycle length such that every element of A_n can be expressed as a product of two l-cycles via the following formulae:

$$l = \begin{cases} \lfloor \frac{3n}{4} \rfloor & \text{if } \lfloor \frac{3n}{4} \rfloor \text{ odd} \\ \lfloor \frac{3n}{4} \rfloor + 1 & \text{otherwise} \end{cases} \tag{6.1}$$

We define $\lfloor i \rfloor$ in Equation 6.1 to be the largest integer smaller than i. We observe that the limit on l undergoes a step change roughly every three elements and this relates to the maximum number of transpositions that can occur in an element of A_n. We now seek to formalise these observations and show that, based on the constructions outlined above, the observed limits apply.

Theorem 6.24. *For all $g \in A_n$ there exist x, y both l-cycles in A_n such that $g = xy$ for all odd l greater than or equal to l_{min} where:*

$$l_{min} = \begin{cases} \frac{3n}{4} & n \textit{ divisible by } 4 \\ \frac{1}{4}(3n-3) & n-1 \textit{ divisible by } 4 \\ \frac{1}{4}(3n-2) & n-2 \textit{ divisible by } 4 \\ \frac{1}{4}(3n-1) & n-3 \textit{ divisible by } 4 \end{cases}$$

Proof. As previously we note that we need not consider every element of A_n simply that we need show that we can generate one element of each shape(conjugacy

Table 6.3: Estimate of minimum l such that every element of A_n is two l-cycles

n	l	n	l
5	3	33	25
6	5	34	25
7	5	35	27
8	7	36	27
9	7	37	27
10	7	38	29
11	9	39	29
12	9	40	31
13	9	41	31
14	11	42	31
15	11	43	33
16	13	44	33
17	13	45	33
18	13	46	35
19	15	47	35
20	15	48	37
21	15	49	37
22	17	50	37
23	17	51	39
24	19	52	39
25	19	53	39
26	19	54	41
27	21	55	41
28	21	56	43
29	21	57	43
30	23	58	43
31	23	59	45
32	25	60	45

class in S_n), we may then use conjugation in S_n to generate each element of that shape. We also observe that if there exists h_1, an l-cycle, such that $gh_1 = h_2$, where h_2 is also an l-cycle, then h_2 and h_1^{-1} are the required l-cycles.

We note that Lemmas 6.19, 6.22 and 6.23 together with Lemma 6.15 give us a working construction of l-cycles. We now need to establish a lower limit on l and

observe that for l greater than this limit we can create longer l by statbilising less elements in the support of g or by moving some elements outside of the support of g.

First we observe that for a cycle, c, of length $l_1 > 2$ the shortest equal length cycles that we can express c as a product of two of are roughly length $\frac{l_1}{2}$. We next observe that for n divisible by 4 A_n contains elements consisting solely of $\frac{n}{2}$ transpositions and our construction only allows us to convert 2 transpositions into a 3-cycle therefore in this case our constructions require two cycles of length $\frac{3n}{4}$. Therefore, in general, the more transpositions an element contains the larger l it will require.

We now move to the general case. Let k_o be the number of odd length cycles in g and n_o the total size of their support, k_e be the number of even length cycles of length greater than 2 and n_e be the total size of their support and finally we let k_t be the number of transpositions.

First we consider the shortest cycle that can be formed from the cycles of odd length. Now each cycle can be expressed as the product of two cycles of length equal to half the size of its support plus one. Therefore we can express all of the odd cycles as the product of two cycles of length $\frac{n_o}{2} + \frac{k_o}{2} = \frac{n_o+k_o}{2}$. We note that as odd length cycles are of length at least 3 then $k_o \leq \frac{n_o}{3}$ and we deduce that $\frac{n_o+k_o}{2} \leq \frac{n_o+\frac{n_o}{3}}{2} = \frac{2n_o}{3} < \frac{3n_o}{4}$ as previously observed.

We now turn to the even length cycles. There are two cases depending on if g contains an even number of transpositions.

1. *g contains an even number of transpositions.* The transpositions can be expressed as the product of two cycles of length $\frac{3k_t}{4}$. Now each pair of even length cycles of length greater than 2 can be expressed as as the product

of two cycles of length equal to half the size of their support plus one. Therefore we can express all of the even cycles as the product of two cycles of length $\frac{n_e}{2} + \frac{k_e}{2}$. The even length cycles are of length at least 4 so $k_e \leq \frac{n_e}{4}$ and we deduce that $\frac{n_e+k_e}{2} \leq \frac{n_e+\frac{n_e}{4}}{2} = \frac{5n_e}{8} < \frac{3n_e}{4}$ as previously noted.

2. *g contains an odd number of transpositions.* We need to include one of the transpositions in with the longer even length cycles. Now the transpositions can be expressed as the product of two cycles of length $\frac{3(k_t-1)}{4}$ and the longer even length cycles can be expressed as the product of two cycles of length $\frac{(n_e+2)+(k_e+1)}{2}$. Again the even length cycles are of length at least 4 so $\frac{(n_e+2)+(k_e+1)}{2} \leq \frac{(n_e+\frac{n_e}{4}+3}{2} = \frac{5n_e+12}{8} < \frac{3(n_e+2)}{4}$ for $n_e > 4$ as observed earlier.

We are now in a position to write down an equation for the shortest l such that g can be written as a product of two l-cycles.

$$l = \begin{cases} \frac{n_o+k_o}{2} + \frac{n_e+k_e}{2} + \frac{3k_t}{4} & g \text{ has an even number of transpositions} \\ \frac{n_o+k_o}{2} + \frac{n_e+k_e+3}{2} + \frac{3(k_t-1)}{4} & \text{otherwise} \end{cases}$$

We deal with each limit in turn and attempt to find the shortest two cycles in S_n such that g can be expressed as a product of two cycles of the given length.

Observe that, if g contains 2 even length cycles of length l_1, l_2 say, then they will require a cycle of length $\frac{l_1+l_2}{2}+1$. However, A_n must also contain an element where the support of these cycles is moved by transpositions alone and this would require a cycle of length $\frac{3(l_1+l_2)}{4} > \frac{l_1+l_2}{2} + 1$ provided $l_1 + l_2 > 4$ which is always true given our constraints on l_1 and l_2. Therefore we need not consider elements where there is more than one long even length cycle. Equally, if the long even cycle is of length $l_1 > 4$ then there will be an element of A_n which moves all bar 4 elements in transpositions and this will require a longer cycle.

Therefore our equations become:

$$l = \begin{cases} \frac{n_o+k_o}{2} + \frac{3k_t}{4} & g \text{ has an even number of transpositions} \\ \frac{n_o+k_o}{2} + 6 + \frac{3(k_t-1)}{4} & \text{otherwise} \end{cases}$$

We have now minimised the number of cases including even length cycles that we need to consider. We now turn our attention to the odd length cycles, examining the term for odd length cycles it is clear that for a given n_o l will be larger the more odd length cycles there are. We consider various values of n_o, we restrict our attention to small n_o, as if n_o is large, then there will be an element in A_n where the support of odd cycles is of size $n_o - 4$ that will require a larger l as the four other elements are move by two transpositions.

Table 6.4: Cycle lengths required for various sizes of odd cycle support

n_o	Shapes	$max(\frac{1}{2}(n_o + l_o))$
3	[3]	2
4	NA	NA
5	[5]	3
6	[3,3]	4
7	[7]	4
8	[5,3]	5
9	[9],[3,3,3]	6
10	NA	NA

In Table 6.4 we use the notation $[x, x, y]$ to mean the multi-set consisting of two lots of x and a single y. We note that if g contains a 7-cycle, then there will be an element in A_n that is identical to g on the stabiliser of the 7-cycle and contains two 3-cycles acting on the support of the 7-cycle and will require the same l so we may ignore elements containing 7-cycles. Equally we may ignore the case where 8 points are moved by odd cycles as A_n will contain an element where

the support of the odd cycles is moved by 4 transpositions which will require a larger l. We now have a very limited number of cases to consider. We first demonstrate that our limits are necessary.

1. n divisible by 4, A_n contains an element consisting solely of transpositions with $l = \frac{3n}{4}$

2. $n-1$ divisible by 4, A_n contains an element consisting solely of transpositions and a single fixed point which requires $l = \frac{3n-3}{4}$

3. $n-2$ divisible by 4, A_n contains an element consisting of two three cycles with the remaing points all moved by transpositions which requires $l = 4 + \frac{3(n-6)}{4} = \frac{3n-2}{4}$

4. $n-3$ divisible by 4, A_n contains an element consisting of a 3-cycle with the remaing points all moved by transpositions which requires $l = 2 + \frac{3(n-3)}{4} = \frac{3n-1}{4}$

Having shown the limits are necessary we now attempt to prove that they are sufficient. Table 6.5 gives all possible combinations of maximal shapes together with their value when $n - i$ is divisible by 4. In each case we consider where there are k pairs of transpositions and the remainder of the support is made up of the multi-set as shown, so for example $k * [2,2] + [2,4]$ would be an element consisting of k pairs of transpositions plus a transposition and a 4-cycle.

We can see that in no cases are our stated limits are exceeded and we are done. □

Of course we have not proved that the limits given in Theorem 6.24 are the best that can be done merely that they are the best that can be achieved using

Table 6.5: Required cycle lengths for maximal shapes

Shape	l	$n-1$	$n-2$	$n-3$
k*[2,2]	$3k$	$\frac{1}{4}(3n-3)$	$\frac{1}{4}(3n-6)$	$\frac{1}{4}(3n-9)$
k*[2,2] + [2,4]	$3k+4$	$\frac{1}{4}(3n-11)$	$\frac{1}{4}(3n-2)$	$\frac{1}{4}(3n-5)$
k*[2,2] + [3]	$3k+2$	$\frac{1}{4}(3n-7)$	$\frac{1}{4}(3n-10)$	$\frac{1}{4}(3n-1)$
k*[2,2] + [3,3]	$3k+4$	$\frac{1}{4}(3n-11)$	$\frac{1}{4}(3n-2)$	$\frac{1}{4}(3n-5)$
k*[2,2] + [5]	$3k+3$	$\frac{1}{4}(3n-3)$	$\frac{1}{4}(3n-6)$	$\frac{1}{4}(3n-9)$
k*[2,2] + [3,3,3]	$3k+6$	$\frac{1}{4}(3n-3)$	$\frac{1}{4}(3n-6)$	$\frac{1}{4}(3n-9)$
k*[2,2] + [2,4,5]	$3k+7$	$\frac{1}{4}(3n-11)$	$\frac{1}{4}(3n-14)$	$\frac{1}{4}(3n-5)$
k*[2,2] + [2,4,3]	$3k+6$	$\frac{1}{4}(3n-3)$	$\frac{1}{4}(3n-6)$	$\frac{1}{4}(3n-9)$
Maximum		$\frac{1}{4}(3n-3)$	$\frac{1}{4}(3n-2)$	$\frac{1}{4}(3n-1)$

the constructions outlined so far. We also note that although we showed that the limit is required in some cases we note that the observed limit may not always be an odd number so the cycles may not be in A_n.

We note that in proving Theorem 6.24 we have relied heavily on the construction for pairs of transpositions. Indeed, if we are able to show that the construction for transpositions is minimal, then it is clear that Theorem 6.24 becomes the best we can do. A direct computation in GAP shows that it is not possible to express 4 transpositions as the product of two cycles of the same length less than 6 a similar calculation shows that it is equally not possible to express 6 transpositions as the product of two cycles of the same length less than 9. We now provide a proof for the limit on transpositions.

Lemma 6.25. *Let $g = (1,2)(3,4)\dots(n-1,n)$ for n divisible by 4 then the shortest cycle length l such that g can be expressed as the product of two l-cycles is $\frac{3n}{4}$.*

Proof. First we note that if g can be expressed as the product of two l-cycles, then there exists an l-cycle, c, such that gc is an l-cycle. We now proceed to show that c must have length at least $\frac{3n}{4}$. Observe that the support of c must contain

at least one element from the support of each transposition or gc would contain a transposition. Therefore c must have support of size at least $\frac{n}{2}$. Next we observe that to stabilise an element in the support of g then c must contain both elements in the support of transposition, furthermore they must be consecutive. Therefore for gc to be a single cycle and stabilise one element c must have length at least $\frac{n}{2}+1$ giving gc of length $n-1$. In general the shortest c such that i elements are stablised will have length $\frac{n}{2}+i$. Now we require c and gc to be cycles of the same length, this will only occur when $i=\frac{n}{4}$ as required. □

Lemma 6.25 tells us that the construction used in Lemma 6.19 is the best we can do. We can now deduce that the limits of Theorem 6.24 are the best we can do as it is clear that for the 3,4, and 5 cycles we cannot do any better. We now restate Theorem 6.24 in its final form.

Theorem 6.26. *For all $g \in A_n$ there exist x, y both l-cycles in A_n such that $g = xy$ if and only if l is odd and greater than or equal to l_{min} where:*

$$l_{min} = \begin{cases} \frac{3n}{4} & n \text{ divisible by } 4 \\ \frac{1}{4}(3n-3) & n-1 \text{ divisible by } 4 \\ \frac{1}{4}(3n-2) & n-2 \text{ divisible by } 4 \\ \frac{1}{4}(3n-1) & n-3 \text{ divisible by } 4 \end{cases}$$

6.7 Proof of conjecture 6.8 and related results

We now return to Conjecture 6.8. Direct computation shows that while the Conjecture is true it does not need to be as general, indeed a fixed power of g will suffice.

Theorem 6.27. *Let $n > 3$ be odd and let $g = (1, 2, \ldots, n)$ and let c be a standard shape representative in A_n then cg^{-2} is an n-cycle.*

Proof. We begin by settling on some notation. We remind ourselves that c is a standard shape representative so the support is in ascending order. Now let $c = c_1 c_2 \ldots c_k$ where the c_i are disjoint cycles and let the last point of cycle c_i be s_i thus $c_1 = (1, 2, \ldots, s_1)$, $c_2 = (s_1 + 1, s_1 + 2, \ldots, s_2)$ and cycle c_i is of length $s_i - s_{i-1}$.

Observe that cg^{-1} will have a given shape namely it will be a single cycle $(n, n-1, \ldots, s_k + 1, s_k, s_{k-1}, \ldots, s_1)$.

Now we consider the image of any point, m, under cg^{-2}. Now if m is in the stabiliser of cg^{-1} (that is it is not either one of the s_i or in the stabiliser of c), then the image of m is simply $m - 1$ except where $m = 1$ in which case it is n. We note that in the case of $s_i + 1$ this will be s_i, that is the largest point in the support of the previous cycle of c. Equally, the image of any point stabilised by c is $m - 2$. This leaves us only to consider the image of each of the s_i, this will be $s_{i-1} - 1$ except where $i = 1$ when it will be $n - 1$.

Having dealt with the general construction there are four cases that we consider:

1. The number of fixed points is even and the number of cycles is even.

2. The number of fixed points is even and the number of cycles is odd.

3. The number of fixed points is odd and the number of cycles is even.

4. The number of fixed points is odd and the number of cycles is odd.

In each case we consider the image of n.

1. If the number of cycles is even, then there must be either no odd length cycles or an even number of them so the support of c is of even size. As n is odd and the size of the support is even the number of fixed points cannot be even so this case does not occur.

2. The construction is illustrated in Figure 6-2.

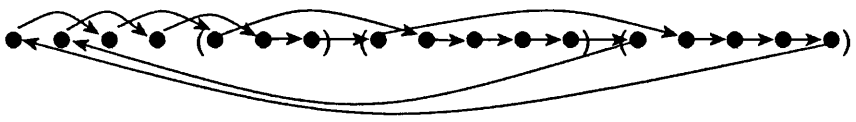

Figure 6-2: cg^{-2} with an even number of fixed points and odd number of cycles

We now generalise this, the image of n steps through the fixed points two at a time until we get s_k when the image is $s_{k-1}-1$. The image then descends through the support of c_{k-1} until it reaches s_{k-2} when it goes to $s_{k-3}-1$ and so on until s_1 is reached the image will then be $n-1$ and we will then step through the remaining fixed points of c in steps of two until we reach s_k-1 we then descend through the support of c_k until we reach s_{k-1}. The image is then $s_{k-2}-1$ and we continue in this way until the first cycle is reached which we then descend and the image returns to n. We have now covered all n points in a single cycle as required.

3. As before the construction is illustrated in Figure 6-3.

We now generalise this, the image of n steps through the fixed points two at a time until we reach s_k-1 we then descend through the support of c_k until we reach s_{k-1} whose image is $s_{k-2}-1$ and we continue in this way until we reach s_1 whose image is $n-1$. We now step through the remaining fixed points of c in steps of two which takes us to s_k whose image is $s_{k-1}-1$ we

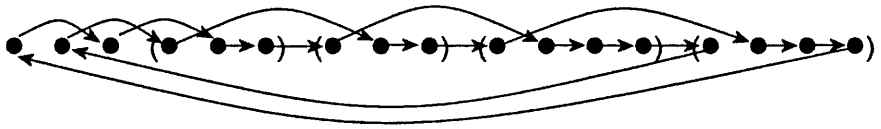

Figure 6-3: cg^{-2} with an odd number of fixed points and an even number of cycles

then descend through the support of c_{k-1} until we reach s_{k-2}. We continue in this fashion until we reach $s_1 - 1$ and we then descend through the support of c_1 until the image returns to n. We have now covered all n points in a single cycle as required.

4. If there are an odd number of cycles, then c has an odd number of odd length cycles as even length cycles come in pairs in A_n. Now if c has an odd number of odd length cycles, then c has an odd size support. As n is odd and the size of the support is odd the number of fixed points cannot also be odd so this case does not occur.

□

We note that in proving Theorem 6.27 we did not have recourse to the fact that the cycles were listed with descending length only that each cycle of c was of the form $(a, a+1, a+2, \ldots, a+i)$.

Having observed the special properties that g^{-2} exhibits in A_n we return to the original hypothesis of Conjecture 6.8 which considered the group $\langle g \rangle$. Table 6.6 gives the number of elements in $\langle (1, 2, \ldots, 9) \rangle$ such that pre-multiplying by a standard shape representative in A_9 gives rise to a 9-cycle.

We note that for two cycle shapes g^{-2} is the only element of $\langle g \rangle$ that gives rise to a 9-cycle. While not all groups have such shape representatives A_9 certainly is

Table 6.6: Number of elements of $\langle(1,2,\ldots,9)\rangle$ that generate a 9-cycle

Shape	Number of 9 cycles
(1,2)(3,4)	2
(1,2)(3,4)(5,6)(7,8)	4
(1,2,3)	3
(1,2,3)(4,5)(6,7)	1
(1,2,3)(4,5,6)	3
(1,2,3)(4,5,6)(7,8,9)	3
(1,2,3,4)(5,6)	3
(1,2,3,4)(5,6,7)(8,9)	2
(1,2,3,4)(5,6,7,8)	4
(1,2,3,4,5)	4
(1,2,3,4,5)(6,7)(8,9)	3
(1,2,3,4,5)(6,7,8)	2
(1,2,3,4,5)(6,7,8)	2
(1,2,3,4,5,6)(7,8)	1
(1,2,3,4,5,6,7)	4

not unique in having shape representatives where only g^{-2} will suffice. Table 6.7 shows the smallest number of elements of $\langle(1,2,\ldots,n)\rangle$ that will generate an n-cycle for a standard shape representative in A_n.

