DISSERTATION

THE MÖBIUS NUMBER OF THE SYMMETRIC GROUP

Submitted by

Kenneth M Monks

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Summer 2012

Doctoral Committee:

Advisor: Alexander Hulpke

Tim Penttila
Jeff Achter
Walter Toki

ABSTRACT

THE MÖBIUS NUMBER OF THE SYMMETRIC GROUP

The Möbius number of a finite group is its most important nontrivial combinatorial invariant. In this paper, we compute the Möbius numbers of many partially-ordered sets, including the odd-partition posets and the subgroup lattices of many infinite familes of groups. This is done with an eye towards computing the Möbius number of the symmetric group on 18 points.

TABLE OF CONTENTS

Chapter 1

Preface

This work is primarily a result of my advisor's excellent graduate combinatorics class. I came into graduate school like many graduate students, studying math but not knowing what area appealed most to me. Alexander Hulpke's combinatorics class quickly showed me that discrete math was my favorite area, and in particular his inspiring lecture on Möbius numbers led me to ask if he had any research projects involving these mysterious invariants! Five years of research later, here is the work I have done. I could not have asked for a better advisor and am extremely grateful for all the time he devoted to me.

Beyond my advisor, I owe a huge thanks to the wonderful support group I have had over the years. My family was incredibly helpful getting me a head start on my education as a child and through my undergraduate education. Upon entering graduate school, my coadvisor Tim Penttila became a very inspiring and valuable mentor. Robert Liebler and the fellow attendees of the seminar he created, the Rocky Mountain Algebraic Combinatorics Seminar, also provided much support and guidance throughout my research. Lastly, a large thanks goes out to the very friendly community of graduate students I had, always there as resources, sounding boards, and friends.

Chapter 2

Background

2.1 Posets and Lattices

As the Möbius number is a combinatorial invariant of a lattice, we begin by defining a lattice, and a more general structure, a poset.

Let $\leq$ be a binary relation on a set P. We say $\leq$ is a ***partial-ordering*** on P if and only if it satisfies the following properties:

reflexive: $\forall x \in P, x \leq x$

transitive: $\forall x, y, z \in P, (x \leq y \text{ and } y \leq z) \Rightarrow x \leq z$

antisymmetric: $\forall x, y \in P, (x \leq y \text{ and } y \leq x) \Rightarrow x = y$

A ***poset*** $(P, \leq)$ is a set P with a partial-ordering $\leq$. If P is a finite set, we say $(P, \leq)$ is a ***finite poset***. In this thesis, all posets will be finite. If the ordering $\leq$ is clear, then the poset $(P, \leq)$ is typically abbreviated as P. If $x \leq y$ but $x \neq y$, we write $x < y$.

An ***interval*** in a poset P, written $[x, y]$, is the set of all elements in P between x and y. That is, $[x, y] = \{z \in P : x \leq z \leq y\}$.

Suppose $x, y, z \in P$ satisfy the following three properties:

(i) $x \leq z$

(ii) $y \leq z$

(iii) $\forall w \in P, (x \leq w \text{ and } y \leq w) \Rightarrow z \leq w$

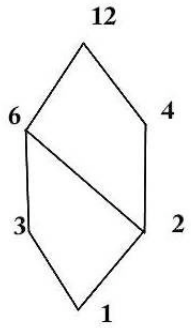
In this case we say z is the **least upper bound** or **join** of x and y, written $z = x \vee y$. That is, z is the smallest element that is greater than or equal to both x and y. Similarly we can define the **greatest lower bound** or **meet** of x and y, written $z = x \wedge y$, as the largest element that is less than or equal to both x and y.

If P is a poset where every pair of elements has a unique least upper bound and a unique greatest lower bound, we say P is a **lattice**. Since we are only concerned with finite posets, for our purposes every lattice L has a unique maximum element, written 1_L, and a unique minimum element, written 0_L. These elements are obtained by taking $x_1 \vee x_2 \vee \cdots \vee x_n = 1_L$ and $x_1 \wedge x_2 \wedge \cdots \wedge x_n = 0_L$, where $L = \{x_1, x_2, \ldots, x_n\}$.

Typically a lattice is visualized via a **Hasse diagram**, a graph with one vertex for each element of the lattice and one edge drawn for each maximal inclusion. It is always drawn such that y is higher than x if $x \leq y$.

If x, y are elements of a lattice P with $x \wedge y = \widehat{0}_P$ and $x \vee y = \widehat{1}_P$, we say that x is a **complement** of y, or x **complements** y.

For example, we can consider the lattice of divisors of 12 where the ordering is given by divisibility. Here the meet of two elements is their greatest common divisor an the join of two elements is their least common multiple. That is, $x \leq y$ if and only if $x|y$. We draw the corresponding Hasse diagram below. In this lattice, 3 is a complement for 4 but not for 6. In fact, 6 has no complement.



We say that x is a **modular element** of a lattice if no two complements of x are comparable. For example, in the lattice above, every element is modular.

2.2 The Principle of Inclusion-Exclusion

Möbius numbers can be seen as a generalization of the Principle of Inclusion-Exclusion. We state the Principle of Inclusion-Exclusion and notice a key property which will then be generalized to create the definition of Möbius numbers.

Consider subsets $A_1, A_2, \ldots, A_n$ of some set A. The Principle of Inclusion-Exclusion says that the size of $A_1 \cup A_2 \cup \cdots \cup A_n$ can be obtained if one knows the sizes of intersections of an arbitrary number of the A_i. Specifically,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \cdots$$

$$+(-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

where all indices are chosen from $\{1, 2, \ldots, n\}$. We can view this as a lattice $(L, \leq)$ on the set of all intersections of the A_i along with their union where the ordering relation is subset.

Notice that intersections of subsets are alternately counted with the coefficient +1 or -1 in order to not over- or under-count any element and the notion of how many times you have counted an element comes entirely from the structure of the inclusion of subsets in other sets. One can see that the sum of the coefficients over any interval in this lattice must be zero in order to count each element exactly once. This concept can be generalized to any finite lattice; this is how we define the Möbius function.

2.3 Defining Möbius Numbers

Definition 1 *Let L be a finite lattice. Then the* **Möbius function** *of L is $\mu : L \times L \to \mathbb{Z}$ and is recursively defined as follows:*

$$\sum_{z \in [x,y]} \mu(x, z) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases} .$$

Notice that this is a perfectly well-posed definition: the base case is given by intervals of size 1. Identify ordered pairs of elements of L with intervals in L in the natural way. Then for

any interval $[x, y]$ of size $n > 1$ we can assume we know the Möbius number for any interval of size less than n and use the definition to get

$$\mu(x, y) = -\sum_{z \in [x,y], z \neq y} \mu(x, z)$$

since any such $[x, z]$ will have at most $n - 1$ elements.

Recall that every finite lattice L has a minimum and maximum element, respectively just the meet of all elements and the join of all elements. Call these elements 0 and 1.

Definition 2 *Let L be a finite lattice. The* **Möbius Number** *of L is written $\mu(L)$ and is defined as $\mu(L) = \mu(0, 1)$.*

Notice that if L_n is the lattice of divisors of a positive integer n, then $\mu(n) = \mu(L_n)$ where $\mu(n)$ is the classical number-theoretic Möbius function given by:

$$\mu(n) = \begin{cases} -1 & \text{if } n \text{ is square-free and } r \text{ is odd} \\ 0 & \text{if } n \text{ is not square-free} \\ 1 & \text{if } n \text{ is square-free and } r \text{ is even} \end{cases}$$

where r is the number of distinct prime factors of n. Thus this definition generalizes the classical number-theoretic Möbius function, hence the name.

Additionally, as mentioned before, the coefficients of 1 and -1 that appear in the formula for Principle of Inclusion-Exclusion are simply the Möbius numbers in the poset of intersections of sets, ordered by containment.

2.4 The Möbius Number of a Group

Given any finite group G, we get a corresponding lattice of subgroups. The elements of the lattice of subgroups are simply all subgroups of G. The meet of two subgroups is their intersection and the join of two subgroups is the subgroup generated by them.

Definition 3 *Let G be a finite group. The lattice of subgroups of G is written $\mathcal{L}(G)$. The* **Möbius number** *of G is written $\mu(G)$ and is defined as $\mu(G) = \mu(\mathcal{L}(G))$.*

Notice that if G is isomorphic to the cyclic group C_k then $\mu(G) = \mu(k)$ since the subgroups of G will correspond exactly to the divisors of k with the same inclusion.

2.5 The Thesis Question

This brings us to the fundamental question of the thesis: What is the Möbius number of S_n, the symmetric group of degree n?

The motivation for this comes from the fact that the Möbius number is a very useful combinatorial invariant of a lattice. The Principle of Inclusion/Exclusion, the formula for the inverse for the Riemann-Zeta function, and the Euler characteristic of a simplicial complex are examples of uses of Möbius numbers in combinatorics, number theory, and topology (see for example section 3.8.8 in [20]).

In group theory, Möbius numbers were first used by Philip Hall [7] to count epimorphisms. As the full symmetry group of a set, the symmetric groups are a natural class of groups for which to seek the Möbius numbers. Additionally, every finite group embeds as a subgroup of some symmetric group via its regular representation. Thus $\mu(S_n)$ really involves the subgroup lattice of every permutation group of degree n and thus ultimately every group of order n. Therefore this is really a question about all finite groups and trying to understand not only the subgroup lattice of the symmetric group but the subgroup lattices of all groups.

Viewed in this light, there is a particularly interesting aspect of this problem due to a theorem in [11].