We now turn our attention to S_n, again for n odd. We observe that this will not give rise to an n-cycle as where c is a odd element of S_n cg^{-2} will also be an odd element. For motivation we consider all of the conjugacy classes composed of odd elements of S_7, the results are shown in Table 6.8.

We can see that in general there is not one shape that arises from multiplication by g^{-2}. Equally, the cycle shapes are clearly not arbitrary as they consist of no more than two cycles with support of size at least 6.

Theorem 6.28. *Let $n > 3$ be odd and let $g = (1,2,\ldots,n)$ and let c be a standard shape representative in S_n then cg^{-2} is one of the following:*

Table 6.7: Minimumm number of elements generating an n-cycle

n	Minimum number of elements
5	2
7	2
9	1
11	3
13	2
15	1
17	2
19	2
21	1
23	2
25	1

Table 6.8: Odd shape representatives in S_7 multiplied by $(1,2,3,4,5,6,7)^{-2}$

Shape	Result
$(1,2)$	$(1,7,5,3)(2,6,4)$
$(1,2)(3,4)(5,6)$	$(1,7,5,4)(2,6,3)$
$(1,2,3)(4,5)$	$(1,7,5,2)(3,6,4)$
$(1,2,3,4)$	$(1,7,5,3,2)(4,6)$
$(1,2,3,4)(5,6,7)$	$(1,7,3,2)(4,6,5)$
$(1,2,3,4,5)(6,7)$	$(1,7,4,3,2)(5,6)$
$(1,2,3,4,5,6)$	$(1,7,5,4,3,2)$

1. *An n-cycle*

2. *An $n-1$-cycle*

3. *Two disjoint cycles whose combined support is of size n*

Proof. We use the same notation as in Theorem 6.27 and observe that for even elements we can apply Theorem 6.27 directly giving cg^{-2} as a single cycle of length n. This leaves us only to consider odd elements of S_n.

Observe that, irrespective of whether c is even or odd, cg^{-1} will have the same general structure namely it will be the single cycle

$$(n, n-1, \ldots, s_k+1, s_k, s_{k-1}, \ldots, s_1).$$

We consider the same possibilities as in Theorem 6.27 in turn:

1. The number of fixed points is even and the number of cycles is even. In this case we consider the orbits of n and $n-1$. The construction is illustrated using Figure 6-4 where the orbit of n is shown by solid lines and $n-1$ by dotted lines.

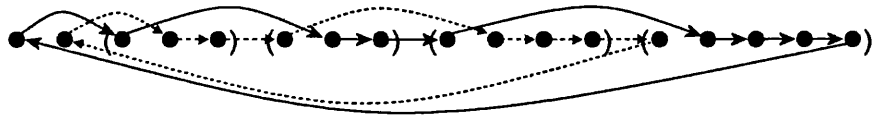

Figure 6-4: cg^{-2} with an even number of fixed points and an even number of cycles

We start with the image of n this will step through the fixed points two at a time until it reaches s_k whose image is $s_{k-1}-1$. The image then descends through the support of c_{k-1} until it reaches s_{k-2} when it goes to $s_{k-3}-1$ and so on until s_1-1 and the image will descend through c_1 until 1 is reached and the image will then be n, this is the end of our first cycle. We now consider the image of $n-1$ this will step through the remaining fixed points of c in steps of two until it reaches s_k-1 when the image descends through the support of c_k until we reach s_{k-1}. The image is then $s_{k-2}-1$ and we continue in this way until the s_2-1 is reached and the image then descends c_2 to s_1 and then returns to $n-1$ .Thus we have now covered all

n points in two cycles as required.

2. The number of fixed points is even and the number of cycles is odd. For any element to be odd it requires an odd number of even length cycles but this would mean there were an even number of odd length cycles given even size support which contradicts the assertion that the number of fixed points is even hence all such elements will be in A_n.

3. The number of fixed points is odd and the number of cycles is even. For any element to be odd it requires an odd number of even length cycles but as there are an even number of cycles this would mean there were an odd number of odd length cycles and hence the support is of odd size and therefore the number of fixed points is even which contradicts the assertion that the number of fixed points is odd hence all such elements will be in A_n.

4. The number of fixed points is odd and the number of cycles is odd. First we consider the special case where there is a single fixed point and a single cycle. In this case $cg^{-2} = (1, n, n-2, n-3, \ldots, 2)$. We now turn to the general case and again we consider the orbits of n and $n-1$. The construction is illustrated using figure 6-5 where the orbit of n is shown by solid lines and $n-1$ by dotted lines.

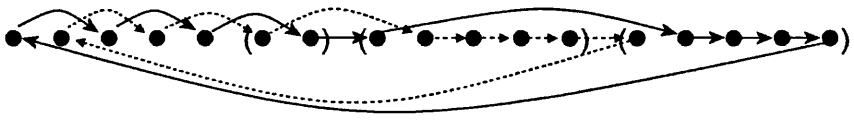

Figure 6-5: cg^{-2} with an odd number of fixed points and an odd number of cycles

We consider the orbit of n first, it will step through the fixed points two

at a time until it reaches $s_k - 1$ it will then descend through the support of c_k until it reaches s_{k-1} where the image is $s_{k-2} - 1$ and will continue in this way until we reach $s_1 - 1$ when it will then descend c_1 until it reaches 1 whose image is n, this is the end of our first cycle. We now consider the image of $n - 1$ which steps through the remaining fixed points of c in steps of two which takes us to s_k whose image is $s_{k-1} - 1$ it will then descend through the support of c_{k-1} until it reaches s_{k-2}. It will continue in this fashion until it reaches $s_2 - 1$ and will then descend through the support of c_2 until we reach s_1 and the image returns to $n - 1$. We have now covered all n points in two cycles as required.

□

We can see from the proof of Theorem 6.28 that it is possible us to read off the length of each of the cycles although this will depend on the parity of the number of fixed points. We have already established that where c is an even element we will have a single cycle of length n. We now turn our attention to when c is an odd element. If the number of fixed points is even, then one cycle will be of length $\frac{n-s_k}{2} + \sum_{i=1}^{k} Length(c_i)$ for i odd with the other being of length $\frac{n-s_k}{2} + \sum_{i=1}^{k} Length(c_i)$ for i even. The situation is similar where the number of fixed points is odd in this case one cycle will be of length $\frac{n-s_k-1}{2} + \sum_{i=1}^{k} Length(c_i)$ for i odd with the other being of length $\frac{n-s_k+1}{2} + \sum_{i=1}^{k} Length(c_i)$ for i even. We note that the only time that we get a single cycle is where c is an $n-1$ cycle and in this case the support of cg^{-2} is of size $n-1$, indeed this is the only case where the support is not of size n.

Chapter 7

Generating A_n from standard shape representatives

Having shown in Chapter 6 that any element can be expressed as a product of two p cycles it is natural to ask the question *if c is a standard shape representative and g is the cycle $(1, 2, \ldots, n)$, what can we deduce about $\langle c, g \rangle$?* We begin by looking at the case where n is prime. For relatively small primes it is possible to calculate $\langle c, g \rangle$ using GAP. This direct computation yields that the only c for which $\langle c, g \rangle \neq A_p$ are $c = id$ and $c = g$. For all but these trivial cases $\langle c, g \rangle = A_p$ for every p in the range $5 \leq p \leq 53$. The same is not true where n is not prime. In this case there are other standard shape representatives where $\langle c, g \rangle \neq A_n$, Table 7.1 gives the total number of shapes and the number which do not generate the whole of A_n for all odd $n \leq 53$.

7.1 Shapes that do not generate A_n

We begin by proving a basic result

Table 7.1: Number of standard shapes,c for whom $\langle c, g\rangle \neq A_n$

n	Total Shapes	Non-generating Shapes
5	4	2
7	8	2
9	16	3
11	29	2
13	52	2
15	90	6
17	151	2
19	248	2
21	400	10
23	632	2
25	985	5
27	1,512	17
29	2,291	2
31	3,431	2
33	5,084	31
35	7,456	12
37	10,836	2
39	15,613	54
41	22,316	2
43	31,659	2
45	44,601	105
47	62,416	2
49	86,809	9
51	120,025	153
53	165,028	2

Lemma 7.1. *Let $g = (1, 2, \ldots, n)$, n odd, and let c be a standard shape representative in A_n. Then $\langle c, g\rangle = \langle g\rangle$ if and only if $c = g$ or $c = id$*

Proof. For $\langle c, g\rangle = \langle g\rangle$ we need $c = g^i$ for some $1 \leq i \leq n$. Clearly this is true for the identity now for c not the identity $(1)c = 2$ as it is a standard shape representative and $(1)g^i = 2$ only when $i = 1$ so $c = g$ and these are the only cases. □

Lemma 7.1 tells us that there are always at least two c such that $\langle c, g\rangle < A_n$ it does not give us any information about how many other standard shape representatives generate groups smaller than A_n, or indeed anything about the size of the group generated.

For motivation we consider the following standard shape representative in A_9 let $c = (1,2,3)(4,5,6)(7,8,9)$. We note that $\langle c, g\rangle$ is a group with 81 elements so is not A_9. To understand this we consider the following block structure $\{1,4,7\},\{2,5,8\},\{3,6,9\}$. Now any power of g permutes these blocks. Equally, powers of c permute these blocks and we see that $\langle g, c\rangle$ has a non-trivial block structure and hence is imprimitive and so is is not A_9. Clearly we can extend this construction to yield an imprimitive permutation group whenever n is composite.

Lemma 7.2. *Let $g = (1,2,\ldots,n)$, n odd, and let*

$$c = (1,2,\ldots,r)(r+1,r+2,\ldots,2r)\ldots(n-r+1,n-r+2,\ldots,n)$$

where $n = mr$. Then $\langle g, c\rangle < A_n$

Proof. We begin by partitioning $\{1,2,\ldots,n\}$ into equivalence classes modulo r and consider the action of $\langle g, c\rangle$ on these partitions. Any power of g permutes these partitions so preserves the block structure. Equally, any power of c permutes these partitions and so preserves the block structure. Therefore $\langle g, c\rangle$ is not primitive. A_n is primitive so we deduce that $\langle g, c\rangle \neq A_n$ □

Lemma 7.2 tells us that there are more than two standard shape representatives for which $\langle g, c\rangle < A_n$. We note that for $n = 15$ we have so far accounted for 4 standard shape representatives namely the identity, g, and the elements consisting solely of the 3 and 5 cycles. However, Table 7.1 asserts that there are

6 such shapes, the remaining two shapes are:

$$(1,2,3,4,5,6)(7,8,9,10,11,12)(13,14,15) \text{ and}$$

$$(1,2,3,4,5,6,7,8,9)(10,11,12)(13,14,15).$$

Now we consider the same partitions of $\{1,2,\ldots,15\}$ modulo 3 and we note that our block structure is still preserved by each of these elements and we obtain the following corollary.

Corollary 7.3. *Let $g = (1,2,\ldots,n)$, n odd, and let $c = c_1c_2\ldots c_k$ where $c_i = (s_{i-1}+1, s_{i-1}+2, \ldots, s_i)$, $s_k = n$ and $r|s_i - s_{i-1}$ or $c = id$ then $\langle g,c\rangle < A_n$.*

Proof. We partition $\{1,2,\ldots,n\}$ into equivalence classes modulo r and consider the action of powers of g and c respectively, both respect the partitions and hence $\langle g,c\rangle < A_n$ □

Of course we have not yet shown that these are the only standard shape representatives for which $\langle g,c\rangle < A_n$. However, a direct computation in GAP shows that this is the case for all $n \leq 51$. We now proceed to look at cases where greatest common divisor of the cycle lengths and n is 1. We note that where the size of the support of c is less than n then c contains at least one 1-cycle so the greatest common divisor of the cycle lengths is 1.

7.2 Shapes that generate A_n

We now turn our attention to standard shape representatives that generate A_n, we first deal with the case where c fixes at least one point.

7.2.1 Standard shapes with support size less than n

We begin with a straightforward case, where the standard shape representative consists of two transpositions. We then extend to other standard shape representatives by reducing them to this case. In the course of the discussion we look at some other special cases of elements that generate A_n.

Lemma 7.4. *Let* $g = (1, 2 \ldots, n)$, $n > 4$ *odd, and let* $c = (1,2)(3,4)$. *Then* $\langle g, c \rangle = A_n$

Proof. First we observe that every element in A_n can be written as the product of an even number of transpositions. Therefore we need only show that $\langle g, c \rangle$ contains arbitrary pairs of transpositions and we are done.

We start by showing that $\langle g, c \rangle$ contains all pairs of transpositions of the form $(x, x+1)(y, y+1)$. Now $c^{g^i} = (1,2)^{g^i}(3,4)^{g^i} = (i+1, i+2)(i+3, i+4)$ for $0 \leq i < n-1$ where addition is modulo n. This means if we choose $i = x - 1$, then $c^{g^{x-1}} = (x, x+1)(x+2, x+3)$ and we have the first transposition of our pair but not necessarily the second. However, we note that as i steps through all possible values the second transposition of c will step though all transpositions of the form $(a, a+1)$ and in particular $(y, y+1)$, we also note that if we multiply c^{g^i} by $c^{g^{i+2}}$, then the middle two transpositions cancel. In particular if we post-multiply $c^{g^{x-1}}$ by $c^{g^{x+1}}$, then the middle two transpositions will cancel and we will obtain a different final transposition. Moreover we may repeat this process, increasing the power of g by two, modulo n, each time until the required final transposition occurs.

Of course the above pair of transpositions is not arbitrary, we now address this. We use induction, let $t = (a, a+2)$, and we observe that t can be expressed as $(a, a+1)(a+1, a+2)(a, a+1)$ which uses transpositions of the given form.

We can extend this to an arbitrary $t = (a, a+i)$ by induction on i as

$$t = (a, a+i-1)(a+i-1, a+i)(a, a+i-1)$$

Similarly we can extend this to our required arbitrary pair of transpositions as we write each of the transpositions using this algorithm and then multiply them, the resulting expression will have an even number of transpositions, each pair of which is of the form $(a, a+1)(b, b+1)$ and we know we can generate any pair of this form and we are done. □

We next turn to some other simple cases and start with an obvious corollary of Lemma 7.4

Corollary 7.5. *Let $g = (1, 2 \ldots, n)$, $n > 4$ odd, and let $c = (a, a+1)(b, b+1)$ $a, b \in \{1, \ldots, n\}$ and $a \neq b$ where addition is modulo n. Then $G = \langle g, c \rangle = A_n$*

Proof. Without loss of generality we may assume that $a < b$ and $a = 1$ (as we may conjugate to make this happen).

First we deal with the case where $b = 2$, in this case we observe that

$$cc^g = (1,2)(2,3)(2,3)(3,4) = (1,2)(3,4)$$

We may now apply Lemma 7.4 and we are done.

We now turn to the case where $b > 2$. Let $c' = c^{g^{2-b}} = (3-b, 4-b)(2,3)$ and consider

$$cc' = (1,2)(b, b+1)(3-b, 4-b)(2,3)$$

Now we want the two middle transpositions to have disjoint support and support disjoint from $\{1, 2, 3\}$. If the two middle transpositions are not disjoint then one

of the following conditions is true:

1. $b = 3 - b \Rightarrow 2b = 3 \Rightarrow b = \frac{n+3}{2}$.

2. $b = 4 - b \Rightarrow 2b = 4$ so either $b = 2$ which we have already ruled out, or $b = \frac{n+4}{2}$ but this cannot happen as n is odd.

3. $b + 1 = 3 - b \Rightarrow 2b = 2$ but $b \neq 1$ the only other option is $b = \frac{n+2}{2}$ but this cannot happen as n is odd.

4. $b + 1 = 4 - b \Rightarrow 2b = 3$ and we are in case 1 again.

Now we ensure that the middle transpositions are disjoint from $\{1, 2, 3\}$.

1. $b = 1, 2$ we have already dealt with and if $b = 3$, then we can apply Lemma 7.4 directly.

2. $b + 1 = 2, 3$ we have already dealt with leaving only $b + 1 = 1$ this implies $b = n$ so $c = (n, 1)(1, 2)$ conjugation by g gives $c^g = (1, 2)(2, 3)$ and we have already dealt with this case.

3. $3 - b = 1, 2 \Rightarrow b = 2$ or 1 respectively both of which we have already dealt with. Now if $3 - b = 3$, then $b = n$ and we have just dealt with this case.

4. $4 - b = 2, 3 \Rightarrow b = 2$ or 1 respectively, and we have dealt with these cases. Now if $4 - b = 1$, then $b = 3$ and we may apply Lemma 7.4 directly.

Now provided that $b \neq \frac{n+3}{2}$, the two middle transpositions commute with $(2, 3)$ and are disjoint so $cc' = (1, 2)(2, 3)(b, b+1)(3-b, 4-b)$ and we may square this to get $(1, 2, 3)$ and square again to get $(1, 3, 2) = (1, 2)(2, 3) \in G$ and we have already shown that this implies $G = A_n$.

Now if $b = \frac{n+3}{2}$, then $c = (1,2)(\frac{n+3}{2}, \frac{n+3}{2}+1)$ and we can conjugate c by $g^{\frac{n+3}{2}-1}$ to get $(\frac{n+3}{2}, \frac{n+3}{2}+1)(n+2, n+3)$ and if we post-multiply c by this, then we get $(1,2)(2,3) \in G$ and we are done

□

So far we have required that the transpositions consist of adjacent elements, but we now show that we need not insist on this.

Lemma 7.6. *Let $g = (1,2,\ldots,n)$, $n > 6$ odd, and let $c = (1,2)(a, a+2)$ where $3 < a \leq n-3$. Then $\langle g, h \rangle = A_n$*

Proof. Let $c' = c^g = (2,3)(a+1, a+3)$ so $cc' = (1,2)(a, a+2)(2,3)(a+1, a+3)$ now if $3 < a \leq n-3$, then the transpositions including a are disjoint from $\{1,2,3\}$ and are clearly disjoint from each other so $cc' = (1,3,2)(a, a+2)(a+1, a+3)$ and $(cc')^4 = (1,3,2) = (1,2)(2,3)$ and we can apply Corollary 7.5. □

Now it is clear that we can extend Lemma 7.6 to cover the case where $c = (1,2)(a, a+i)$ provided that $a + i \leq n-1$ as the construction will still work.

Corollary 7.7. *Let $g = (1,2,\ldots,n)$, $n > 6$ odd, and let $c = (1,2)(a, a+i)$ where $a > 3$ and $a + i \leq n-1$. Then $\langle g, h \rangle = A_n$*

Equally, we need not restrict the first transposition. If $c = (b, b+1)(a, a+i)$, then we may conjugate by g^{-b} to revert to the original case and we get

$$c^{g^{1-b}} = (1,2)(a-b, a+i-b)$$

where addition is modulo n and this satisfies the conditions of Corollary 7.7 provided $a + 1 - b > 3$ and $a + i - b < n - 1$.