Theorem 4 *The Möbius number of a group is always divisible by the order of its derived subgroup.*

In the case of the symmetric group of degree n, we have that the derived subgroup is the alternating group of degree n, which has order $n!/2$. Thus even though the subgroup lattice of every group appears in the subgroup lattice of the symmetric group, somehow the Möbius numbers of the symmetric groups cannot just be wild or random; it must always somehow nicely work out to be a multiple of $n!/2$. Using the techniques in this paper, we hope to explain this enigma in more cases.

2.6 Prior Work

As stated above, given any group G, the set of subgroups ordered by inclusion forms a lattice, $\mathcal{L}(G)$. Trying to find the Möbius function of the subgroup lattice of S_n has proven to be a very challenging task. For small n one can simply construct the entire subgroup lattice of S_n and compute the Möbius number in GAP. The values of $\mu(S_n)$ for $n \in \{2, 3, \ldots, 8\}$ are:

n	2	3	4	5	6	7	8
$\mu(S_n)$	$-\frac{2!}{2}$	$\frac{3!}{2}$	$-\frac{4!}{2}$	$\frac{5!}{2}$	$-6!$	$\frac{7!}{2}$	$-\frac{8!}{2}$

Also, if $n \geq 3$, $|Aut(S_n)| = n!$ for $n \neq 6$ and $|Aut(S_6)| = 2 \cdot 6!$. Thus, Stanley [20, Page 191] asked if $\mu(S_n) = (-1)^{n-1} |Aut(S_n)|/2$ for all $n \geq 3$. This question has been answered in the negative [19].

While brute force computation works fine for small n, this approach quickly fails. For example for n only equal to 12, there are over 10.5×10^9 subgroups across more than ten thousand conjugacy classes! (It should be noted that from this point on in the paper, whenever we refer to numbers of subgroups we always mean numbers of conjugacy classes of subgroups; information gathered for one member of a conjugacy class is easily transferred to all other members.) Thus more theory must be brought to the problem. Using more general techniques, the value of $\mu(S_n)$ has been computed for three infinite families, namely n prime, n twice a prime, or n a power of 2.

Theorem 5 *[19] Let n be a prime or a power of two. Then*

$$\mu(S_n) = (-1)^{n-1} \frac{n!}{2}.$$

It should be noted that the case where n is prime was worked out in [13] as well using very different techniques.

Thus these two families agree with the formula presented in Stanley's question. However, this is not the case with the third family (for example $n = 14$ is a counterexample).

Theorem 6 *[19] Let $n = 2p$ where p is an odd prime. Then*

$$\mu(S_n) = \begin{cases} -n! & \text{if } n-1 \text{ is prime and } p \equiv 3 \pmod 4 \\ \frac{n!}{2} & \text{if } n = 22 \\ -\frac{n!}{2} & \text{otherwise} \end{cases}.$$

Additionally, the author has computed $\mu(S_{12}) = -12!$, which is the smallest counterexample to Stanley's question [12].

Shareshian's proofs in [19] primarily used a closure operation (see Subsection 3.1) that reduced the problem of finding the Möbius number of S_n to finding out certain information about the transitive permutation groups on n points. When n is prime, twice a prime, or a power of two, the transitive subgroups of S_n are relatively easy to describe. For example if n is prime then the only transitive groups are in fact the **primitive groups** on n points, by definition permutation groups that do not preserve any nontrivial partition of $\{1, 2, \ldots, n\}$. If a transitive group does preserve a nontrivial partition it is called **imprimitive**. Primitive permutation groups have been described in detail in the O'Nan-Scott Theorem [6] which is also heavily used in his proof. However, these techniques are unlikely to extend successfully to other infinite families. For example, up to conjugacy, S_{18} has 983 transitive subgroups, but only four are primitive. Thus the number of transitive subgroups quickly explodes for other values of n that allow more imprimitive groups. See Section 4 for our approach on how to get around this explosion of imprimitive groups.

Chapter 3

Combinatorial Tools

In this section, we state two very useful theorems for computing Möbius numbers proved in [5].

3.1 Closure Operations

In this subsection, we examine a certain type of structure-preserving map from a poset to itself. Suppose we have a map from P to P, written as $\overline{\cdot}$, satisfying the following three properties for all $x, y \in P$:

$$(i)\ \ x \leq \overline{x}$$

$$(ii)\ \ \overline{x} = \overline{\overline{x}}$$

$$(iii)\ \ x \leq y \Rightarrow \overline{x} \leq \overline{y}$$

Such a map is called a **closure operator**. If $x \in P$ has $\overline{x} = x$, we say that x is **closed**. Given a closure operator, we can take the subposet consisting of only the closed elements of P, which we call the **quotient poset** $\overline{P}$. This name is used because $\overline{P} \cong P/\sim$ where $\sim$ is the equivalence relation given by $x \sim y \Leftrightarrow \overline{x} = \overline{y}$.

Usually computing a Möbius number from the definition involves far too many terms in the recursion; applying closure operations greatly reduces this. The following theorem is often referred to as Crapo's Closure Theorem.

Lemma 7 *[5] Let $\bar{\cdot}$ be a closure operator on P and $x, y \in P$. Let $\mathcal{S} = \{z \in P : \overline{z} = \overline{y}\}$. Then*

$$\sum_{z \in \mathcal{S}} \mu_P(x, z) = \begin{cases} \mu_{\overline{P}}(\overline{x}, \overline{y}) & \text{if } x = \overline{x} \\ 0 & \text{if } x < \overline{x} \end{cases}.$$

Notice that the more closed elements we have, the more complicated the quotient poset is, but the fewer terms there will be in the sum. Conversely, if we don't have many closed elements, we'll have a small quotient poset but have many more terms in the sum. Thus in picking a closure operation we have a trade-off between the sum being more complicated and the quotient poset being more complicated. We will revisit this trade-off in Section 4.

3.2 Crapo's Complement Theorem

Theorem 8, often referred to as Crapo's Complement Theorem [5], is a very powerful tool in obtaining the Möbius number of a lattice.

Theorem 8 *[5] Let L be a lattice with minimum element 0 and maximum element 1. Define ζ on $L \times L$ as the characteristic function of the relation $\leq$. Let $x \in L$ and let $x^{\perp}$ be the set of complements to x in L. Then*

$$\mu(L) = \sum_{y,z \in x^{\perp}} \mu(0, y)\zeta(y, z)\mu(z, 1).$$

In particular, if there exists $x \in L$ such that x has no complement in L, then $\mu(L) = 0$.

3.3 Normal Subgroups are Modular in the Subgroup Lattice

Notice also that if H and K are subgroups of G then H is a complement for K in the lattice of subgroups of G if and only if $H \cap K$ is the trivial group and $< H, K >= G$. The following simple but useful lemma shows why typically in applying Crapo's Complement Theorem (Theorem 8) we want to look at complements to a normal subgroup.

Lemma 9 *Let $H \lhd G$. Let K_1 and K_2 be two different complements to H in G. Then $K_1 \not\leq K_2$.*

Proof. By the Second Isomorphism Theorem, any complement to H must be isomorphic to G/H. In particular, $|K_1| = |G/H| = |K_2|$. Thus if K_1 and K_2 are distinct they are not comparable since if one was a subgroup of the other, they would be equal. ■

Equivalently rephrased in lattice-theoretic terms, a normal subgroup is always a modular element of the subgroup lattice. Thus when using a normal subgroup, we get a much simpler form of the Complement Theorem.

Corollary 10 *Let $H \lhd G$. Then*

$$\mu(G) = \sum_{K \in H^{\perp}} \mu(K)\mu(K, G).$$

We show one more important application of the complement theorem. This will become useful in Section 7.

Lemma 11 *[19] Let $H \leq S_n$ and $H \not\leq A_n$ where H does not contain an odd involution. Then $\mu(H) = 0$.*

Proof. We show that the proper subgroup $H \cap A_n$ of H has no complement in $\mathcal{L}(H)$ and then apply Crapo's Complement Theorem.

Assume K complements $H \cap A_n$. That is, $K(H \cap A_n) = H$ and $K \cap (H \cap A_n) = \{()\}$. Since $K(H \cap A_n) = H \not\leq A_n$, and $H \cap A_n$ contains only even elements, K must contain some odd element k. Since k is an odd element in H, k cannot be an involution, so $k^2 \neq ()$. Thus $\langle k^2 \rangle$ is a nontrivial subgroup contained in $K \cap (H \cap A_n)$, which is a contradiction.

Thus $H \cap A_n$ does not have a complement in $\mathcal{L}(H)$, so $\mu(H) = 0$. ■

Chapter 4

2-Closures

4.1 Choosing a Closure Operation

As stated above, there is a trade-off in choosing what closure operation to use when applying Crapo's Closure Theorem (Theorem 7) to a lattice L. Applying a closure operation that has many closed elements means that few get sent to the maximum element of L. In this case the quotient lattice $\overline{L}$ is large, but the sum in Theorem 7 has few terms. The extreme case of this is if we take the trivial closure operation that maps every element of a lattice to itself. In this case the Closure Theorem simply tells us that $\mu(L) = \mu(L)$. In the other extreme, we could take the closure operation that maps every element of L to the maximum element of L. Then we just get back the defining recursion of the Möbius function: $\sum_{x \in L} \mu(0, x) = 0$.