Having dealt with most pairs of transpositions we now consider longer cycles. The first standard shape representative we consider is the standard 3-cycle.

Lemma 7.8. *Let $g = (1, 2 \ldots, n)$, $n > 4$ odd, and let $c = (1, 2, 3)$. Then $\langle g, c \rangle = A_n$*

Proof. $c^{-1} = (1, 3, 2) = (1, 2)(2, 3)$ and we may apply Corollary 7.5 □

Clearly there is very little that is special about the 3-cycle $(1, 2, 3)$ and we next consider the 3-cycle $(1, 2, a)$ where $a > 3$.

Lemma 7.9. *Let $g = (1, 2 \ldots, n)$, $n > 3$ odd, and let $c = (1, 2, a)$, $a > 3$. Then $\langle g, c \rangle = A_n$*

Proof. First note that if $a = n$, then $c^g = (1, 2, 3)$ and we may apply Lemma 7.8. We now deal with the case where $3 < a < n$. Let $c' = c^g = (2, 3, a + 1)$ and we consider the commutator $[c^{-1}, c']$:

$$\begin{aligned} cc'^{-1}c^{-1}c' &= (1, 2, a)(2, a + 1, 3)(1, a, 2)(2, 3, a + 1) \\ &= (1, a + 1, 3, 2, a)(1, a, 2)(2, 3, a + 1) \\ &= (1, a + 1, 3)(2, 3, a + 1) \\ &= (1, 2, 3) \end{aligned}$$

We have shown that the group contains $(1, 2, 3)$ and we may now apply Lemma 7.8 and we are done. □

We now extend Lemma 7.8 to cover the case where c is any odd length cycle.

Lemma 7.10. *Let $g = (1, 2 \ldots, n)$, $n \geq 5$ odd, and let $c = (1, 2, \ldots, m)$, m odd and $3 \leq m < n$. Then $\langle g, c \rangle = A_n$*

Proof. If $m = 3$, then we may apply Lemma 7.8 directly. We note that $m \leq n - 2$ as we require m to be odd. Now for $m \geq 5$ we observe that $(c^g)^{-1}c = (1, 2, m + 1)$ and we have already shown in Lemma 7.9 the group will be A_n. □

So far we have restricted our attention to standard shape representatives which consist of at most two non-trivial orbits. We now address the more general case where the standard shape representative is any whose support is smaller than n.

Lemma 7.11. *Let $g = (1, 2, \ldots, n)$, n odd, and let c be a standard shape representative with support size less than n. Then $\langle g, c \rangle = A_n$*

Proof. First we remind ourselves of the definition of a standard shape representative and let $c = c_1 c_2 \ldots c_k$ where the c_i are disjoint cycles such that $c_i = (s_{i-1} + 1, s_{i-1} + 2, \ldots, s_i)$ and $Length(c_{i+1}) \leq Length(c_i)$

Now if c consists solely of transpositions and 1-cycles and $s_k \leq n - 3$, then

$$c\left(c^{g^2}\right)^{-1} = (1, 2)(s_k + 1, s_k + 2)$$

We may apply Corollary 7.5 and we are done. If $s_k = n - 1$, then $c\left(c^{g^2}\right)^{-1} = (1, 2, n)$ and conjugation by g yields $(1, 2, 3)$ and we may apply Lemma 7.8 and we are done.

We now turn to the case where c does not consist solely of transpositions and 1-cycles.

We consider the case where c has no transpositions first. Let

$$c' = c(c^g)^{-1} = (1, s_1 + 1, s_2 + 1, \ldots, s_k + 1, s_k, s_{k-1}, \ldots, s_1)$$

and let

$$c'' = (c^g)^{-1} c = (2, s_1 + 2, s_2 + 2, \ldots, s_{k-1} + 2, s_k + 1, s_{k-1} + 1, s_{k-2} + 1, \ldots, 1)$$

We now consider the commutator $[c', c'']$ in two parts firstly:

$$\begin{aligned} c'^{-1}c''^{-1} &= (s_1, s_2, \ldots, s_k, s_k+1, s_{k-1}+1, \ldots, s_1+1, 1) \\ &\quad (1, s_1+1, \ldots, s_k+1, s_{k-1}+2, s_{k-2}+2, \ldots, 2) \\ &= (s_1, s_2, \ldots, s_k, s_{k-1}+2, s_{k-2}+2, \ldots, 2, 1) \end{aligned}$$

Secondly :

$$\begin{aligned} c'c'' &= (1, s_1+1, s_2+1, \ldots, s_k+1, s_k, s_{k-1}, \ldots, s_1) \\ &\quad (2, s_1+2, s_2+2, \ldots, s_{k-1}+2, s_k+1, s_{k-1}+1, s_{k-2}+1, \ldots, 1) \\ &= (s_k+1, s_k, s_{k-1}, \ldots, s_1, 2, s_1+2, s_2+2, \ldots, s_{k-1}+2) \end{aligned}$$

Finally we can combine the above to get:

$$\begin{aligned} c'^{-1}c''^{-1}c'c'' &= (s_1, s_2, \ldots, s_k, s_{k-1}+2, s_{k-2}+2, \ldots, 2, 1) \\ &\quad (s_k+1, s_k, s_{k-1}, \ldots, s_1, 2, s_1+2, s_2+2, \ldots, s_{k-1}+2) \\ &= (1,2)(s_k+1, s_k) \end{aligned}$$

We may now apply Corollary 7.5 and we are done for this case.

This leaves only the case where c contains some transpositions, the construction in this case is almost identical to that given above. In a standard shape representative cycles are listed in descending length order so the transpositions occur at the end. Let $c_{k'}$ be the last cycle which is not a transposition. We define c' and c'' as before and we consider the same commutator. First we look

at $c'^{-1}c''^{-1}$:

$$\begin{aligned} c'^{-1}c''^{-1} &= (s_1, s_2, \ldots, s_k, s_k+1, s_{k-1}+1, \ldots, s_1+1, 1) \\ &\quad (1, s_1+1, \ldots, s_k+1, s_{k-1}+2, s_{k-2}+2, \ldots, 2) \\ &= (s_1, s_2, \ldots, s_{k'}, s_{k'-1}+2, s_{k'-2}+2, \ldots, 2, 1) \end{aligned}$$

Secondly :

$$\begin{aligned} c'c'' &= (1, s_1+1, s_2+1, \ldots, s_k+1, s_k, s_{k-1}, \ldots, s_1) \\ &\quad (2, s_1+2, s_2+2, \ldots, s_{k-1}+2, s_k+1, s_{k-1}+1, s_{k-2}+1, \ldots, 1) \\ &= (s_{k'}, s_{k'-1}, \ldots, s_1, 2, s_1+2, s_2+2, \ldots, s_{k'}+2) \end{aligned}$$

Finally we can combine the above to get:

$$\begin{aligned} c'^{-1}c''^{-1}c'c'' &= (s_1, s_2, \ldots, s_{k'}, s_{k'-1}+2, s_{k'-2}+2, \ldots, 2, 1) \\ &\quad (s_{k'}, s_{k'-1}, \ldots, s_1, 2, s_1+2, s_2+2, \ldots, s_{k'}+2) \\ &= (1,2)(s_{k'}, s_{k'}+2) \end{aligned}$$

If $3 < s_{k'} \leq n-3$, then we can apply Lemma 7.6 and we are done. If $s_{k'} = 3$, then c consists of a 3-cycle and transpositions so $c^2 = (1,3,2) = (1,2)(2,3)$ and we can apply Lemma 7.8. This leaves only the case where $s_{k'} = n-2$ but as we have insisted that c contains at least one transposition this would imply that c had support size n which we have already ruled out. □

We observe that in proving Lemma 7.11 we have insisted that transpositions are listed last this is not strictly required although the exposition is then less clear (essentially if transpositions occur in the middle, then they will simply

cancel out).

7.2.2 Shapes with support size n

Finally we turn our attention to the case where c is a standard shape representative with support of size n. We note that in proving Lemma 7.11 we have relied on the fact that $s_k + 1$ is not 1. In this case the situation is somewhat different. As before we let

$$c' = c(c^g)^{-1} = (1, s_1 + 1, \ldots, s_{k-1} + 1)(s_k, s_{k-1}, \ldots, s_1)$$

and let

$$c'' = (c^g)^{-1}c = (s_{k-1} + 1, s_{k-2} + 1, \ldots, 1)(2, s_1 + 2, \ldots, s_{k-1} + 2).$$

Now when we look at the commutator $[c', c'']$ we get the following:

$$\begin{aligned} c'^{-1}c''^{-1} &= (s_{k-1} + 1, s_{k-2} + 1, \ldots, 1)(s_1, s_2, \ldots, s_k) \\ &\quad (1, s_1 + 1, \ldots, s_{k-1} + 1)(s_{k-1} + 2, s_{k-2} + 2, \ldots, 2) \\ &= (s_1, s_2, \ldots, s_k)(s_{k-1} + 2, s_{k-2} + 2, \ldots, 2) \end{aligned}$$

and also

$$\begin{aligned} c'c'' &= (1, s_1 + 1, \ldots, s_{k-1} + 1)(s_k, s_{k-1}, \ldots, s_1) \\ &\quad (s_{k-1} + 1, s_{k-2} + 1, \ldots, 1)(2, s_1 + 2, \ldots, s_{k-1} + 2) \\ &= (s_k, s_{k-1}, \ldots, s_1)(2, s_1 + 2, \ldots, s_{k-1} + 2) \end{aligned}$$

It is clear that $[c', c'']$ is the identity and we cannot use the same construction as in Lemma 7.11. We recall that Corollary 7.3 gave conditions where $\langle c, g \rangle < A_n$ and direct calculation in GAP showed that for $n \leq 51$ only those representatives that met the conditions of Corollary 7.3 failed to generate A_n.

The following theorem is a restricted version of a theorem originally due to C. Jordan, the full theorem can be found in [9] as Theorem 5.6.2 and in [16] as Theorem 13.2.

Theorem 7.12. *Let G be a primitive permutation group on n letters and let H be a transitive subgroup of G on m letters fixing the remaining $n - m$ letters. If H is primitive, then G is $n - m + 1$ transitive.*

Now if we can show that $\langle c, g \rangle$ is primitive, then we could possibly apply Theorem 7.12 to show that the group is at least 4-transitive. Thanks to the classification of finite simple groups [4] all groups which are at least 4-transitive are known. They must be the Mathieu groups, $M_{11}, M_{12}, M_{23}, M_{24}$, the symmetric group or the alternating group. Looking back to Table 7.1 we have already empirically ruled out the Mathieu groups and we know the group is not the symmetric group as it is generated by two even permutations so if $\langle c, g \rangle$ is at least 4-transitive, then it must be A_n. First we show that $\langle c, g \rangle$ is primitive via the following theorem.

Theorem 7.13. *Let $g = (1, 2, \ldots, n)$, n odd, and let c be a standard shape representative in A_n, if the greatest common divisor of the cycle lengths of c is 1, then provided that c is not the identity $G = \langle g, c \rangle$ is primitive.*

Proof. Clearly G is a transitive group as it contains an n-cycle. Suppose that B is a block of G which contains 1. Suppose that $B, Bg, Bg^2, \ldots Bg^{r-1}$ are

distinct, but that $(1)g^r \in Bg^i$ for some $0 \leq i < r$. It follows that $(1)g^r \in B$ else $(1)g^{r-1} \in Bg^{i-1}$. Thus there are r blocks in the block system, each one consisting of the elements of Ω which are congruent modulo r. We may assume that $r < n$ else the block system is trivial.

The cycle structure of c begins $c = (1, 2, \ldots, s_1)(s_1 + 1, \ldots$. If $s_1 \geq r$, then $c : Bg^{r-1} \mapsto B$ but $(s_1)c = 1$ so $s_1 \in Bg^{r-1}$ i.e. $s_1 = mr$ for some natural number m. Since c acts on the blocks as an r-cycle, each cycle of c must have length which is a multiple of r. This violates the *g.c.d.* condition unless $r = 1$, in which case c is the identity element (a case we have explicitly excluded).

Thus we may assume that $s_1 < r$ and that $(1, 2, \ldots, s_1)$ is a cycle of c. Thus the action of c on some of the blocks must be $B \mapsto Bg \mapsto \cdots \mapsto Bg^{s_1-1} \mapsto B$. Now c must send $r + 1$ either to 2 or $r + 2$, but $(1)c = 2$ so $(r + 1)c = r + 2$. Proceeding in the same way we deduce that $c : r + 1 \mapsto r + 2 \mapsto \cdots \mapsto r + s_1$. Now $(r + s_1)c \neq r + s_1 + 1$ else the c-orbit of $r + 1$ will be larger than the c-orbit of 1, so $(r + s_1)c = r + 1$. Proceeding in the same way we obtain that $(1, \ldots, s_1)$, $(r + 1, \ldots, r + s_1)$, $(2r + 1, \ldots, 2r + s_1)$ etc. are all orbits of c. We recall from Definition 6.1 that the cycle lengths are weakly decreasing and this ensures that s_1 divides r, and that the early part of the cycle structure of c is

$$(1, 2, \ldots, s_1)(s_1 + 1, \ldots, 2s_1) \cdots ((u - 1)s_1 + 1, \ldots, r)$$

where $us_1 = r$. The action of c on blocks is therefore via cycles of length s_1, and since cycle lengths weakly decrease, all cycles of c have length s_1. This violates the *g.c.d.* condition unless $s_1 = 1$. However, this would entail c being the identity element, a case which we have explicitly excluded. □

We have now shown that $\langle c, g \rangle$ is primitive. Before we demonstrate that it

contains a transitive subgroup that acts primitively on its support we prove the following lemma which we shall need later.

Suppose that $\Omega = \{1, 2, \ldots, n\}$. If k is a positive integer then a k-cycle on Ω is an element of $\mathrm{Sym}(\Omega)$ with just one non-trivial orbit, and that orbit has length k.

Lemma 7.14. *Suppose that H is a permutation group on Ω and that H contains a k-cycle g. Suppose that $B_1, B_2, \ldots, B_r$ is a block system for H then either:*

1. *The support of g is a subset of a single block;*

2. *The support of g is the union of m blocks*

Proof. Suppose for contradiction that the support of g contains elements from two different blocks B_i and B_j but that B_i is not a subset of the support of g. Now g is a single cycle so it acts transitively on its support. There exists an integer l such that $B_i g^l = B_j$. However, as B_i is not entirely contained in the support of g, $B_i g = B_i$ so $B_i g^l = B_i$. Thus $B_i = B_j$ which is absurd.

Thus for each i one of the following is true: the support of g is a subset of B_i, B_i is a subset of the support of g, or B_i is disjoint from the support of g. □

Lemma 7.14 tells us that when a group contains elements with a single non-trivial orbit, these elements restrict the block sizes that can occur. Therefore, if we can construct a transitive subgroup of $\langle g, c \rangle$ that contains elements consisting solely of suitably long cycles that have length coprime to the degree of the subgroup, then we can deploy Lemma 7.14 to show it is primitive, the following lemma shows this can be done.

Lemma 7.15. *Let $g = (1, 2, \ldots, n)$, n odd, and let $c = c_1 c_2 \ldots c_k$ be a standard shape representative in A_n with support of size n and not all cycles the same length, then $\langle c, g \rangle$ contains a primitive subgroup of degree*[1] *less than $\frac{2(n-1)}{3}$*

Proof. Let l_i be the length of c_i. Now c is a standard shape representative so $l_{i+1} \leq l_i$. Now as not all cycles are the same length there exists a cycle $c_{k'}$ such that $l_{k'} > l_k$ but $l_{k'+1} = l_k$ so $c_{k'}$ is the last cycle of length longer than l_k. Let $c' = c^{-1}g = (1, s_1 + 1, s_2 + 1, \ldots, s_{k-1} + 1)$ a cycle of length k. Now let $c'' = c'^{g^{l_k}} = (1 + l_k, s_1 + 1 + l_k, \ldots, s_{k'} + 1 + l_k, s_{k'+1} + 1 + l_k, \ldots, s_{k-1} + 1 + l_k)$. Now for $i < s_{k'}$, $s_i + 1 + l_k$ is in the support of c_{i+1} and is not the first element so is not in the support of c'. However, for $s_{k'} \leq i < k$ we get $s_i + 1 + l_k = s_{i+1} + 1$ and so the support intersects that of c', finally $s_{k-1} + 1 + l_k = 1$ so $c'' = (1 + l_k, s_1 + 1 + l_k, \ldots, s_{k'-1} + 1 + l_k, s_{k'+1} + 1, s_{k'+2} + 1, \ldots, s_{k-1} + 1, 1)$. Now we let $c''' = c'c''^{-1} = (1, s_1 + 1, \ldots, s_{k'} + 1, s_{k'-1} + 1 + l_k, s_{k'-2} + 1 + l_k, \ldots, 1 + l_k)$ this is a cycle of length $2k' + 1$. Now we consider the group $C = \langle c', c''' \rangle$ this group acts on $k + k'$ letters. We intend to show C is transitive and primitive. Now each of the generators acts transitively on its support and both supports include 1, therefore C acts transitively on its entire support.

Now we turn to primitivity. Let r be any divisor of $k + k'$ now for there to be blocks of size r Lemma 7.14 tells us that there are only four possible options:

1. $k \leq r$ and $2k' + 1 \leq r$.
2. $k \leq r$ and $r | 2k' + 1$.
3. $2k' + 1 \leq r$ and $r | k$.
4. $r | k$ and $r | 2k' + 1$.

[1] We use the term *degree* of the subgroup to mean the size of its support, we hope this lax usage will not cause confusion

We show that none of these cases can occur:

1. This case cannot occur as it implies $k+k' \leq r+\frac{r-1}{2} < 2r$ so r cannot divide $k+k'$.

2. In this case we have $\{1, s_1+1, \ldots, s_{k-1}+1\}$ in a single block. c''' has support drawn from this block and other blocks. Lemma 7.14 tells us that the support of an element consisting of a single cycle must either include the whole of a block or none of it. However, the support of c''' contains 1 but does not contain $s_{k-1}+1$ and hence this case cannot occur.

3. As before the support of c''' must be drawn from a single block but neither intersects the support of c' trivially or is a subset of the support of c' so this case cannot occur.

4. Now $k+k' = mr$ and $r|k$ so let $k = m_1 r$ so $k' = r(m-m_1)$ now r cannot divide $2k'+1 = 2r(m-m_1)+1$ so this case cannot occur.

We conclude that C is primitive.

Finally we turn our attention to the degree of C. Now we want to maximise $k+k'$, this will occur when the c_i are shortest therefore we want to only use 4-cycles, 3-cycles and transpositions.