In [19], the closure operation primarily used is closure on orbits. That is, define the closure operation $\bar{\cdot}$ on $\mathcal{L}(S_n)$ for any $G \leq S_n$ by $\overline{G} = S(\mathcal{O}_1) \times S(\mathcal{O}_2) \times ... \times S(\mathcal{O}_m)$ where $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_m$ are the orbits of G and $S(\mathcal{O}_i)$ is the symmetric group on $\mathcal{O}_i$. Following Wielandt [21], we call this group the **1-closure** of G (the naming is fortunate -what he calls the 1-closure is actually a closure operation on the lattice). With such a closure operation, the closed subgroups are all direct products of symmetric groups. These correspond bijectively to the set of partitions of $\{1, 2, \ldots, n\}$. Thus the quotient lattice is isomorphic to the lattice of partitions of a set with n elements. The Möbius number of this lattice is easily worked out to be $(-1)^{n-1}(n-1)$ using induction and the Complement Theorem, for example see [20, Example 3.10.4] or [12]. The groups that get sent to S_n under this closure

operation are by definition the transitive subgroups of S_n, since they only and only they have one orbit on n points. Thus

$$\sum_{\substack{G \leq S_n \\ G \text{ transitive}}} \mu(G) = (-1)^{n-1}(n-1)!. \tag{4.1}$$

Thus on the closure operation trade-off, Shareshian [19] used a closure operation that was very heavily weighted to one side: the Möbius number of the quotient lattice was extremely easy to compute, however for arbitrary degrees (other than the families in Theorems 5 and 6) there will be an enormous number of transitive groups (see Theorem 14) and thus many terms in the sum. Our goal is to pick a new closure operation where the sum has fewer terms in exchange for the quotient lattice being more complicated but still tractable.

4.2 The 2-Closure of a Group

Given any group G acting on $\{1, 2, \ldots, n\}$, we can define a new action of G on the set of pairs of distinct points from $\{1, 2, \ldots, n\}$ by defining $[a, b]^g = [a^g, b^g]$ for $a, b \in \{1, 2, \ldots, n\}$ and $g \in G$. We call this the **action on pairs**. If a group has just a single orbit on pairs of distinct points, it is called **2-transitive**.

One can then define (again following Wielandt [21]) the **2-closure** of $G \leq S_n$ to be the largest subgroup of S_n having the same orbits on pairs as G. We write $2\text{cl}(G)$ for this largest subgroup. This is easily seen to be a closure operation on the lattice of subgroups of a group. Clearly $G \leq 2\text{cl}(G)$ and $2\text{cl}(G) = 2\text{cl}(2\text{cl}(G))$. Additionally it preserves incidence, since if $G \leq H$, the orbits of G on pairs are a refinement of the orbits of H on pairs. Thus any group that preserves the orbits on pairs of G must also preserve the orbits on pairs of H, so $2\text{cl}(G) \leq 2\text{cl}(H)$. A permutation group G with $G = 2\text{cl}(G)$ is called **2-closed**. (Note that this closure operation has been studied before, for example in [21]. However the author is unaware of its prior use to compute Möbius numbers.)

Note that any 2-transitive group is automatically primitive, since a pair of points chosen from the same nontrivial block could get set to a pair of points lying in different blocks. Thus

this is a stronger reduction than reducing to only transitive or primitive groups. However, we will pay for this in that the quotient lattice will become more difficult to compute.

4.3 Cyclic Groups are 2-Closed

It will be useful to have classes of groups that we know up front are 2-closed; this will be further discussed in Section 4.5. We can then guarantee that these will show up in the quotient lattice when the 2-closure operation is applied. Here we show any cyclic group is 2-closed.

Theorem 12 *Any permutation representation of a cyclic group is 2-closed.*

Proof.

Let G be a cyclic permutation group. Let $H = 2\text{cl}(G)$. First notice that by definition, G and H have the same orbits on pairs. When looking at an orbit on pairs, one can read off the orbits of a point stabilizer by simply examining a single orbit on pairs and seeing how many places the second coordinate can go while the first remains fixed. Thus the orbits of a point stabilizer in G are the same as the orbits of the corresponding point stabilizer in H, since G and H have the same orbits on pairs. We will repeatedly apply this observation below. We proceed by induction on the number of orbits.

Assume G has only one orbit on the points $\{1, 2, \ldots, n\}$. Then $Stab_G(1)$ is trivial and has trivial orbits, so $Stab_H(1)$ has trivial orbits and is trivial as well. Thus H and G are both acting regularly, so $|H| = n = |G|$. Additionally, $G \leq H$. Thus $G = H$.

Now assume G has m orbits called $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$. Let π be the projection homomorphism onto orbits 2 through m. That is, if $G =< c_1 c_2 \cdots c_m >$ where each c_i is a cycle on $\mathcal{O}_i$, we have that $\pi(c_1 c_2 \cdots c_m) = c_2 \cdots c_m$. Then we know that $\pi(G)$ is 2-closed by induction hypothesis since $\pi(G)$ will have one fewer orbits. Thus $\pi(H) = \pi(G)$. Additionally by examining a pair consisting of two points from $\mathcal{O}_1$, we can see that on the first orbit H projects onto $C_1 :=< c_1 >$.