We deal with the case where c contains only 3-cycles and transpositions first. Now $n = 3k' + 2(k-k') = 2k + k'$ so $k = \frac{n-k'}{2}$ now $Degree(C) = k+k' = \frac{n-k'}{2} + k' = \frac{n+k'}{2}$ and this is maximised when k' is maximised so there are only two transpositions so $k' = \frac{n-4}{3}$ whereby $Degree(C) = \frac{2(n-1)}{3}$.

Now if c contains a 4-cycle, then we assume it contains k'' of them and we get

$n = 4k'' + 3(k' - k'') + 2(k - k') = 2k + k' + k''$ so $k = \frac{n-k'-k''}{2}$ and so

$$Degree(C) = k + k' = \frac{n - k' - k''}{2} + k' = \frac{n + k' - k''}{2}$$

This is maximised when $k' - k''$ is maximised and this will occur when k' is maximum and k'' is minimum so c contains a single transposition and a single 4-cycle so $k' = \frac{n-6}{3} + 1$ and $Degree(C) = \frac{4n-6}{6} \leq \frac{2(n-1)}{3}$ □

Now for $n \geq 7$ we can deduce that $\langle c, g \rangle$ is at least 4-transitive and for $n \geq 9$ is at least 5-transitive so for $n \geq 7$ it must be the alternating group. For $n < 7$ the case is less clear. For $n = 3$ the only standard shape representative that has support size n is $(1, 2, 3) = g$ and $\langle g \rangle = A_n$. However, for $n = 5$ the only shape with support size n is $(1, 2, 3, 4, 5)$ and $\langle g \rangle < A_n$.

7.3 Conclusion

We are now in a position to state the theorem in full.

Theorem 7.16. *Let $g = (1, 2, \ldots, n)$, n odd, and let c be a standard shape representative in A_n. If the greatest common divisor of the cycle lengths of c is 1, then $\langle c, g \rangle = A_n$ or $\langle g \rangle$; the latter only occurs when $c = g$ or $c = id$.*

Proof. Clearly if $c = g$ or id then $\langle c, g \rangle = \langle g \rangle$.

We have dealt with the case where the size of the support of c is less than n in Lemma 7.11. Finally where the size of the support of c is n we may apply Theorem 7.13 and Lemma 7.15 to show that $\langle c, g \rangle$ is primitive and has a transitive primitive subgroup of degree less than $\frac{2(n-1)}{3}$ and we deploy Theorem 7.12 to show that $\langle c, g \rangle$ is at least 4-transitive, and at least 5-transitive for $n \geq 9$ and hence A_n. □

Chapter 8

Generating S_n from standard shape representatives

Having shown that the standard n-cycle together with most standard shape representatives generates A_n when n is odd, we seek to extend this to the symmetric group. Clearly where n is odd this can only happen where the shape representative is odd.

For even $n \leq 34$ direct computation in GAP shows that Theorem 7.16 holds with S_n taking the same rôle as A_n with one exception. Our aim in this chapter will be to extend this to a formal proof. We begin by looking at the exception, this occurs when $n = 6$ and $c = (1,2)(3,4)$ the following lemma gives the answer in this case.

Lemma 8.1. *The subgroup of S_6 generated by $(1,2,3,4,5,6)$ and $(1,2)(3,4)$ is isomorphic to S_5*

Proof. Let $x, y \in S_5$ be the permutations $x = (1,2,3)(4,5)$, $y = (1,4)(2,3)$.

Let $P = \langle (1,2,3,4,5) \rangle$ so $P \in \mathrm{Syl}_5(S_5)$. There are six Sylow 5-subgroups

of S_5, each one generated by a unique element of the shape $(1,2,a,b,c)$ where $\{a,b,c\} = \{3,4,5\}$. Thus we may identify each group via one of the six possible ordered triples with entries 3, 4 and 5. Now let $P_5 = P = (3,4,5)$. A direct calculation yields that $P_6 = P^x = (5,3,4)$, $P_1 = P^{x^2} = (4,5,3)$, $P_2 = P^{x^3} = (3,5,4)$, $P_3 = P^{x^4} = (4,3,5)$ and $P^{x^5} = P_4 = (5,4,3)$.

Conjugation by x on these Sylow 5-subgroups gives rise to the permutation $(1,2,3,4,5,6)$ where the numbers are the subscripts of the groups. A similar calculation reveals that conjugation by y on these Sylow 5-groups gives rise to the permutation $(1,2)(3,4)$.

There is homomorphism $\alpha : S_5 \longrightarrow S_6$ defined by associating to each $g \in S_5$ the permutation which describes conjugation by g on the Sylow 5-subgroups of S_5.

Let $N = \text{Ker } \alpha$. Since x conjugates the Sylow 5-subgroups in a 6-cycle, then $|S_5 : N| \geq 6$ so $|A_5 : A_5 \cap N| \geq 3$. Now A_5 is simple so $A_5 \cap N$ is trivial so $|N| \leq 2$.

If N had order 2, then it would be central in S_5. The centre of S_5 is trivial so N is trivial and α is a monomorphosm.

Now $\alpha : x \mapsto (1,2,3,4,5,6)$ and $y \mapsto (1,2)(3,4)$.

Notice that $x^2 = (1,3,2)$, $x^3 = (4,5)$, $[x,y] = (1,2,5,3,4)$.

Let $L = \langle x,y \rangle$ now as L contains both a 5-cycle and a transposition then it must be S_5 and we are done. □

Thus the subgroup of S_6 generated by $(1,2,3,4,5,6)$ and $(1,2)(3,4)$ is a copy of S_5. This is not surprising because Aut S_6 does not consist just of inner automorphisms, and one might expect point stabilizers to be sent to interesting places by non-inner automorphisms of S_6.

Having dealt with the exception we we now proceed as in Chapter 7 by demonstrating some concrete generators of S_n constructively.

8.1 Shapes that do not generate S_n

Clearly Lemma 7.1 extends to the symmetric group. We restate its more general form here.

Lemma 8.2. *Let $g = (1, 2, \ldots, n)$ and let c be a standard shape representative in S_n. Then $\langle c, g\rangle = \langle g\rangle$ if and only if $c = g$ or $c = id$*

Our computations in GAP tell us that Corollary 7.3 applies equally to the symmetric group, Lemma 8.3 extends this result.

Lemma 8.3. *Let $g = (1, 2, \ldots, n)$, and let $c = c_1 c_2 \ldots c_k$ where*

$$c_i = (s_{i-1} + 1, s_{i-1} + 2, \ldots, s_i)$$

$s_k = n$ and $r | s_i - s_{i-1}$ or $c = id$ then $G = \langle g, c\rangle < S_n$.

Proof. We partition $\{1, 2, \ldots, n\}$ into equivalence classes modulo r and consider the action of powers of g and c respectively, both respect the partitions and hence G is imprimitive and so $G < S_n$ □

8.2 Shapes that generate S_n

We now turn our attention to standard shape representatives that generate S_n, as before we deal with the case where the size of the support of c is less than n first.

8.2.1 Standard shapes with support size less than n

It is well known that the standard n-cycle and the transposition $(1,2)$ will generate S_n. We begin by giving a short proof of this result.

Lemma 8.4. *Let $g = (1,2\ldots,n)$, and let $c = (1,2)$ then $G = \langle g, c\rangle = S_n$*

Proof. First we observe that every element in S_n can be written as a product of transpositions. Therefore we need only show that G contains all transpositions and we are done.

We may repeatedly conjugate by g to show that G contains all transpositions of the form $(a, a+1)$ where addition is modulo n. We now use induction, observe that $(a, a+i) = (a, a+i-1)(a+i-1, a+i)(a, a+i-1)$, the middle transposition is of the required form and we may use induction on the two end transpositions and we are done □

We now consider the case where c has a single non-trivial orbit. Before we look at general cycles we deal with two special cases of 3-cycles.

Lemma 8.5. *Let $g = (1,2,\ldots,n)$, n even, and let $c = (1,2,a)$. Then $G = \langle g, c\rangle = S_n$*

Proof. If $a = n$, then we let $c' = c^g = (1,2,3)$. Now if $3 < a < n$, then we let

$$\begin{aligned} c' = [c^{-1}, c^g] &= (1,2,a)(2,a+1,3)(1,a,2)(2,3,a+1) \\ &= (1,a+1,3,2,a)(1,a,2)(2,3,a+1) \\ &= (1,a+1,3)(2,3,a+1) \\ &= (1,2,3) \end{aligned}$$

Observe that $(c'^{-1}g)^{g^{-3}} = (1, 2, \ldots, n-2)$. We set up an iterative process. Let $g_0 = g$ and let $g_{i+1} = (c'^{-1}g_i)^{g_i{}^{-3}}$, now $g_i = (1, 2, \ldots, n-2i)$ so $g_{\frac{n-2}{2}} = (1, 2)$ and we may apply Lemma 8.4 we are done. □

We now generalise this to cover any 3-cycle that has two numerically adjacent elements

Corollary 8.6. *Let $g = (1, 2, \ldots, n)$, n even, and let $c = (a, a+1, b)$ then $G = \langle g, c \rangle = S_n$*

Proof. We note that $c^{g^{1-a}} = (1, 2, b-a+1)$ so we may apply Lemma 8.5 □

We now prove a result which is useful for standard shape representatives that contain a 3-cycle, transpositions and 1-cycles only.

Lemma 8.7. *Let $g = (1, 2, \ldots, n)$ and let c be a standard shape representative in S_n consisting of a single 3-cycle plus transpositions and 1-cycles. If one of g or c is an odd permutation, then $G = \langle g, c \rangle = S_n$*

Proof. Observe that $c^4 = (1, 2, 3)$. Now if n is even, then we may apply Lemma 8.5 directly. However, if n is odd, then this is not the case, instead we apply Lemma 7.10 to show that $A_n \leq G$ and since G contains at least one odd permutation we conclude that $G = S_n$. □

We now turn our attention to the case where c consists of a single cycle. Of course if the cycle is of odd length and n is odd then we already know that $\langle g, c \rangle$ will be A_n rather than S_n.

Lemma 8.8. *Let $g = (1, 2 \ldots, n)$, and let $c = (1, 2, \ldots, m)$, $2 \leq m < n$, then*

$$G = \langle g, c \rangle = \begin{cases} A_n & n, m \text{ both odd} \\ S_n & \text{otherwise} \end{cases}$$

Proof. First we deal with the case where both m and n are odd. In this case Lemma 7.10 applies and $G = A_n$.

Now if n is odd and m is even, then consider $(c^g)^{-1} c = (1, 2, m{+}1)$. Lemma 7.9 tells us that $\langle g, (1, 2, m+1)\rangle = A_n$. Now $G \geq \langle g, (1, 2, m+1)\rangle$ so $G \geq A_n$ but G contains an odd element so $G > A_n$ and as A_n is a maximal subgroup of S_n so we deduce $G = S_n$

This deals with all of the cases where n is odd and we turn our attention to the case that n is even. First observe that if $m = n - 1$, then $gc^{-1} = (n-1, n)$ which we may conjugate by g^2 to get $(1, 2) \in G$ and by Lemma 8.4 we are done. Equally, if $m = 2$, then $c = (1, 2)$ and we are done.

Now if $2 < m < n - 1$, then we observe that $c\,(c^g)^{-1} = (1, m+1, m)$. Now let $c' = (1, m, m+1)^{g^{1-m}} = (1, 2, n+2-m)$. Now $n + 2 - m \neq 1, 2$ as this would require $m \geq n - 1$ so we may apply Lemma 8.5 and we are done. □

Having dealt with transpositions and single cycles we now turn our attention to other standard shape representatives where the size of the support is smaller than n. We first examine the proof of Lemma 7.11 and note that it relied on Corollary 7.5. Unfortunately the analogue of Corollary 7.5 fails in S_n when $b - a | n$ so we cannot use the same construction.

Instead we seek to expand on the proof given for A_n when the standard shape representative had support size n. First we note that Theorem 7.13 applies irrespective of whether the size of the support of c is n or not. Indeed when the size of the support is less than n the greatest common divisor condition is automatically met as c contains 1-cycles.

We first prove a result about c when c consists solely of transpositions.

Lemma 8.9. *Let $g = (1, 2, \ldots, n)$,n even, and let $c = c_1 c_2 \ldots c_k$ be a standard*

shape representative in S_n with the c_i being disjoint transpositions and $2k \leq n-2$. Then $G = \langle g, c \rangle = S_n$ or G is isomorphic to S_5

Proof. The case where G is isomorphic to S_5 occurs when $n = 6$ and $k = 2$ and this is shown in Lemma 8.1.

We now deal with the general case. we will show in all cases, except one, that G is S_n by showing that it is more transitive than any other group of that degree. In practice this means for all but $n = 12$ or 24 we need to show G is at least 4-transitive, for $n = 12$ or 24 we need to demonstrate G is at least 6-transitive as M_{12} and M_{24} are both 5-transitive. We use three constructions and convert each case to one of these:

1. We let

$$c' = cc^{g^2} = (1,2)(2k+1, 2k+2)$$

and let

$$c'' = c^{-1}g = (1, 3, \ldots, 2k+1, 2k+2, \ldots, n)$$

so c'' is a cycle of length $n-k+1$. Let $C = \langle c', c'' \rangle$, clearly c'' acts transitively on its support, this only leaves 2 but we may map any element to 2 via a suitable power of c'' composed with c' so C is transitive. C has degree $n-k+2$ and we may use Lemma 7.14 to show that C is primitive. We may now use Theorem 7.12 to show G is $k-1$ transitive, so G is 6-transitive if $k \geq 7$ and 4-transitive if $k \geq 5$

2. If $c = (1,2)(3,4)\ldots(2k-1, 2k)$ and $n \geq 6$ and $2k+1$ prime, then let

$$c' = cc^g = (1, 3, \ldots, 2k-1, 2k+1, 2k, 2k-2, \ldots, 2).$$

We let $C = \langle c' \rangle$. Now c' is of prime length so C is a transitive primitive subgroup of G of degree $2k+1$ so by Theorem 7.12 G is at least $(n-2k)$-transitive.

3. If $c = (1,2)(3,4)\ldots(2k-1,2k)$ and $n \geq 6$ then, let

$$c' = cc^g = (1,3,\ldots,2k-1,2k+1,2k,2k-2,\ldots,2)$$

c' is a cycle of length $2k+1$. Let

$$c'' = cc^{g^2} = (1,2)(2k+1,2k+2).$$

We let $C = \langle c', c'' \rangle$. Now C is of degree $2k+2$. C is clearly transitive as it is transitive on the support of c' which only leaves $2k+2$ but we can map any element to $2k+2$ by mapping it it $2k+1$ and then applying c''. Now Lemma 7.14 tells us that C is primitive as it contains a cycle of length $2k-1$ which is coprime to the degree of C. We now apply Theorem 7.12 to show that G is at least $(n-2k-1)$-transitive.

We now consider how many transpositions c has:

1. $k = 1$. Now $c = (1,2)$ and we may apply Lemma 8.4 directly.

2. $k = 2$. Now $c = (1,2)(3,4)$. Now if $n = 6$, then we are in the special case. For $n \geq 8$ we use case 2 to show G is at least $(n-4)$-transitive and so is at least 4-transitive, in particular for $n \geq 12$ G is at least 8-transitive.

3. $k = 3$. For $n = 8$ we observe that $\left(cc^{g^2}\right)^{g^2} = (1,2)(3,4)$ and we are in case 2 and G is at least 4-transitive. For $n \geq 10$ we observe that $2k+1 = 7$

so we are in case 2 and G is at least 4-transitive, and for $n \geq 12$ G is at least 6-transitive .

4. $k = 4$. For $n = 10$ we observe that $\left(cc^{g^2}\right)^{g^2} = (1,2)(3,4)$ and we are in case 2 and G is at least 6-transitive. For $n = 12$ we let $c' = cc^{g^2} = (1,2)(9,10)$ and let $c'' = c'^{g^5} = (2,3)(6,7)$. Now we consider:

$$c''' = c'c'' = (1,2)(9,10)(2,3)(6,7) = (1,3,2)(6,7)(9,10).$$

Now we may square c''' to get $(1,2,3) \in G$ and Lemma 8.5 tells us that $G = S_n$. Now for $n \geq 14$, we are in case 3, $n - 2k - 1 \geq 5$ so G is at least 5-transitive, in particular when $n = 24$, G is at least 15-transitive.

5. $k = 5$. For all n except 12 and 24 we can use case 1 and G is at least 4-transitive. We need only worry about the two Mathieu groups. For $n = 12$ we observe that $\left(cc^{g^2}\right)^{g^2} = (1,2)(3,4)$ and we are in case 2 and G is at least 8-transitive. For $n = 24$ we observe that $2k + 1 = 11$ which is prime so we are in case 2 and G is at least 14-transitive.

6. $k = 6$. For $n \neq 24$ we may apply case 1 to show G is at least 5-transitive. For $n = 24$ we observe that $2k + 1 = 13$ which is prime so we are in case 2 and G is at least 12-transitive.

7. $k \geq 7$ We may apply case 1 and G is at least 7-transitive.

□

We now turn our attention to proving an analogue of Lemma 7.15 for c with support of size less than n.

Lemma 8.10. *Let $g = (1, 2, \ldots, n)$, and let $c = c_1 c_2 \ldots c_k$ be a standard shape representative in S_n with support size $s_k < n$ and at least one cycle of length greater than 2. Then $G = \langle c, g \rangle$ contains a primitive subgroup. The degree of which is $2k + 2$ if c contains no transpositions, and $2k + 1$ otherwise.*

Proof. We use the notation and construction of Lemma 7.11. We recall that:

$$c' = c\,(c^g)^{-1} = (1, s_1 + 1, s_2 + 1, \ldots, s_k + 1, s_k, s_{k-1}, \ldots, s_1)$$

and

$$c'' = (c^g)^{-1} c = (2, s_1 + 2, s_2 + 2, \ldots, s_{k-1} + 2, s_k + 1, s_{k-1} + 1, s_{k-2} + 1, \ldots, 1)$$

Therefore, c' is a cycle of length $2k + 1$. Now provided that the non-trivial orbits of c are not all of length 2 then let:

$$c''' = [c'c''] = \begin{cases} (1,2)(s_k, s_k + 1) & c \text{ contains no transpositions} \\ (1,2)(s_{k'}, s_{k'+1}) & \text{otherwise} \end{cases}$$

We consider the group $C = \langle c', c''' \rangle$.

Now in the case where c contains no transpositions, C has degree $2k + 2$. C clearly acts transitively on the support of c' which only leaves 2 but we can reach 2 via a suitable power of c' and post-multiplying by c''' so C is transitive. Lemma 7.14 tells us C is primitive as it contains a cycle one shorter than the degree of C which therefore has length coprime to the degree of C.

Now if c contains transpositions, then the support of c''' is contained within the support of c' so C has degree $2k + 1$ and is clearly transitive. We recall from the proof of Lemma 7.14 that if the support of a cycle is drawn from more than

one block the cycle permutes the blocks. For contradiction we assume that C has a block structure. Now as 1 and 2 are adjacent in c' they cannot be in the same block. However, 1 and 2 are in the same cycle in c''' so c''' must map the block containing 1 to the block containing 2. c''' only moves two other elements and we conclude that these must constitute the remainder of the blocks including 1 and 2. Therefore, the blocks must be of size 2, but $2k+1$ is odd so blocks of size 2 cannot occur so we conclude that C is primitive. □

We are now in a position to prove the analogue of Lemma 7.11.

Lemma 8.11. *Let $g = (1, 2, \ldots, n)$ and c be a standard shape representative in S_n and let the size of the support of c be less than n. Then*

$$G = \langle g, c \rangle = \begin{cases} \langle g \rangle & c = g \text{ or } c = id \\ A_n & n \text{ odd and } c \text{ an even element of } S_n \\ \text{Isomorphic to } S_5 & n = 6 \text{ and } c = (1,2)(3,4) \\ S_n & \text{otherwise} \end{cases}$$

Proof. The cases where $c = g$ or id follow directly from Lemma 8.2. Similarly, the case where n is odd and c an even standard shape representative is covered by Lemma 7.11. The case where $n = 6$ and $c = (1,2)(3,4)$ is covered in Lemma 8.1.

We now turn our attention to the cases where one of g or c is an odd element. Clearly, G is transitive and we deploy Theorem 7.13 to show that it is also primitive.

We deal with the case where c consists solely of transpositions first. Now if n is odd and $s_k < n-2$, then $cc^{g^2} = (1,2)(s_k+1, s_k+2)$ and we can use Lemma 7.4 to show $A_n \leq G$ and conclude that, as G contains an odd cycle, $G = S_n$. If n is odd and $s_k = n-1$, then $c\left(c^{g^2}\right)^{-1} = (1,2,n)$ and conjugation by g yields $(1,2,3)$

and we may apply Lemma 7.8 to show $A_n < G$ and conclude that, as G contains an odd cycle, $G = S_n$.

Now if n is even and c consists solely of transpositions, then we may apply Lemma 8.9 and we are done.

We first note that, if c is a single cycle, then Lemma 8.8 assures us that $G = S_n$.

Provided that G is at least 4-transitive it must be one of S_n, A_n, M_{11}, M_{12}, M_{23}, or M_{24}. We may rule out A_n as we have insisted that either c or g is odd. We will show that G is not one of the Mathieu groups by showing, for suitable n, that G is either 5 or 6 transitive. For all but $n = 11, 12, 23$, or 24 we will show G is 4-transitive. Now we can show G is highly transitive if either c has relatively small support or c contains some long cycles.

We construct C as in Lemma 8.10. Now if c does not contain any transpositions, then C is of degree $2k + 2$ and is primitive and transitive therefore G is $n - 2k - 1$ transitive. Similarly, if c contains some transpositions, then C is of degree $2k + 1$ and is primitive and transitive therefore G is $n - 2k$ transitive.

Recall that $|Supp(c)| = s_k$. Now each cycle in c contains at least two elements so $k \leq \frac{s_k}{2}$. Now if $s_k \leq n - 7$, then we are done as G is at least $n - 2\frac{n-7}{2} - 1 = 6$-transitive. We have already insisted that the size of the support of c is at most $n - 1$. We now consider the remaining cases where $n - 6 \leq s_k \leq n - 1$.

1. $s_k = n - 6$ This implies G is at least 5-transitive. Now if c contains a transposition, then G is at least 6-transitive and we are done. If c contains a cycle of length at least 3, then $k \leq \frac{n-9}{2} + 1 = \frac{n-7}{2}$ and we deduce G is at least 6-transitive.

2. $s_k = n - 5$ This implies G is at least 4-transitive. If c contains a cycle of

length at least 4, then G is at least 6-transitive and we are done. This leaves only the case where c contains only 3-cycles and transpositions. If c contains two or more 3-cycles, then G is at least 6-transitive. If c contains a single 3-cycle and transpositions, then $c^4 = (1,2,3)$ and we can use Lemma 8.7.

3. $s_k = n - 4$ This implies G is at least 3-transitive. If c contains a cycle of length at least 5, then G is at least 6-transitive and we are done. Equally, if c contains two 4 cycles or a 4-cycle and a 3-cycle, then G is at least 6-transitive and we are done. If c contains a 4-cycle plus transpositions then G is $n - 2k$ transitive and $k = \frac{n-6}{2}$ so G is at least 6-transitive. This leaves only the case where c contains 2 3-cycles plus transpositions or a single 3-cycle. If c contains two 3-cycles plus transpositions, then $n \geq 10$ as $s_k \geq 6$. Now $c^4 = (1,2,3)(4,5,6)$ and is a standard shape representative and we can deduce G is at least 5-transitive and is at least 6-transitive for $n \geq 11$. If c has a single 3-cycle then, $c^4 = (1,2,3)$ now if n is even, then we may apply Lemma 8.5 and we are done. If n is odd, then we may apply Lemma 7.8 to deduce $A_n \leq G$ and as G contains an odd cycle we deduce $G = S_n$.

4. $s_k = n - 3$ This implies G is at least 2-transitive. If c contains a cycle of length at least 6, then G is at least 6-transitive and we are done. Equally, if c contains two cycles of length at least 4, then G is at least 6-transitive and we are done. This leaves only 3 possible cases:

   (a) *The longest cycle in c is a 5-cycle.* If c contains any other cycles, then G is at least 6 transitive. If not, then we may apply Lemma 8.8 and we are done.

(b) *The longest cycle in c is a 4-cycle.* If c contains at least 2 4-cycles, then G is at least 6-transitive. If c contains at least 2 3-cycles, then G is at least 6-transitive. If c consists of a 4-cycle, a 3-cycle and possibly some transpositions, then $c^4 = (5,6,7)$ and we may conjugate by g^{-3} to get $(1,2,3) \in G$. Now if n is even, then we can then apply Lemma 8.5. If n is odd, then we apply Lemma 7.8 to show $A_n < G$ and deduce $G = S_n$. Now if c consists of a 4-cycle plus transpositions only then G is $n-2k$ transitive and $k = \frac{n-5}{2}$ so G is 5-transitive and n must be odd as the support is of even size so $G = S_n$.

(c) *The longest cycle in c is a 3-cycle.* If c contains any transpositions, then $|Supp(c^4)| \leq n-5$ and we are in case 2. This leaves only the cases where c consists solely of 3-cycles. If $c = (1,2,3)$, then we may apply Lemma 8.5. If $c = (1,2,3)(4,5,6)$, then $n = 9$ and G is $9-4-1 = 4$-transitive and we are done. If $c = (1,2,3)(4,5,6)(7,8,9)$, then $n = 12$ and we require G to be 6-transitive. Now observe that $c(c^g)^{-1} = (1,4,7,10,9,6,3)$ which generates a transitive primitive group of degree 7 and Theorem 7.12 tells us G is at least 6-transitive.

5. $s_k = n-2$ If c contains a cycle of length at least 7, then G is 6-transitive and we are done. This leaves only 4 possible cases.

(a) *The longest cycle in c is a 6-cycle.* If c contains any other cycle, then G is at least 6-transitive. If c contains a single 6-cycle, then we may use Lemma 8.8.

(b) *The longest cycle in c is a 5-cycle.* If c also contains a cycle of length at least 4, then G is at least 6-transitive and we are done. Otherwise c only contains 3-cycles and transpositions, in any case $c^6 = (1,2,3,4,5)$

and we may apply Lemma 8.8.

(c) *The longest cycle in c is a 4-cycle.* If c contains 2 4-cycles and any other cycle, then G is at least 6-transitive and we are done. If c contains any 3 cycles, then $|Supp(c^4)| \leq n-6$ and we may conjugate c^4 to make it a standard shape representative. Now $k < \frac{n-6}{3}$ and so G is at least 6-transitive as $n \geq 9$. This only leaves the case where c has 4-cycles and transpositions. Now if c has 2 4-cycles, then $c' = c^2 = (1,3)(2,4)(5,7)(6,8)$ and we consider $c'c'^g = (1,5,9,7,3)$. $\langle c'c'^g \rangle$ is a transitive primitive subgroup of G of degree 5, so for $n \geq 10$ Theorem 7.12 tells us that G is at least 6-transitive. Now if c has only one 4-cycle, then let $c' = c^2 = (1,3)(2,4)$ and $c'c'^g = (1,5,3)$ and this generates a transitive primitive subgroup of G of degree 3 so for $n \geq 7$ Theorem 7.12 tells us that G is at least 5-transitive and for $n \geq 8$ G is at least 6-transitive.

(d) *The longest cycle in c is a 3-cycle.* If c contains any transpositions then $|Supp(c^4)| \leq n-4$ so if $n > 7$, then G is at least 4-transitive, for $n \geq 10$ G is at least 5-transitive and for $n \geq 13$ G is at least 6-transitive, this leaves only M_{12} but for $n = 12$ the only standard shape representative consisting of 3-cycles and transpositions with support size $n-2$ has 2 transpositions so $|Supp(c^4)| = n-6$ and G is at least 7-transitive. Now if c consists solely of 3-cycles, then G is at least 4-transitive for $n \geq 11$, 5-transitive for $n \geq 14$, and 6-transitive for $n \geq 17$. Now if $n = 4$, then we may use Lemma 8.5 directly. Now if $n = 8$, then let $c' = c\,(c^g)^{-1} = (1,4,7,6,3)$ now the cyclic subgroup of G generated by c' is of degree 5 and is transitive and primitive as c' has prime length,

so by Theorem 7.12 G is at least 4-transitive. We now come to $n = 11$, now M_{11} is 4-transitive and we are only assured of 4-transitivity by our standard construction. Let $c' = c\left(c^{g^3}\right)^{-1} = (1,2,3,10,11)$ now $\langle c' \rangle$ is a transitive primitive subgroup of G of degree 5 so by Theorem 7.12 G is at least 7-transitive.

6. $s_k = n - 1$ If c contains a cycle of length at least 8, then G is 6-transitive and we are done. This leaves 6 cases:

   (a) *The longest cycle in c is a 7 cycle.* Now if c contains any other cycle, then G is 6-transitive. Otherwise c must be a single 7-cycle and we may use Lemma 8.8.

   (b) *The longest cycle in c is a 6-cycle.* Now if c also contains a 4,5 or 6-cycle, then G is at least 6-transitive and we are done. Now if c contains only a 6-cycle and transpositions, then $n \geq 9$. Observe that $c^2 = (1,3,5)(2,4,6)$ now let $c' = c^2\left((c^2)^g\right)^{-1} = (1,7,5)$. We deduce that G contains a transitive primitive group of degree 3 and Theorem 7.12 gives us G is at least 7-transitive. Now if c contains a 6-cycle, some 3-cycles and some transpositions then G is $n - 2k$ transitive and $k \leq \frac{n-10}{2} + 2 = \frac{n-6}{2}$ so G is at least 6-transitive. This leaves only the case where c has only a 6-cycle and 3-cycles. Now $n \geq 10$, let $c' = c^3 = (1,4)(2,5)(3,6)$ and observe that $c'c'^g = (1,7,4)$, we deduce that G contains a transitive primitive subgroup of degree 3 so G is at least 8-transitive for $n \geq 10$.

   (c) *The longest cycle in c is a 5-cycle.* If c has more than one 5-cycle, then G is at least 6-transitive and we are done. If c has only one 5-cycle, then the other cycles have length coprime to 5 so there is a power of

c that is $(1,2,3,4,5)$ and we may apply Lemma 8.8.

(d) *The longest cycle in c is a 4-cycle.* If c contains 3 4-cycles, then G is at least 6-transitive and we are done. If c contains any 3 cycles, then $n \geq 8$ and $|Supp(c^4)| \leq n-5$, furthermore we may conjugate by a power of g so that we have a standard shape representative with at most $\frac{n-5}{3}$ cycles and so for $n \geq 8$ G is at least 5-transitive and for $n \geq 11$ G is at least 6-transitive. This leaves only the case where c has less than 3 4-cycles and no 3-cycles. Now if c has 2 4-cycles, then let $c' = c^2 = (1,3)(2,4)(5,7)(6,8)$ and we consider $c'c'^g = (1,5,9,7,3)$ now this generates a transitive primitive subgroup of G of degree 5, so for $n \geq 9$ we may use Theorem 7.12 to show G is at least 5-transitive and for $n \geq 11$ G is at least 7-transitive. Now if c has only 1 4-cycle, then let $c' = c^2 = (1,3)(2,4)$ and $c'c'^g = (1,5,3)$ and this generates a transitive primitive subgroup of G of degree 3 so for $n \geq 7$ we may use Theorem 7.12 to show G is at least 5-transitive and for $n \geq 9$ G is at least 7-transitive. This leaves the case where $n = 5$ in this case c must be $(1,2,3,4)$ and we may apply Lemma 8.8.

(e) *The longest cycle in c is a 3-cycle.* If c contains any transpositions, then $|Supp(c^4)| \leq n-3$ so G is at least 4-transitive for $n > 6$, 5-transitive for $n \geq 11$ and 6-transitive for $n \geq 14$, this leaves only M_{12}. For $n = 12$ the only standard shape representatives consisting of 3-cycles and transpositions with support size $n-1$ are $c = (1,2,3)(4,5)(6,7)(8,9)(10,11)$ and $c = (1,2,3)(4,5,6)(7,8,9)(10,11)$, in the first case $c^4 = (1,2,3)$ and we may apply Lemma 8.5. In the second case $c\left(c^{g^3}\right)^{-1} = (1,2,3,11,10)$ and we conclude that G has

a primitive transitive subgroup of degree 5 and so by Theorem 7.12 G is at least 8-transitive. Now if c consists solely of 3-cycles, then G is at least 4-transitive for $n \geq 13$, and 6-transitive for $n \geq 19$. We consider the cases where $n = 4, 7, 10$ separately. Now if $n = 4$, then we have a single 3-cycle and we may apply Lemma 8.5. If $n = 7$, then $c = (1,2,3)(4,5,6)$ and $c\left(c^{g^3}\right)^{-1} = (2,3,7)$ and so by Theorem 7.12 G is at least 5-transitive. Finally, if $n = 10$ then $c = (1,2,3)(4,5,6)(7,8,9)$ and $c\left(c^{g^3}\right)^{-1} = (2,3,10)$ and so by Theorem 7.12 G is at least 8-transitive and we are done.

□

8.2.2 Shapes with support size n

Finally we turn our attention to the case where c is a standard shape representative with support of size n. As before we generate a transitive primitive subgroup of $G = \langle g, c \rangle$ and then use Theorem 7.12 to show that G is highly transitive.

We begin by expanding Lemma 7.15 to cover even elements.

Lemma 8.12. *Let $g = (1,2,\ldots,n)$, and let $c = c_1 c_2 \ldots c_k$ be a standard shape representative in S_n with support of size n and not all cycles the same length, then $G = \langle c, g \rangle$ contains a primitive subgroup of degree less than $\frac{2n-1}{3}$*

Proof. We use the same construction as in Lemma 7.15 and observe that we may still conclude that C is both transitive and primitive. We now turn our attention to the degree of C.

We want to maximise $k + k'$, this will occur when the c_i are shortest therefore we want to only use 4-cycles, 3-cycles and transpositions.

We deal with the case where c contains only 3-cycles and transpositions first. Now $n = 3k' + 2(k - k') = 2k + k'$ so $k = \frac{n-k'}{2}$ now $Degree(C) = k + k' = \frac{n-k'}{2} + k' = \frac{n+k'}{2}$ and this is maximised when k' is maximised so there is only one transposition so $k' = \frac{n-2}{3}$ whereby $Degree(C) = \frac{2n-1}{3}$.

Now if c contains a 4-cycle, then we assume it contains k'' of them and we get $n = 4k'' + 3(k' - k'') + 2(k - k') = 2k + k' + k''$ so $k = \frac{n-k'-k''}{2}$ and so $Degree(C) = k + k' = \frac{n-k'-k''}{2} + k' = \frac{n+k'-k''}{2}$ and this is maximised when $k' - k''$ is maximised and this will occur when k' is maximum and k'' is minimum so c contains a single transposition and a single 4-cycle so $k' = \frac{n-6}{3} + 1$ and $Degree(C) = \frac{4n-6}{6} \leq \frac{2(n-1)}{3}$ □

Now for $n \geq 8$ we can deduce that G is at least 4-transitive and hence if $n \neq 11, 12, 23$, or 24, then G is either A_n or S_n.

8.3 Conclusion

We now conclude chapters 7 and 8 with a final summary of our main results from this section.

Theorem 8.13. *Let $g = (1, 2, \ldots, n)$ and let c be a standard shape representative in S_n. If the greatest common divisor of the cycle lengths of c is 1, then:*

$$G = \langle g, c \rangle = \begin{cases} \langle g \rangle & c = g \text{ or } c = id \\ A_n & n \text{ odd and } c \text{ an even element of } S_n \\ \text{Isomorphic to } S_5 & n = 6 \text{ and } c = (1,2)(3,4) \\ S_n & \text{otherwise} \end{cases}$$

Proof. Clearly if $c = g$ or id, then $\langle c, g \rangle = \langle g \rangle$.

Theorem 7.16 covers the case when n is odd and c is an even element. Equally, Lemma 8.1 deals with the case where $n = 6$ and $c = (1,2)(3,4)$.

This leaves only the cases where either n is even or c is an odd element. We have already dealt with the cases where the size of the support of c is less than n in Lemma 8.11. We now turn our attention to the case where the size of the support of c is n. Lemma 8.12 tells us that G contains a transitive primitive subgroup of degree at most $\frac{2n-1}{3}$. If $n \geq 17$, then we conclude that G is at least 7-transitive and we are done. If $n \geq 11$, then G is at least 5-transitive and if $n \geq 8$, then G is at least 4-transitive. This leaves only the cases where $n < 8$ or $n = 12$ where G could be M_{12}. We deal with each in turn:

1. If $n = 3$, then the only element with support size n is $c = (1,2,3) = g$ which we have ruled out.

2. If $n = 4$, then the only elements with support size n are $c = (1,2,3,4) = g$ which we have ruled out and $c = (1,2)(3,4)$ which we have ruled out as the greatest common divisor of the cycle lengths is 2.

3. If $n = 5$, then the only elements with support size n are $c = (1,2,3,4,5) = g$ which we have ruled out and $c = (1,2,3)(4,5)$ now $c^4 = (1,2,3)$ and we may apply Lemma 8.11.

4. If $n = 6$, then the only elements with support size n are $c = (1,2,3,4,5,6)$ which we have ruled out, $c = (1,2,3)(4,5,6)$,$c = (1,2,3,4)(5,6)$, and $c = (1,2)(3,4)(5,6)$ all of which we have ruled out as the greatest common divisor of their cycle lengths is greater than 1.

5. If $n = 7$, then there are only 4 elements with support size n. We have ruled out the case where $c = (1,2,3,4,5,6,7) = g$. If $c = (1,2,3,4,5)(6,7)$, then

$c^6 = (1,2,3,4,5)$ and we may apply Lemma 8.11. If $c = (1,2,3,4)(5,6,7)$, then $(c^4)^{g^{-4}} = (1,2,3)$ and we may apply Lemma 8.8. If $c = (1,2,3)(4,5)(6,7)$, then $c^4 = (1,2,3)$ and we may apply Lemma 8.8.