Thus H is a subdirect product of C_1 with $< c_2 \cdots c_m >$. Assume $H > G$. Then $c_1^k \in H$ but not in G for some natural number k, or $c_2^j \cdots c_m^j \in H$ but not G for some natural number j. (We get such elements as generators of the normal subgroups in our subdirect product.) Let 1 be a point in $\mathcal{O}_1$ and 2 be a point in $\mathcal{O}_2$. In the first case, the orbits of $Stab_H(2)$ are larger than that of $Stab_G(2)$ since the cycle type of c_1^k must actually be a cycle type that was not found in $Stab_G(2)$. In the second case, the orbits of $Stab_H(1)$ are larger than that of $Stab_G(1)$ for the same reasoning. Either case is a contradiction, since the orbits on pairs of H and G are the same.

Thus G is always 2-closed.

■

Note that this result cannot be extended to all abelian groups. For example $\langle (1,2)(3,4), (3,4)(5,6) \rangle$ is abelian but has 2-closure equal to $\langle (1,2), (3,4), (5,6) \rangle$, a strictly larger group.

4.4 Applying the 2-Closure Operation and a Reduction to 2-Transitive Groups

Let $\mu_2(G)$ be the Möbius number of the lattice of 2-closed subgroups of G. If we apply the Closure Theorem to the 2-closure operation, we get

$$\sum_{\substack{G \leq S_n \\ G \text{ 2-transitive}}} \mu(G) = \mu_2(S_n) \tag{4.2}$$

There are extremely few 2-transitive groups compared to transitive groups. For example on 18 points, there are 983 transitive groups but only four 2-transitive groups. In general, there are provably far fewer 2-transitive groups than transitive by results of Pyber and Shalev [17]. A result of Pyber and Shalev shows there are asymptotically few primitive subgroups (and thus even fewer 2-transitive subgroups).

Theorem 13 *[17] The number of conjugacy classes of primitive subgroups of S_n is at most $n^{c \log n}$ for some constant c.*

Comparatively, a result of Pyber says there are asymptotically an enormous number of transitive groups in the case of prime powers. It follows that there is an enormous number of transitive groups for any degree by taking wreath products of these transitive groups on prime powers (for example building a transitive group on 36 points by taking the wreath product of a transitive group on 4 points with a transitive group on 9 points).

Theorem 14 *[16] Let p be a prime. The number of transitive subgroups of S_n, $n = p^\alpha$ is at least $2^{a_p \frac{n^2}{\log n}}$ for some constant a_p.*

Thus the number of terms in the right hand side of the sum in Equation 4.2 will be extremely small compared to the number of terms in the right hand side of the sum in Equation 4.1. Additionally, the sizes of the groups that do appear (besides the alternating and symmetric groups) will be small by a theorem of Praeger and Saxl.

Theorem 15 *[15] Any primitive group of degree n that is not A_n or S_n has order less than 4^n.*

The symmetric group can have transitive subgroups much larger than this, for example in S_{18} the order of $S_9 \wr S_2$ (see Section 4.5 for a definition of $\wr$) is larger than 4^{18}.

In addition to being small in number and harmless in size, doubly-transitive groups are much more tightly classified. Although algorithms for constructing all transitive groups of a given degree exist [8], there is not in general an easy description of all transitive groups of an arbitrary degree. However, the 2-transitive groups are fully classified for any degree as a consequence of the Classification of Finite Simple Groups (see for example Theorem 5.3 of [4]). Thus the sum in the Closure Theorem is vastly simplified. This essentially reduces the problem of finding $\mu(S_n)$ to finding $\mu_2(S_n)$, at least for most n. It should be noted that $\mu(A_n)$ will come up as a term in the sum in 4.2 since A_n will be 2-transitive. However, the subgroup lattice of A_n and the subgroup lattice of S_n are so similar that typically A_n itself can be dealt with by some ad-hoc techniques. For example in [12], A_{12} was easily discarded in the computation of $\mu(S_{12})$.

To compute $\mu_2(S_n)$ at first glance one would need all 2-closed subgroups. However, getting a description of all 2-closed subgroups of S_n is not feasible. If we again apply the 1-closure operation to the lattice of 2-closed subgroups, we get a reduction to only the transitive 2-closed subgroups.