6. If $n = 12$, then if c contains a single transposition, then the remaining support of c has size 10 so must contain a cycle of length at least 4 in which case C has degree at most 7 and Theorem 7.12 tells us that G is at least 6-transitive so cannot be M_{12}. If c does not contain a transposition, then c has at most 3 cycles and so C has degree at most 5 and Theorem 7.12 tells us that G is at least 8-transitive. Now if c contains more than one transposition then c is one of the following elements:

   - $c = (1,2,3,4,5)(6,7,8)(9,10)(11,12)$ and $c^6 = (1,2,3,4,5)$ so G has a transitive primitive subgroup of degree 5 and so G is at least 7-transitive.
   - $c = (1,2,3)(4,5,6)(7,8)(9,10)(11,12)$ and $c^4 = (1,2,3)(4,5,6)$ which is a standard shape representative with support size less than n so $G = S_n$.

   No other shapes occur as all other shapes with support size 12 have the greatest common divisor of their cycles lengths greater than 1.

□

Chapter 9

Proving groups primitive using cycle shapes

Motivated by Lemma 7.14 and a result of Davenport and Smith [7] we turn our attention to whether we can prove a group primitive using information about the cycle structures of the elements of the group. Clearly where the actual generators are known in a concrete sense then it will be possible to reason about the action of the generators on specific elements of the set the group is acting on and show the group is primitive. We do not deal with this case here, instead we concentrate on the case where only the cycle decomposition of the group elements is known. This may seem like an unnecessary constraint but such a problem is real when considering polynomial factorisation.

We begin by considering the effects a prime length cycle has on the block structure that can occur.

Lemma 9.1. *Let G be a transitive permutation group of degree n and let $c = c_1c_2 \dots c_m \in G$ where the c_i are disjoint cycles. If c contains a cycle, c_j, of prime length p, then one of the following is true:*

1. *G is primitive.*

2. *The blocks of imprimitivity of G are of size greater than or equal to p and c_j has support drawn from a single block.*

3. *G has at least p blocks of imprimitivity.*

Proof. Clearly G can be primitive. We now assume that G is imprimitive and consider the way the p-cycle could act on the blocks. Now if the blocks have at least p elements, then the support of the p-cycle could be drawn from a single block and we are done. However, if the blocks have size smaller than p, then the p-cycle must act on the blocks by permuting them. For contradiction we assume that the support of the p-cycle has at least two elements drawn from the same block, B. Therefore there must be a smallest power,k, of the p-cycle such that $Bc_j^k = B$ equally $Bc_j^{2k} = B$ and we deduce that $Bc_j^{ak} = B$ for all a. Now p is prime so either $k = p$ or k is coprime to p. If $k = p$, then our assumption that the support of c_j contained more than one element of B is wrong. If k is coprime to p then ak will take every value between 1 and p and we conclude that the support of c_j is drawn from a single block. □

Now Lemma 9.1 may not seem overly powerful but the basic construction can be applied to cycles that are not of prime length and we now do this.

Lemma 9.2. *Let G be a transitive permutation group of degree n and let $c = c_1c_2 \dots c_m \in G$ where the c_i are disjoint cycles. If c contains a cycle, c_j, of length l, then one of the following is true:*

1. *G is primitive*

2. *The blocks of imprimitivity of G are of size greater than or equal to l and c_j has support drawn from a single block*

3. The support of c_j consists of $\frac{l}{d}$ elements drawn from each of d blocks.

Proof. Clearly G can be primitive. We now assume G is imprimitive and consider the way c_j could act on the blocks. If the block size is at least l then clearly the support of c_j can be drawn from a single block. Now let

$$c_j = (\alpha_1, \alpha_2, \ldots, \alpha_l)$$

and let B be the block containing α_1. Suppose that, $B, Bg, Bg^2, \ldots Bg^{r-1}$ are distinct, but that $(\alpha_1)g^r \in Bg^i$ for some $0 \leq i < r$. It follows that $(\alpha_1)g^r \in B$ else $(\alpha_1)g^{r-1} \in Bg^{i-1}$. Thus c_j acts on r blocks and the support of c_j contains precisely $\frac{l}{r}$ elements from each block. □

The real strength of Lemmas 9.2 and 9.1 is not when used on single cycles but by considering how each cycle may move a block. For motivation we consider g an element of a transitive group G of degree 30. First we consider the possible block sizes for the group they are $\{2, 3, 5, 6, 10, 15\}$, now if our chosen element has the following cycle structure $\{9, 7, 5, 5, 4\}$, then we can begin to eliminate possible block sizes. We start with the 7-cycle, either the group has at least 7 blocks or the blocks are at least size 7, this eliminates blocks of size 5 and 6 so the possible block sizes are $\{2, 3, 10, 15\}$. Now for blocks of size 10 and 15 we need cycles where the sizes of the supports sum to 3 and 8 respectively (as they must act on a single block) and we see this cannot occur leaving only blocks of sizes 2 and 3. Now the 7-cycle must act on 7 blocks moving them in a cycle, the only way the remainder of each block could be moved consistently would be if g contained another 7-cycle or a 14-cycle but neither of these is true and we conclude that G is primitive.

The above example shows the strength of prime length cycles whose length is co-prime to the degree of the group. They work in two ways the first is that for blocks larger than p to exist the element must have cycle(s) whose lengths sum to precisely the block size minus p. The second is that where they act on more than one block there must be enough elements in cycles of length divisible by p to cover a complete number of blocks. We now formalise this using the following result.

Theorem 9.3. *Let G be a transitive imprimitive permutation group of degree n with blocks of size b and let $c = c_1c_2 \dots c_m \in G$ where the c_i are disjoint cycles (possibly of length 1). If c contains a cycle,c_j, of prime length p, then either c contains cycles distinct from c_j whose lengths sum to $b - p$ or c contains one or more cycles distinct from c_j whose length is divisible by p whose total support is of size $p(b-1)$.*

Proof. Now if the support of c_j is drawn from a single block, B, then that block is stabilised by c. Now let c_k be disjoint from c_j but have support drawn from B. If the support of c_k is not drawn entirely from B, then there exists a power of c_k such that $Bc_k^l \neq B$ but B is stabilised by c so this is absurd. We conclude that any cycle with support drawn from B must have support a subset of B and it follows that c contains cycles whose lengths sum to $b - p$.

Now if the support of c_j is drawn from more than one block, then by Lemma 9.1 the support of c_j is drawn from precisely p blocks. Let B be one of these blocks then we may label the blocks by the power of c_j that maps B to it so $Bc_j^0 = B = B_0$, $Bc_j = B_1$, $Bc_j^2 = B_2$ and so on. Now let c_k be another cycle whose support includes an element from B. Now if c_k has support drawn from a block,B', other than one of B_i, then there exists a power of c_k such that $Bc_k^r = B'$

but $Bc_j^r = B_i$ but $B_i \neq B'$ which is absurd so the support of c_k is drawn from the B_i. Equally if c_k is of length l, then $Bc_k^l = B$ but $Bc_j^l = B$ only occurs when $p|l$ so as the B_i are blocks of G we conclude that $p|l$ and any cycle whose support is drawn from the B_i has length divisible by p. Finally we note that as each of the B_i are moved by c every element from each of the B_i must be involved in a non-trivial cycle and we are done. □

Previously we extended Lemma 9.1 to cover cycles of composite length. Clearly it would be useful to extend Theorem 9.3 to cover cycles of composite length as we are not guaranteed cycles of prime length exist. Where the support of a cycle is drawn from a single block the result transfers directly as we do not rely on the cycle being prime in our proof. Where the support is drawn from more than one block we know that it is drawn from $\frac{l}{d}$ blocks for some divisor d of l. Now the same argument as above applies with $\frac{l}{d}$ taking the same role as p and all of the cycles must have length divisible by $\frac{l}{d}$ and the total size of their support must be $l\left(\frac{b}{d}-1\right)$.

Corollary 9.4. *Let G be a transitive imprimitive permutation group of degree n with blocks of size b and let $c = c_1c_2\ldots c_m \in G$ where the c_i are disjoint cycles (possibly of length 1). If c contains a cycle,c_j, of length l, then either c contains cycles distinct from c_j whose lengths sum to $b-l$ or for some divisor,d, of l c contains one or more cycles distinct from c_j whose length is divisible by $\frac{l}{d}$ and whose total support is of size $l\left(\frac{b}{d}-1\right)$.*

We conclude by considering how these results may be used in practice. Even with these results it seems unlikely that we would be able to prove a group primitive based on a single element unless it contained a long prime cycle together with relatively few cycles of length 1. However, if one had information on the

cycle shapes of a number of group elements it becomes more likely that all block sizes will be eliminated. A possible iterative approach is outlined below:

Algorithm 9.1. *[Block elimination]*

1. *Let* $D = \{d_i | d_i$ *divides* $Degree(G)\}$.
2. *For each* $g \in G$ *remove from* D *those* d_i *that are incompatible with* g.
3. *If* $D = \emptyset$ *and* G *is transitive then* G *is primitive.*

Our constraint that we do not know the support of each cycle merely their shape means that we cannot carry information between group elements. If we did know the support of each cycle, then we would be able to specify the possible blocks and therefore could test if each element was consistent with a given set of blocks and not just a block structure by similar reasoning on how its support must act on blocks.

Chapter 10

Conclusion

We conclude this thesis by drawing together the main results from each section.

In the first part of the thesis we examined those elements in S_n that have trivially intersecting cyclic groups but which nonetheless satisfy a word of length shorter than their order the main result of this section is:

Theorem 10.1. *Suppose that $n \geq 8$, then there exist $g, h \in S_n$ with $\langle g \rangle \cap \langle h \rangle = id$, $o(g), o(h) > n$ and there is a word ω of length n on g and h with $\omega = 1$.*

We also used a family of Frobenius groups where nearly all elements were of prime order to show that there are groups where two prime power elements of order p have a shortest word also of length p. We also gave a bound on the proportion of elements in a group which can have prime order. These are summarised by the following two results:

Theorem 10.2. *Let p be a prime then there exists a group G and elements $g, h \in G$ both of order p such that the shortest positive word on g and h that is not of order p is of length p.*

Theorem 10.3. *Let G be a finite group and p a prime. If $|G| = p^n q$ and p and q are co-prime then the proportion of p-power elements is at most $(p^n - 1)/p^n$*

In the second part of the thesis we turned the problem on its head and looked at expressing elements of S_n and A_n as products of cycles of a given length. These results were largely known and are summarised via the following theorem:

Theorem 10.4. *For all $g \in A_n$ there exist x, y both l-cycles in A_n such that $g = xy$ if and only if l is odd and greater than or equal to l_{min} where:*

$$l_{min} = \begin{cases} \frac{3n}{4} & n \text{ divisible by } 4 \\ \frac{1}{4}(3n-3) & n-1 \text{ divisible by } 4 \\ \frac{1}{4}(3n-2) & n-2 \text{ divisible by } 4 \\ \frac{1}{4}(3n-1) & n-3 \text{ divisible by } 4 \end{cases}$$

However, in the course of the work we also prove the following result:

Theorem 10.5. *Let $n > 3$ be odd and let $g = (1, 2, \ldots, n)$ and let c be a standard shape representative in S_n then cg^{-2} is one of the following:*

1. *An n-cycle*
2. *An $n-1$-cycle*
3. *Two disjoint cycles whose combined support is of size n*

We also give specific conditions on when each of the above cases occur. Finally in the second part of the thesis we proved an interesting result regarding the element shapes that can arise from the product of two elements both of which have trivial stabilizer and are composed entirely of transpositions:

Theorem 10.6. *Let n be even and Ω be of size n, and let Π be the set of elements in S_Ω composed of precisely $n/2$ disjoint transpositions then only elements with*

an even number of each cycle shape may be expressed as a product of two elements of Π. *Moreover, for each transposition only one point will appear in each cycle.*

In the third part of the thesis we extended our arguments relating to expressing elements as products of a given shape to look at the groups generated by two elements of a given shape. In particular we looked at the groups generated by the n-cycle $(1, 2, \ldots, n)$ and a standard representative of each conjugacy class of S_n. The main result of this section is:

Theorem 10.7. *Let* $g = (1, 2, \ldots, n)$ *and let* c *be a standard shape representative in* S_n. *If the greatest common divisor of the cycle lengths of* c *is 1, then:*

$$G = \langle g, c \rangle = \begin{cases} \langle g \rangle & c = g \text{ or } c = id \\ A_n & n \text{ odd and } c \text{ an even element of } S_n \\ \text{Isomorphic to } S_5 & n = 6 \text{ and } c = (1,2)(3,4) \\ S_n & \text{otherwise} \end{cases}$$

Appendix A

Parker Vectors

A.1 Introduction

The Parker vector of a group was defined by Richard Parker and a detailed description can be found in [5] section 2.8. The Parker vector of a permutation group G of degree n is defined as $P = \{p_1, p_2, \ldots, p_n\}$ a sequence of numbers with each p_i representing the average number of points moved by i-cycles for elements of G. This vector is always composed of integer entries and the sum of these entries will always be n. Our interest in the Parker vector, like that of Parker himself, stems from an original interest of the author in looking at polynomial factorisation and it is with these calculations in mind that the work of this chapter is undertaken.

A.1.1 Parker vector for specific groups

The Parker vector for the symmetric group, S_n, is a sequence of 1's and, for $n \neq 6$, this is unique i.e. there is no other group with such a Parker vector. Similarly the Parker vector for the alternating group, A_n, is a sequence of $1's$ ending in either

$\{0,2\}$ or $\{2,0\}$ this is unique for all n. However, this unique mapping between groups and their Parker vector is not generally true and therefore except, in exceptional circumstances, it is not possible to identify a group using its Parker vector alone.

Extending this to Parker vectors for direct products of S_{m_i} we find that again the Parker vector will be of a specific type. Essentially the Parker vector for such a group will be the sum of the individual Parker vectors for each group. For example, the Parker vector for $S_3 \times S_4 \times S_2$ is $\{3,3,2,1,0,0,0,0,0\}$. Therefore, assuming we know a group is a product of S_{m_i} and we know the Parker vector for the group we can deduce the m_i' by repeatedly removing the largest group. In our previous example we could deduce the largest m_i was 4 contributing $\{1,1,1,1,0,0,0,0,0\}$ to the vector, subtracting this gives a residual vector of $\{2,2,1,0,0,0,0,0,0\}$. Repeating allows us to deduce the group also contains S_3 and then S_2 and we have a complete breakdown of the group. Of course, if our original assumption that the group is a direct product of S_{m_i} is incorrect then so is this analysis.

A.1.2 Polynomial factorisation

Let T be a square-free univariate polynomial over $\mathbb{Z}$. Now we consider T_p the reduction of T when considered as a polynomial over $\mathbb{Z}_p$ where p is a prime, and ignoring finitely many bad primes where p divides the leading coefficient. Now if we factorise T_p, in $\mathbb{Z}_p$, then the degrees of the irreducible factors are the cycle lengths of the Frobenius automorphism. Furthermore, as we have removed the bad primes the Frobenius automorphism lifts to an element of the Galois group G_T of T over $\mathbb{Z}$. Now if the lifting produces a random element of G_T for suitably

large primes then we can use this to calculate the Parker vector of G_T. In order to calculate the Parker vector of a group it suffices to know the cycle shapes of all the elements of the group. Thus, given sufficient time, it would be possible to calculate the Parker vector for G_T to any required degree of certainty.

In general the Galois group for an irreducible polynomial will be S_m where m is the degree of the polynomial. Where this is the case we can use the sampling and reduction technique outlined above to find this with relative ease, experimental work performed by Puttock [11] shows that, on average, this can be done using only 5 primes. Furthermore, by extending this to an arbitrary reducible polynomial its Galois group will, in general, be the direct product of finitely many S_{m_i} with $\sum S_{m_i} = n$, the degree of the polynomial, with each of the S_{m_i} being the Galois group for one of the irreducible factors.

Assuming the the Galois group of a given polynomial is the direct product of S_{m_i}'s and that it is possible to calculate the Parker vector of a group via repeated random sampling of the group then it would be possible to use the information derived from repeated factorisations modulo p to determine the degrees of all of the factors in the polynomial. Indeed, p_1 gives the number of factors in the polynomial. Algorithm A.1 gives a high level overview of the approach that would need to be taken to calculate the m_i's using repeated factorisation.

Algorithm A.1. *[Parker Factorisation]*

1. *Generate the Parker vector to required confidence retaining each factorisation*
2. *Find the longest factor and lift to a true factor, if this fails, then try another longest factor or search for more*
3. *Factorise the identified factor over each prime and remove from the data*

4. *Repeat the removal of largest factors on the remainder until all factors are removed*

Using the approach outlined in Algorithm A.1 is essentially a large scale data gathering exercise using a large numbers of factorisations and knowledge of the Parker vector's properties to determine when to stop gathering data. While such an approach would certainly remove the combinatorial explosion often associated with polynomial factorisation the cost associated with gathering sufficient data to ensure the largest factor were known to any degree of confidence may well be too great to be of practical interest.

A.2 Similarity of Parker vectors

We have already noted that the Parker vector for S_n is unique for $n \neq 6$. However, when considering convergence of Parker vectors it is useful to know how close to the Parker vector for S_n the Parker vector for an arbitrary transitive group can be. GAP contains a library of all transitive permutation groups whose degree is 23 or less. By enumerating the conjugacy classes of the group it is relatively fast to calculate the Parker vector for small groups. Table A.1 shows the number of zero entries in the Parker vector for all small transitive groups whose degree is between 8 and 23, excluding S_n and A_n.

Table A.1: Number of zeros in Parker vector for small transitive groups

n	Total number of groups	Number of zeros in Parker vector 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
8	48	1	5	12	14	15	1	0														
9	34	0	0	6	10	10	4	2	0													
10	43	0	3	8	8	11	11	2	0	0												
11	6	0	0	1	0	1	1	0	2	1	0											
12	299	0	0	8	13	33	114	94	35	2	0	0										
13	7	0	0	0	0	0	2	0	1	1	2	1	0									
14	61	0	0	2	6	4	7	11	12	7	9	3	0	0								
15	102	0	0	0	2	8	17	20	20	19	10	4	2	0	0							
16	1,952	0	0	0	3	7	4	15	63	178	165	316	970	230	1	0						
17	8	0	0	0	0	0	1	0	1	0	0	2	1	1	1	1	0					
18	981	0	0	0	2	6	9	17	17	33	132	219	320	134	91	1	0	0				
19	6	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	2	1	0			
20	1,115	0	0	0	0	3	6	2	14	37	110	124	89	188	344	160	35	3	0	0		
21	162	0	0	0	0	0	3	8	4	7	10	12	18	14	31	26	14	12	3	0	0	
22	57	0	0	0	0	2	6	1	2	1	3	1	4	3	5	5	9	5	8	2	0	0
23	5	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	2	1

Table A.1 shows that for larger n not only are no Parker vectors identical to those for S_n and A_n there is a significant difference between them. Davenport and Smith [7] have shown that if a transitive group contains a p-cycle with $\frac{n}{2} < p \leq n-3$, then the group is at least 4-transitive and hence, assuming it is not one of the four Mathieu groups which are more than 4 transitive, is either S_n or A_n. Therefore we can put a bound on the minimum number of non-zero entries the Parker vector of a transitive group may have by enumerating the number of primes, p, in the range $\frac{n}{2} < p \leq n-3$. Table A.2 extends Table A.1 to show the theoretical minimum number of zero entries in the Parker vector of transitive groups for various n.

Table A.2: Minimum zeros in Parker vector of transitive groups

n	Minimum zeros
25	3
30	3
50	6
100	10
150	13
200	20
500	41

Applying this for $8 \leq n \leq 23$ the theoretical bound is only achieved for $n = 8$ and for all other n the theoretical bound appears to be conservative. However, for larger n we have no evidence save for this bound and must assume this is the best we can do. Working out the above figures for all n between 10 and 1,000 gives the smallest number of zeros as 6.7% of n and the largest as 15% with the average being 8%. This bound only applies to transitive groups and therefore it is possible to find a Parker vector much closer to that of S_n for a non-transitive group, for example, the Parker vector for $S_{n-2} \times S_2$ only differs from that of S_n

in four places p_1, p_2, p_{n-1}, and p_n.

A.3 Convergence of Parker Vectors

To be of use in determining the factors of a polynomial the Parker vector would need to converge rapidly to its final version as without this convergence any algorithm would rapidly become less efficient than attempting to construct a factorisation from a small number of probes and lifting it to a final factorisation. In this section we discuss various methods for determining when a Parker vector is sufficiently determined to be of use in the factorisation of a polynomial.

A.3.1 Pointwise Method

The most simple method for determining whether a Parker vector has stablised is to look at each entry within the vector in turn and determine how far from being an integer the particular entry is and terminating the search when all entries are within a given tolerance, ignoring the test one the first probe as this will always be an integer.

When constructing such an algorithm certain practical questions arise the first such question is what is an acceptable level of tolerance, μ, to set on each entry in order to be reasonably confident that the vector returned is correct. In order to test the best level to set this a number of tests using S_n were performed. Table A.3 shows the effect of varying μ on mean convergence time for small n. In addition to the effect on convergence times μ affects the number of times the algorithm will terminate with incorrect results this is also shown.

Table A.3 shows that while for very small n a large tolerance leads to rapid convergence it also gives rise to an unacceptable number of errors. However, for

Table A.3: Sensitivity to μ for 1,000 tests

n	0.1		0.2		0.25		0.4	
	Mean	Fails	Mean	Fails	Mean	Fails	Mean	Fails
5	295	25	69	102	44	131	17	290
6	445	5	109	61	68	104	24	319
7	653	1	154	31	90	115	32	324
8	807	0	205	30	132	41	44	314
9	996	0	251	16	164	31	51	280
10	1,262	0	314	8	198	25	65	237
15	2,475	0	646	0	417	3	154	82
20	3,929	0	1,010	0	660	1	251	44
30	-	-	1,890	0	1,199	0	493	4

medium to large n the number of errors generated rapidly drops to zero with a massive gain in speed.

Table A.4 below shows the mean and upper / lower decile number of probes to reach convergence for S_n for various n using pointwise convergence and a minimum number of probes set at n and $\mu = 0.25$.

Table A.4: Convergence times for 1,000 tests using pointwise algorithm and $\mu = 0.25$

n	Lower decile	Mean	Upper decile
5	8	44	100
6	10	68	152
7	13	90	190
8	32	132	269
9	45	164	319
10	60	198	375
15	168	417	743
20	305	660	1,077
30	632	1,199	1,882
40	1,025	1,867	2,856

This shows that pointwise convergence is exceptionally slow for large n. In-

deed, the algorithm appears to have an average convergence time of about $3 \times n^{1.8}$ with the lower decile being $1.4 \times n^{1.8}$ and the upper decile being around $5 \times n^{1.8}$. This approach is therefore clearly far too computationally expensive to be of any practical benefit in calculating potential factorisations. Indeed the only practical advantage that the pointwise method has over any other is its equal applicability to all groups as it does not make any assumptions about the underlying group structures.

While it is not particularly computationally expensive to calculate the variance of each point as it is merely involves dividing the running total of cycles of each length found by the number of probes it is a computation that is almost certainly of little benefit when the number of test conducted is small. Indeed it is reasonable to assume that incorrect termination is most likely to occur where the number of probes prior to detecting convergence is small. For this reason it is almost certainly worth generating a significant amount of data before testing convergence. As discussed earlier the lower decile for n falls at roughly $1.4 \times n^{1.8}$, running the algorithm again with the convergence check only being run after $n^{1.8}$ probes gives the following results.

Table A.5: Convergence times for pointwise algorithm with late convergence test

n	Lower decile	Mean	Upper decile
10	64	202	382
15	168	414	718
20	304	644	1039
25	480	968	1,578
30	655	1,233	1,949

From Table A.5 we can see that the late convergence test has no appreciable effect on any of the convergence times. More surprisingly it does not materially

effect the number of incorrect results reported proving that while the cost is minimal it does not help eliminate errors as hoped for.

A.3.2 Probabilistic method

If one were to assume a priori that the probes were taken from a group that is the direct product of S_{m_i} as discussed in section A.1.1 then one ought to be able to use this knowledge to improve the convergence time.

Indeed, if the primary concern is not, as in section A.3.1, to determine the entire Parker vector but merely to identify the biggest S_{m_i} used in forming the group the algorithm ought to be much better than $O(n^{1.8})$. We discuss one such method below.

In order to improve the effectiveness of the algorithm we would need to develop a test for when the longest single cycle, and hence the largest S_{m_i}, has been found. For this a little knowledge about S_n is essential.

Cycle distribution in S_n

The distribution of cycles in S_n is critical in understanding how quickly any probabilistic algorithm will converge. Indeed the Parker vector itself tells us a little about the distribution of cycles within a group and most importantly within S_n. The Parker vector represents the average number of points moved by cycles of each length in elements of the group. Therefore, if p_i is the i^{th} entry in the Parker vector for a group G then the average number of i-cycles in elements of G is $\frac{p_i}{i}$. In general this does not helps us identify the probability of a random element of G containing an i-cycle and a more complicated formula is needed, see below. However, if $i > \frac{n}{2}$, then each element may only contain one i-cycle

therefore the average number of i-cycles and the probability of obtaining such an i-cycle are coincidental. Moreover, if an element contains such an i-cycle, then it cannot contain any other k-cycle with $k > \frac{n}{2}$. Therefore, if $i > \frac{n}{2}$, then the probability of finding a cycle longer than i in S_n is

$$\sum_{j=i+1}^{n} \frac{1}{j}$$

Indeed one can further extend this to calculate when sampling from S_n the probability that a k-cycle of any length will occur in an element.

In order to identify the number of elements, K, with at least one k-cycle we need to consider the following argument, based on standard inclusion/exclusion arguments. If we are trying to calculate elements with at least one k-cycle, then the logical starting point is to consider how many possible k-cycles can be generated from n elements and then how may ways the remaining $n-k$ elements can be formed into cycles. However, such an approach will overcount where the remaining ordering contains a k-cycle and these must be removed. Similarly, removing the overcounting of double k-cycles will undercount triple k-cycles which must be added back in and so on. We are left with the following equation:

$$K = \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor} (-1)^i \times K_i$$

With K_i being the number of elements in S_n which contain at least i k-cycles, given this sum we only need calculate each K_i. Such an element can be written in the form $k_1 k_2 \ldots k_i \times tail$ where each k_j is an independent k-cycle and the tail is any arrangement of the remaining $n - ik$ elements. k_1 can be chosen in $\binom{n}{k}$ ways, k_2 in $\binom{n-k}{k}$ ways and in general k_j can be chosen in $\binom{n-(j-1)k}{k}$ ways. Given

k elements these can be arranged in $k!$ ways. However, when considered as cycles, 1 in k of these arrangements will be equivalent so each contributes $(k-1)!$ to the product. The tail in all cases can be written in $(n-ik)!$ ways, although this tail may contain further k-cycles. Putting all of this together we get the following:

$$\begin{aligned} K_i &= (n-ik)! \times \prod_{j=1}^{i} \binom{n-(j-1)k}{k} \times (k-1)! \\ &= (n-ik)! \times \prod_{j=1}^{i} \frac{(n-(j-1)k)!(k-1)!}{(n-jk)!k!} \\ &= (n-ik)! \times \prod_{j=1}^{i} \frac{(n-(j-1)k)!}{(n-jk)!k} \end{aligned}$$

Expanding the product we find that consecutive numerators and denominators cancel out leaving only the first denominator and last numerator which simplifies to the following:

$$\begin{aligned} K_i &= (n-ik)! \times \frac{n!}{(n-ik)!k^i} \\ &= \frac{n!}{k^i} \end{aligned}$$

However, in this expansion we will have included all arrangements of the i k-cycles so have overcounted by $i!$ and the final answer is:

$$= \frac{n!}{i!k^i}$$

Therefore combining the formula for each K_i together we obtain the full expres-

sion of K

$$K = \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor} (-1)^{i+1} \frac{n!}{i!k^i}$$
$$= n! \sum_{i=1}^{\lfloor \frac{n}{k} \rfloor} \frac{(-1)^{i+1}}{i!k^i}$$

In practice the group under consideration will only be the symmetric group if the polynomial is irreducible otherwise it will usually be a direct product of symmetric groups so the above argument helps little. However, once the formula for a symmetric group is known we can readily extend this to direct products of symmetric groups as each is independent. Thus, if $G = S_n \times S_m$ and there are K_n elements of S_n which contain a k-cycle and K_m elements of S_m then we can calculate K_G the number of elements in G which contain a k-cycle. We know that if we pick any element where the contribution from S_n contains a k-cycle then we may choose any element from S_m and vice versa. However, using this approach we have overcounted those elements where both S_n and S_m contribute a k-cycle, the size of this overcounting will be $K_n K_m$. Therefore:

$$K_G = m!K_n + n!K_m - K_n K_m$$

Alternatively, we could have constructed this sum by considering the number of elements in S_n and S_m respectively which contain no k-cycles, call these $\overline{K}_n$ and $\overline{K}_m$ respectively. $\overline{K}_n$ is simply $n! - K_n$ and similarly $\overline{K}_m = m! - K_m$. Using this

argument $\overline{K}_G = \overline{K}_n\overline{K}_m$ and therefore

$$\begin{aligned}
K_G &= |G| - \overline{K}_G \\
&= n!m! - \overline{K}_n\overline{K}_m \\
&= n!m! - (n! - K_n)(m! - K_m) \\
&= m!K_n + n!K_m - K_nK_m
\end{aligned}$$

which is equivalent to that found above. However, if we were to wish to extend this further to arbitrary direct products of S_{m_i}'s then this approach is far more fruitful as the general equation is now:

$$\begin{aligned}
K_G &= \prod_{i=1}^{n} m_i! - \prod_{i=1}^{n} \overline{K}_{m_i} \\
&= \prod_{i=1}^{n} m_i! - \prod_{i=1}^{n} (m_i! - K_{m_i}) \\
&= \prod_{i=1}^{n} m_i! - \prod_{i=1}^{n} \left(m_i! - m_i! \sum_{j=1}^{\lfloor \frac{n}{k} \rfloor} \frac{(-1)^{j+1}}{j!k^j} \right) \\
&= \left(\prod_{i=1}^{n} m_i! \right) \left(1 - \prod_{i=1}^{n} \left(1 - \sum_{j=1}^{\lfloor \frac{n}{k} \rfloor} \frac{(-1)^{j+1}}{j!k^j} \right) \right) \\
&= |G| \left(1 - \prod_{i=1}^{n} \left(1 + \sum_{j=1}^{\lfloor \frac{n}{k} \rfloor} \frac{(-1)^{j}}{j!k^j} \right) \right) \\
&= |G| \left(1 - \prod_{i=1}^{n} \left(\sum_{j=0}^{\lfloor \frac{n}{k} \rfloor} \frac{(-1)^{j}}{j!k^j} \right) \right)
\end{aligned}$$

These sums are relatively quick to calculate and give us the full description in terms of cycle shapes for direct products of symmetric groups.

A.3.3 Implementation of a probabilistic approach

If one is prepared to assume that the group we are sampling from is a direct product of S_{m_i}'s then given sufficient sampling a cycle of length M will be found where M =Max(m_i). We need only determine when we are sufficiently certain that we would have found a cycle of length M' where $M' > M$. This leaves the question of given M what M' should be considered, the easiest assumption would be to consider $M' = M + 1$, in this case the probability that any given probe contains an $(M + 1)$-cycle is $\frac{1}{M+1}$ and therefore the probability of not having found an $(M + 1)$-cycle, if sampling from S_{M+1} after n probes is $\left(1 - \frac{1}{M+1}\right)^n$. While for small M this converges reasonably rapidly for larger M convergence is slow. For M as small as 20 it would take 48 probes in order to reach a confidence of only one in ten that the longest cycle had been found and nearer 150 probes would be required to reach a confidence of one in 1,000. While potentially far too expensive to be of practical use this is significantly better than the time taken for S_{20} to converge using the pointwise algorithm.

In the cycle decomposition c_j of every element of a group which is the direct product of S_{m_i}'s each c_j is solely contributed by one of the S_{m_i}'s. Therefore the only M' that we need to consider are those which can be formed by combining the lengths of c_j's. By doing this in most cases it will be possible to show that any putative $M' > M + 1$. However, this will clearly not be the case if one of the groups concerned is S_1 (for polynomials this would represent a linear factor), or two, or more, of the m_i sum to $M + 1$. Unfortunately, trying to work out all possible arrangements of the c_j's for a given cycle is likely to be computationally expensive. Indeed, this is analogous to the combinatorial explosion we were aiming to avoid by examining the Parker vector. However, as we are sampling

randomly from all group elements a proportion of the M-cycles will come from $S_{M'}$, if it exists. Unfortunately without further prior knowledge of a likely group structure it is hard to gain further structural information as gaining reliable distribution information on cycle shapes is likely to lead to similar convergence problems as the pointwise method which it is broadly analogous to.

We can build some improvements into the algorithm. If $M > \frac{n}{2}$ then the M-cycle must be taken from our putative $S_{M'}$ as we do not have sufficient points in the rest of the group for a different $S_{M'}$. Therefore at least where there is one large S_{m_i} and the smallest $m_i > 1$ then we will be able to greatly improve our convergence.

In order to test the effectiveness of the proposed algorithm tests of all possible products of S_{m_i}'s were performed and the results grouped together according to $n = \sum m_i$. Both the average number of probes required to reach convergence and the number of times the algorithm returned an incorrect M are shown, this increases with n, as the number of groups tested increases, the average gives the average number of incorrect results for each group. For each group 1,000 tests were performed in order to ensure stability in the results with the termination probability set to one in one thousand. In addition the same tests were performed using the pointwise convergence algorithm with $\mu = 0.25$ to compare the relative convergence times. The average fails listed in the table give the average number of times out of the 1,000 tests for each group that the algorithm returned an incorrect result.

From Table A.6 it is clear that the probabilistic algorithm offers vastly superior convergence times to the pointwise algorithm. However, it should be noted that the pointwise algorithm suffers in two ways in this comparison. The first is that it often returns an incorrect result due to too rapid convergence, the second

Table A.6: Convergence times for probabilistic and pointwise algorithms for direct products of S_{m_i}'s

n	Probabilistic			Pointwise		
	Average probes	Total fails	Average fails	Average probes	Total fails	Average fails
10	34	21	0.50	62	477	7.69
15	45	123	0.70	117	913	5.19
20	55	434	0.69	185	937	1.49
25	63	1,497	0.76	256	1,374	0.70

is that it will sometimes take an exceptionally long time to converge therefore lifting the mean convergence time considerably. Further investigation shows that where the pointwise algorithm returns incorrect results it is where the number of probes used is small. However, the average convergence time for the probabilistic algorithm appears to be at worst O(n) much faster than we could hope for with a pointwise test. In addition it appears that the probabilistic termination test is, as expected, conservative in its estimation of a convergence giving an incorrect result far less frequently than one in a thousand.

While there is little improvement to be had from either method there is potential for adoption of a hybrid method. Using the same groups as above it is possible to repeat the tests and gather data on when the Parker vector first converges to the correct value. Using this it should be possible to devise a test which has the generality of the pointwise algorithm but which terminates much more rapidly.

While there is little extra concrete information that can be gained from examining cycle shapes we can still hope to improve the algorithm further. Currently the algorithm does not look at the convergence of the remainder of the Parker vector. Unfortunately there may be very little to be gained from this approach

as in the limit this equates to performing a pointwise test, albeit on a limited number of points.

In addition we have discarded other information when forming the Parker vector namely the frequency with which i-cycles occur. The Parker vector captures some of the shape of the group but not all of it. If at the same time as one were constructing the Parker vector one constructs another vector based on the frequency with which i-cycles occur in a group irrespective of their multiplicity it may be possible to lever more information from the same inspection. For example, the probability vectors of $S_6 \times S_7$ and $S_5 \times S_8$ are

$$\{0.86, 0.63, 0.48, 0.44, 0.36, 0.31, 0.14, 0.00, 0.00, 0.00, 0.00, 0.00, 0.00\}$$

and

$$\{0.87, 0.62, 0.52, 0.41, 0.36, 0.17, 0.14, 0.13, 0.00, 0.00, 0.00, 0.00, 0.00\}$$

These two vectors differ in 6 places whereas the Parker vectors only differ in 2 places. It is not clear how practical it would be to observe these differences given their small size in all but two places.

Appendix B

Word reduction using element shapes

In this Appendix instead of looking at each element we instead consider the shape of an element and how this may reduce the number of words we need to test a given pair of elements in. In order to do this we must define a structure that captures the shape of an element. While it is possible to think of an element as a collection of cycles of given length we instead define the swirl of an element, in order to do this we must first define a swirl shape.

Definition B.1 (Swirl shape). For n a natural number a swirl shape is a multi-set $\{x_1, \ldots, x_n\}$ where $0 < x_i \leq n-1$ and $\sum x_i \equiv 0 \pmod{n}$

We now define the swirl of an element of S_n.

Definition B.2 (Swirl). Let $g \in S_n$. The Swirl of g, written $Swirl(g)$, is the swirl shape obtained by calculating the right shift of each of $\{1, \ldots, n\}$ under g.

The definition is best illustrated by an example. Let $g = (1,2,4,5,3) \in S_5$. Now the right shift of 1 is 1 whereas the right shift of 5 is 3 and the complete

swirl of g is $\{1,2,1,3,3\}$. Of course we have not yet shown that the multi-set of Definition B.2 is a swirl shape. First we note the the largest possible right shift is $n-1$ so the elements of the multi-set are drawn correctly. Next we observe that for each cycle in g the sum of the right shifts must be divisible by n as the right shifts lead back to the first element hence the multi-set is divisible by n. Thus we have shown that a swirl is a swirl shape.