Theorem 16

$$\sum_{\substack{G \leq S_n \\ G \text{ transitive and 2-closed}}} \mu_2(G) = (-1)^{n-1}(n-1)!$$

Proof. We apply the Closure Theorem using the 1-closure operation on the lattice of 2-closed subgroups. The left-hand side of the sum is clear; the only 2-closed groups that get mapped to S_n under the 1-closure operation are the transitive groups. For the right-hand side, we must verify that when applying the 1-closure operation to the lattice of 2-closed subgroups that we do in fact get all possible partitions of the set $\{1, 2, \ldots, n\}$ (the formula on the right-hand side is simply the Möbius number of the lattice of partitions of a set with n elements). Thus we just need to construct one 2-closed group for each partition of the set $\{1, 2, \ldots, n\}$. Since every cyclic group is 2-closed (Theorem 12), we can simply pick a group generated by a single element whose cycle type is given by the partition we want. For example, if $n = 8$ then the partition $\{\{1, 2, 3\}, \{4, 5, 6, 7\}, \{8\}\}$ is realized as the 1-closure of the cyclic (and hence 2-closed) group $\langle(1, 2, 3)(4, 5, 6, 7)(8)\rangle$. Thus the quotient lattice of the lattice of 2-closed subgroups under the 1-closure operation is the entire lattice of partitions. ■

Notice that we now have effectively reduced the problem to finding $\mu_2(G)$ of transitive 2-closed groups $G < S_n$ since the above equation could then be solved for $\mu_2(S_n)$. For a particular degree there are typically not very many of these: in the case of degree 18 we have that only 93 of the 983 transitive subgroups are actually 2-closed.

Thus our primary goal is now to describe what the 2-closed transitive subgroups are for various degrees and then to compute the 2-closed Möbius numbers of transitive 2-closed subgroups. This is the goal of the remainder of this section and a place where much future work can be done.

4.5 Classifying the 2-Closed Transitive Subgroups

We aim to get a description of the 2-closed transitive subgroups. By Theorem 12 we know that in degree n we will always have the cyclic group of order n as a 2-closed transitive subgroup. The symmetric group of degree n will also be 2-closed. Tests in GAP have revealed two promising traits. Many of the remaining transitive 2-closed subgroups are wreath products in natural action of 2-closed groups of smaller degree or subgroups of such wreath products. (The **wreath product in natural action** of two permutation groups A and B is written $A \wr B$. If B acts on m points, $A \wr B$ is the permutation group formed by taking a direct product of m copies of A acting disjointly and then letting B permute the copies of A.) In particular, if A and B are 2-closed permutation groups acting respectively on n and m points with $nm < 32$ then $A \wr B$ is again 2-closed. As it was verified in GAP for so many cases, we make the following conjecture:

Conjecture 17 *Let A and B be 2-closed. Then $A \wr B$ in the natural action is also 2-closed.*

Also, not many of the subgroups of the 2-closed wreath products are again 2-closed. For example, of the 93 2-closed transitive groups on 18 points, only 59 are not wreath products of 2-closed groups of smaller degree (and two of those 59 are accounted for by the cyclic group of degree 18 and the symmetric group of degree 18). Thus it will be necessary to obtain some general conditions for a proper subgroup of a wreath product to be 2-closed.

4.6 Current Progress on the Computing the 2-Closed Möbius Numbers of Transitive 2-Closed Subgroups

One reason the reduction to 2-closed groups seems like a fruitful approach is how much simpler some subgroup lattices get after taking 2-closures. For example, there is no known simple theoretical argument that computes $\mu(S_2 \wr S_3)$. Through a brute force enumeration of the subgroup lattice using GAP, we can obtain $\mu(S_2 \wr S_3) = 48$.

However, consider complements to the subgroup $\langle (1,2)(3,4)(5,6) \rangle$ in the subgroup lattice of $S_2 \wr S_3$. Again through enumeration of the subgroup lattice using GAP, we find it has two

complements:

$$\langle (3,5)(4,6), (1,3,5)(2,4,6), (1,2)(3,4), (3,4)(5,6) \rangle$$

and

$$\langle (1,2)(3,6)(4,5), (1,3,5)(2,4,6), (1,2)(3,4), (3,4)(5,6) \rangle$$

However, neither of these groups is 2-closed. In fact both have 2-closure equal to $S_2 \wr S_3$. Notice $\langle (1,2)(3,4)(5,6) \rangle$ is 2-closed by Theorem 12. Thus in the lattice of 2-closed subgroups of $S_2 \wr S_3$, we have an uncomplemented subgroup, so $\mu_2(S_2 \wr S_3) = 0$ by the Complement Theorem.

Thus it is plausible that we can get a hold on the 2-closed Möbius numbers of groups whose Möbius numbers we couldn't find. We now show that the argument above generalizes to all groups of the form $S_2 \wr S_m$.

4.7 The 2-Closed Möbius Number of $S_2 \wr S_m$

Theorem 18 *For all integers $m > 1$, $\mu_2(S_2 \wr S_m) = 0$.*

Proof.

First we do the case where $m = 2$. One can easily verify that every subgroup of $S_2 \wr S_2$ is 2-closed. Thus the lattice of subgroups of $S_2 \wr S_2$ is isomorphic to its lattice of 2-closed subgroups. Therefore $\mu_2(S_2 \wr S_2) = \mu(S_2 \wr S_2)$ which is zero by Theorem 28 in [12].