Observe that for $g, h \in S_n$ the swirl of gh may be obtained from the swirls of g and h. To show how this may be done let us consider the image of $a \in \{1,\ldots,n\}$ under gh. Now the image of $(a)gh = ((a)g)h$ and considering this as a rotation it is the right shift of a under g followed by the right shift of $(a)g$ under h. So the right shift of a under gh is the sum modulo n of an element from $Swirl(g)$ and an element from $Swirl(h)$. Therefore, $Swirl(gh)$ is the pointwise addition of $Swirl(g)$, considered as an ordered set, and some ordering of $Swirl(h)$.

Next we observe that in our example the average of $Swirl(g)$ is 2, a whole number, which prompts the following definition.

Definition B.3 (Swirl number). The Swirl number of an element is the mean of the multi-set $Swirl(g)$.

Of course we have not yet shown that the the swirl number is always a whole number, and hence that the swirl of an element is in fact a swirl shape although we may do so.

Lemma B.1. *For $g \in S_n$ the swirl number of g is a whole number.*

Proof. We first observe that the swirl of a transposition is $\{k, n-k, 0, \ldots, 0\}$ and hence its swirl number is 1. Now any element of S_n may be expressed as a product of transpositions and we have already shown that the swirl of a product

of elements of S_n may be obtained by pointwise addition of some ordering of the swirls modulo n. Now as the swirl number of a transposition is a whole number the sum of its swirl is divisible by n. Therefore the pointwise addition of two swirls is divisible by n and as the addition can only remove multiples of n so the resulting swirl is still divisible by n and hence the swirl number is a whole number □

We know that $Swirl(gh)$ may be derived from $Swirl(g)$ and $Swirl(h)$. However, there appears to be no such relationship between the swirl numbers of elements. We can see this by considering $g = (1,2,3,4)$ and $h = (2,4,3)$ as elements of S_4 the swirl numbers of g and h are 1 and 2 respectively whereas the swirl number of gh is 1. Similarly, one may observe that the swirl number for $(1,2)^2$ is zero whereas the swirl of $(1,2)$ is 1.

B.1 Using swirls to find related elements

We now turn our attention to how we may use the swirl of an element to assist in determining whether two elements satisfy a given word. Now if g and h satisfy a word ω, then we know that the swirl of ω is $\{0,\ldots,0\}$ as no elements are moved. Furthermore, we have shown that $Swirl(gh)$ may be obtained from $Swirl(g)$ and $Swirl(h)$ by a picking an appropriate ordering of each swirl and then conducting a pointwise addition modulo n. Now we may use this to consider the possible swirls that may arise for a given word length and given g and h.

We first turn our attention to the practical consideration of how many swirls there are for a given n. Table B.1 gives both the number of swirls observed in practice both for all elements of S_n and for n-cycles.

We can see that for all but very small n the advantage of looking at swirls is

Table B.1: Number of swirls

	S_n		n-cycles	
n	Actual	Potential	Actual	Potential
3	4	4	2	2
4	10	10	3	5
5	26	26	8	12
6	80	80	20	38
7	246	246	66	114
8	810	810	229	381

a considerably reduced number of potential pairs. However, the naive approach to determining if two elements can satisfy a word of length l is of order $n!^l$ as each swirl may be arranged in up to $n!$ ways where it is a proper set. However, we know that we may fix g. Now if we choose $g = (1, 2, \ldots, n)$, then the swirl is $\{1, 1, \ldots, 1\}$ which has only one ordering and the problem is reduced to at most $n!^{l-k}$ where there are k g's in ω.

We consider the following two elements of S_6, $g = (1, 2, 3, 4, 5, 6)$ and $h = (1, 2, 5, 4, 6, 3)$, a simple calculation shows that their cyclic groups intersect trivially. Now, $Swirl(g) = \{1, 1, 1, 1, 1, 1\}$ and $Swirl(h) = \{1, 2, 3, 3, 4, 5\}$ and we know that in S_6 no 6-cycles whose cyclic groups intersect trivially satisfy the word g^3h^2gh, yet as Table B.2 shows the swirls may be arranged such that their sum is zero modulo 6.

B.2 Conclusion

We have shown that, while the number of swirls for n-cycles in S_n is considerably smaller than the number of n-cycles using them to eliminate pairs of elements is considerably more time consuming. Furthermore, we can see that we cannot

Table B.2: Swirl addition of $(1,2,3,4,5,6)$ and $(1,2,5,4,6,3)$

1	1	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
1	2	3	3	4	5
4	1	3	2	3	5
1	1	1	1	1	1
3	5	2	3	1	4

conclusively deduce that elements satisfy a given word shape.

However, we see that, at least for small n, the number of possible swirl shapes and the number observed as swirls of elements in S_n are the same which prompts the following.

Conjecture B.2. *For Sw a swirl shape on n there exists a $g \in S_n$ such that $Sw = Swirl(g)$*

We have not been able to prove Conjecture B.2. However, we have tested whether it is true, at least for small n which it is for $n \leq 12$.

Appendix C

Swirls

We have seen in Appendix B that the notion of the swirl of an element does not appear to help us significantly in determining if two elements are related by a word. However, as we can see from conjecture B.2 there are interesting results in their own right regarding swirls and we take a little time here to explore some of these.

We start by considering the swirls that may arise from a single transposition. As before we consider a swirl as a pattern of clockwise shifts when the elements of S_n are arranged in a circle. Now in a transposition all bar two elements remain fixed so there are only two non-zero elements in the swirl, the remaining two must sum to a multiple of n, indeed the sum must be n as the multiple of n denotes the number of of complete circuits performed under the action of the cycle. Indeed, this leads to the observation that the swirl number of an element gives an upper bound on the number of disjoint cycles.

Lemma C.1. *The Swirl shape of a transposition in* S_n *is* $\{m, n-m, 0, \ldots, 0\}$ *where* m *is an integer between 1 and* $n-1$

We now consider a cycle of length r. Again we know that $n-r$ entries in the

swirl are zero, as they are not moved by the cycle. Consider the way a swirl is formed from a permutation, each entry is the clockwise shift between adjacent, in the permutation, elements. Now for a cycle these must sum to a multiple of n, or our cycle would not be complete. Furthermore, the ordered multi-set of elements generated by a cycle must not have an interval sum equal to a multiple of n or the cycle would contain a "sub-cycle" as we would arrive back at the same element. However, simply because a given ordering of a swirl contains an interval sum equal to a multiple of n does not mean the swirl cannot arise from a single cycle. Consider the swirl $\{2,3,4,1,0\}$ from an element of S_5 now this has two interval sums equal to 5 yet is the swirl of $(1,4,3,5)$ as well as $(1,3)(4,5)$. It would appear that we simply require that there is an ordering of the swirl such that no interval sum is a multiple of n, indeed this is sufficient.

Lemma C.2. *The swirl shape of a cycle is a swirl such that there exists an ordering of the swirl such that no interval sum is equal to a multiple of n, all such swirls arise from a cycle in S_n*

Proof. We start by proving that the swirl of a cycle has the required form. Let g be the r-cycle $(a_1, a_2, \ldots, a_r)$ and let right shifts be $\{d_1, d_2, \ldots, d_r\}$. Now for contradiction, assume that some interval sum $\Sigma_{i=l}^{m} d_i = kn$, this would imply that $(a_l, \ldots, a_m)$ is a cycle which can only be true if $l = 1$ and $m = r$.

To show the converse we construct a cycle from the swirl. Order the swirl so that no interval sum is a multiple of n, now starting at 1 form the cycle by adding each element of the swirl in turn modulo n. We are assured that each successive element is unique by the fact that no interval sum is a multiple of n. □

C.1 Elements with a given swirl number

Having established the swirls for some basic elements we now turn our attention to the swirl number of elements. Colloquially the swirl number of an element encapsulates the number of complete circuits the element makes. We use this relaxed way of viewing the swirl number to prompt the following.

Theorem C.3. *For $t \in \{1 \ldots n-1\}$ there exists a multi-set, m, drawn from $\{1 \ldots n-1\}$ such that the sum of the multi-set is nt and no sub-multi-set of m has a sum divisible by n.*

Proof. We show this by constructing a multi-set with the given property. Consider the multi-set $\{t, \overbrace{n-1, \ldots, n-1}^{\text{t lots}}\}$ its sum is certainly nt we need only show that the sum of no multi-set is divisible by n. We know that $n-1$ and n are co-prime and hence no subset consisting of $n-1$ alone will be divisible by n. Similarly, if we choose r lots of $n-1$ and t, then the sum would be $rn + (t-r)$ which is only divisible by n if $t-r$ is divisible by n but as $r < t < n$ this is not possible and we are done. □

This allows us to deduce the following corollary:

Corollary C.4. *For every $t \in \{1 \ldots n-1\}$ there exists a $(t+1)$-cycle in S_n whose swirl number is t.*

Proof. Form the cycle by starting at one and adding each element of the irreducible multi-set of Theorem C.3 in turn. The result will be a cycle as no sub-multi-set is divisible by n and manifestly the swirl number is t. □

We may also observe that:

Corollary C.5. *The maximum swirl number for a $(t+1)$-cycle is t.*

Proof. The multi-set used in the proof of theorem C.3 is the smallest with sum equal to nt and gives a cycle of length $t+1$. □

Alternatively one may observe directly that the swirl number represents the number of complete circuits a cycle makes. No two adjacent elements may account for a complete circuit therefore the swirl number for a cycle must be less than the length of the cycle. Now Theorem C.3 shows that the limit is achievable in all cases.

C.2 Multi-swirls

We remind ourselves of the definition of a swirl of g, it is the swirl shape obtained by calculating the right shift of each of $\{1,\ldots,n\}$ under g. Embedded within this definition is the ordering of the elements we are calculating the right shift with reference too. However, in considering the proof of C.2 we rely on the ordering of the set we are calculating right shifts relative too. This prompts us to consider the effect of varying the order of the set. In order to do this we first need a definition.

Definition C.1 (Circular ordering). Let I be a set of size n, there are $(n-1)!$ ways of writing the elements of I clockwise around a circle. We call these the circular orderings of I.

So far we have only considered one circular ordering, that is the natural one starting with 1 and with the numbers ascending clockwise around the circle. To motivate ourselves further we consider the transposition $(1,12)$ in S_{12} now if we use the natural ordering, then the swirl is $\{11,1,0,\ldots,0\}$. However, if instead we use the order $\{1,2,4,6,8,10,12,3,5,7,9,11\}$, then the swirl is $\{6,6,0,\ldots,0\}$

a distinct swirl shape. Indeed, as a single permutation and the identity form a group this shows us that the sets of swirls arising from two isomorphic groups may be different depending on the circular ordering chosen.

However, if instead of considering only a single swirl for each element we look at the multi-set of swirls arising from an element when all circular orderings are considered we find some interesting results. First we formalise the language.

Definition C.2 (Multi-swirl). Let g be an element of S_n and let $I = \{1, \ldots, n\}$. The multi-swirl of g is the set of swirls arising from all circular orderings of I.

While the swirl of an element is not constant we can see that the multi-swirl is constant. Furthermore we may see the following interesting result.

Theorem C.6. *Conjugate elements have the same multi-swirl.*

Proof. Let g be an element of S_n and let $I = \{1, \ldots, n\}$, there are $(n-1)!$ circular orderings of I, let C be a circular ordering of I.

For a given C, the swirl of g is the multi-set of numbers $r(i)$ where $(i)g$ is r steps anticlockwise from i for $i \in I$.

Now suppose that $h \in S_n$ and C is a circular ordering, now we consider the swirl of g^h. So for each i in I we are interested in the number of steps from i to $(i)(h^{-1}gh)$ as i varies. Suppose that $i = (j)h$ then our interest is in the number of steps from $(j)h$ to $((j)h)h^{-1}gh = ((j)g)h$.

Now we start varying over all possible circular orderings thus removing the action of h above and we are done. □

Thus we know that if two elements are conjugate then they share the same multi-swirl. However, we have not shown that if two elements share the same multi-swirl that they are conjugate. We can show that a swirl does not uniquely

belong in a single multi-swirl. To see this consider the swirl $[0,1,2,3,4]$ this arises from $(1,2)(3,4)$ and $(1,2,3,4)$ which are in different conjugacy classes, indeed this is the only swirl of length 5 that appears in the multi-swirls of two conjugacy classes of S_5. For the more general answer we turn to look at C_3, now as C_3 is abelian each element is in a conjugacy class of size 1. Now the multi-swirl of $(1,2,3)$ is $\{[1,1,1],[2,2,2]\}$ similarly the multi-swirl of $(1,3,2)$ is $\{[1,1,1],[2,2,2]\}$, hence two non-conjugate elements have the same multi-swirl.

This leads us to consider when two swirls can be in the same multi-swirl. Firstly they must share the same number of zeros as they arise from conjugate elements. Similarly, we must be able to form the same number of sub-swirls with the same size from each swirl. However, this is not sufficient, we consider the swirls $[1,3,2,2]$ and $[2,2,2,2]$ arising in S_4, the first only arises as the result of a 4-cycle whereas the second only arises from the product of two transpositions yet neither has any zeros and both have two potential sub-swirls of size 2.

We have shown that conjugate elements have the same multi-swirl. However we can show that conjugate elements need not share the same swirl number as the swirl number is not constant as C varies. To see this consider $(1,2,3)$ and $(1,3,2)$ with $C=\{1,2,3\}$ they have swirl number 1 and 2 respectively whereas with $C=\{1,3,2\}$ the situation is reversed.

We now consider what other information may be contained in the multi-swirl. Certainly, the multi-swirl does not encapsulate the size of the conjugacy class. To see this we consider two conjugacy classes in S_6 namely those containing $(1,2,3)$ and $(1,2,3)(4,5,6)$, now both conjugacy classes have size 40 yet the multi-swirl of $(1,2,3)$ has 6 elements while that of $(1,2,3)(4,5,6)$ has 9.

We may also see that the multi-swirls arising from a group depend on the representation chosen. So far we have considered natural representations of groups,

let us now consider two representations of C_6 namely $G = \langle g = (1,2,3,4,5,6)\rangle$ and $H = \langle h = (1,2,3)(4,5)\rangle$. Trivially the swirls arising from G are multi-sets of size 6 while those from H are of size 5. This should not cause us concern provided the sizes of the multi-swirls correspond. However, table C.1 shows this not to be the case.

Table C.1: Sizes of multi-swirls

G		H	
Element	Size	Element	Size
id	1	id	1
g	20	h	4
g^2	9	h^2	4
g^3	5	h^3	2
g^4	9	h^4	4
g^5	20	h^5	4

Indeed, as well as showing that the sizes of multi-swirls are not constant across representations of a group table C.1 shows us that the relativities of sizes are not preserved with H giving rise to only 3 distinct sizes of multi-swirl and G giving rise to 4. It is clear that we must specify the particular representation of the group under consideration, unless otherwise stated we will use the most natural.

C.3 Swirls in C_p

While we are still not in position to prove Conjecture B.2 we start by considering the swirls that arise from the cyclic groups of prime order.

We start by considering the set of swirls that arise from C_p for p prime. Now $g = (1,2,\ldots,p)$ generates C_p. Now the image of i under g^n is $i+n \mod p$, from this we can see that the swirl arising from g^n is $\{n,\ldots,n\}$.

Lemma C.7. *All swirls of the form* $\{i, i, \ldots, i\}$ *for all* $1 \leq i < p$ *arise naturally from* C_p

We now turn our attention to the multi-swirls arising from C_p. We start by considering the multi-swirl of g, as defined above. First we deduce that the multi-swirl of g may only contain swirls for which there exists an ordering such that no interval sum of the swirl is a multiple of p as if no such ordering exists, then the swirl may only represent an element composed of more than one cycle. Furthermore, we know that no element may be zero as this would give rise to a cycle of length less than p. We now turn our attention to proving that this is a sufficient condition, we do this by giving the circular ordering required to generate the swirl. Starting with 1 we add each element of the swirl in order modulo p, now we are assured we never land on the same element as no interval sum is divisible by p. Moreover, as there are p elements in the swirl we exhaust all possibilities and we have found a circular ordering that gives rise to the swirl.

Theorem C.8. *The multi-swirl for* $(1, 2, \ldots, p)$ *consists of all swirls with only non-zero entries for which there is an ordering with no interval sum divisible by* p.

We now look to C_p in general. Now every element of C_p is a p-cycle and the argument for g above holds we need only prove that a circular ordering exists. We do this by generalising the argument used above, again we start at 1 and mark the $p - 1$ positions on the circle and step round the circle by the number of steps given by the swirl element and record that element of the cycle, we are assured that we never land on the same point as no interval sum is divisible by p.

Theorem C.9. *The multi-swirl for* $h \in C_p$ *for* $h \neq id$ *consists of all swirls with*

only non-zero entries for which there is an ordering with no interval sum divisible by p.

This gives rise to the following obvious corollary.

Corollary C.10. *All non-trivial elements of C_p have the same multi-swirl.*

It is worth noting that although the elements of C_p are not conjugate within C_p they are conjugate within S_p. In examining our proof of theorem C.6 we see that while our proof relies on elements of S_n the result will hold equally in any group provided the elements are conjugate in S_n.

Bibliography

[1] E. Bertram. Even permutations as a product of two conjugate cycles. *J. Combinatorial Theory Ser. A*, 12:368–380, 1972.

[2] E. A. Bertram and V. K. Wei. Decomposing a permutation into two large cycles: an enumeration. *SIAM J. Algebraic Discrete Methods*, 1(4):450–461, 1980.

[3] G. Boccara. Décompositions d'une permutation d'un ensemble fini en produit de deux cycles. *Discrete Math.*, 23(3):189–205, 1978.

[4] P. J. Cameron. Some multiply transitive permutation groups. In *Coding theory, design theory, group theory (Burlington, VT, 1990)*, Wiley-Intersci. Publ., pages 1–11. Wiley, New York, 1993.

[5] P. J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[6] L. Cangelmi. Factorizations of an n-cycle into two n-cycles. *European J. Combin.*, 24(7):849–853, 2003.

[7] J. H. Davenport and G. C. Smith. Fast recognition of alternating and symmetric Galois groups. *J. Pure Appl. Algebra*, 153(1):17–25, 2000.

[8] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004. (`http://www.gap-system.org`).

[9] M. Hall, Jr. *The theory of groups.* The Macmillan Co., New York, 1959.

[10] O. Ore. Some remarks on commutators. *Proc. Amer. Math. Soc.*, 2:307–314, 1951.

[11] R. Puttock. Computations in group theory. Master's thesis, University of Bath, 1996.

[12] J. J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, fourth edition, 1995.

[13] J. Singer. A theorem in finite projective geometry and some applications to number theorey. *Trans. Amer. Math. Soc.*, 43:377–385, 1938.

[14] R. P. Stanley. Factorization of permutations into n-cycles. *Discrete Math.*, 37(2-3):255–262, 1981.

[15] D. W. Walkup. How many ways can a permutation be factored into two n-cycles? *Discrete Math.*, 28(3):315–319, 1979.

[16] H. Wielandt. *Finite permutation groups.* Academic Press, New York, 1964.