Now assume $m \geq 3$. Let $H = \langle (1,2)(3,4)(5,6) \cdots (2m-1, 2m) \rangle$, the diagonal subgroup of the base group. We show that any complement to H in the subgroup lattice of $S_2 \wr S_m$ has 2-closure equal to $S_2 \wr S_m$. Since H is cyclic, H will be an uncomplemented subgroup in the lattice of 2-closed subgroups of $S_2 \wr S_m$ by Theorem 12. The Complement Theorem will then give us that $\mu_2(S_2 \wr S_m) = 0$.

Let K be a complement for H in the subgroup lattice of $S_2 \wr S_m$. Write $\mathcal{O}_H$ for the orbits of H on pairs, and $\mathcal{O}_K$ for the orbits of K on pairs. An easy computation shows that $\mathcal{O}_H = A \cup B$ where

$$A = \{\{[1,2],[2,1]\}, \{[3,4],[4,3]\}, \ldots, \{[2m-1,2m],[2m,2m-1]\}\}$$

and

$$B = \{\{[1,3],[2,4]\},\{[3,1],[2,4]\},\{[1,4],[2,3]\},\{[4,1],[3,2]\},\ldots\}$$

That is, A is the set of pairs of points from the same H-orbit and the B is the set of pairs of points where each point was chosen from a different H-orbit.

Similarly, we compute the orbits on pairs of $S_2 \wr S_m$ as

$$\{[1,2],[2,1],[3,4],[4,3],\ldots,[2m-1,2m],[2m,2m-1]\}$$

and

$$\{[1,3],[2,4],[3,1],[2,4],[1,4],[2,3],[4,1],[3,2],\ldots\}$$

In summary, $S_2 \wr S_m$ has just two orbits on pairs, one orbit where the points in the pairs come from the same block, and one orbit where the the points in the pair come from different blocks.

Notice that the union of all elements in A would give us the first orbit of $S_2 \wr S_m$ and the union of all elements in B would give us the second orbit of $S_2 \wr S_m$. Thus if K and H together generate all of $S_2 \wr S_m$, we must have that the join of $\mathcal{O}_H$ with $\mathcal{O}_K$ must be the orbits on pairs of $S_2 \wr S_m$. Thus $\mathcal{O}_K$ must have an orbit with one pair from each set of A and an orbit with one pair from each set of B. (Notice that saying $\mathcal{O}_K$ has an orbit with one pair from each set in A is equivalent to saying that K must be transitive on the blocks, which is certainly true since H acts trivially on the blocks.) Thus we just need to show without loss of generality that K has an element that maps $[1,2]$ to $[2,1]$ and an element that maps $[1,3]$ to $[2,4]$.

Since H is in fact the center of $S_2 \wr S_m$, H is a normal subgroup. Thus we have $S_2 \wr S_m = H \rtimes K$. Therefore every element of $S_2 \wr S_m$ is expressible in the form hk for some $h \in H$ and $k \in K$. In particular, $(5,6) \in S_2 \wr S_m$. Since there are only two elements in H, either $(5,6) \in K$ as well or $(1,2)(3,4)(7,8)\cdots(2m-1,2m) \in K$.

Assume $(5,6) \in K$. Since K is transitive on the blocks, every transposition in $S_2 \wr S_m$ is also in K. For example, let $k \in K$ be some element with $\{5,6\}^k = \{1,2\}$. Then $k^{-1}(5,6)k = (1,2)$ since we simply relabel the points of $(5,6)$ according to the permutation given by k. Thus

$(1,2),(3,4),(5,6),\ldots,(2m-1,2m)$ are all elements in K, so their product is as well. But their product is the generator of H, which cannot be in K since H and K intersect trivially. Thus $(5,6)$ is not in K.

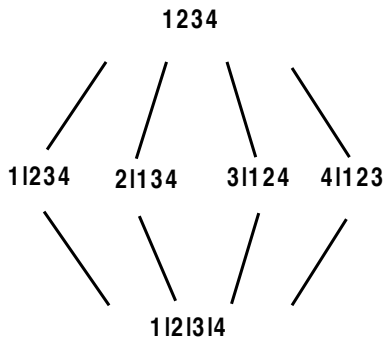
Therefore the other case must hold: $(1,2)(3,4)(7,8)\cdots(2m-1,2m) \in K$. Call this element k. Then $[1,2]^k = [2,1]$ and $[1,3]^k = [2,4]$. Thus K has the same orbits on pairs as $S_2 \wr S_m$, so it is not 2-closed. Applying the Complement Theorem, we have $\mu_2(S_2 \wr S_m) = 0$.

■

Chapter 5

An Even Closure Operation and an Odd Poset

One of the most natural and well-studied posets is the poset Π_n of partitions of an n-element set ordered by refinement. A related object is the subposet of partitions of an n-element set using only odd-size parts and the maximum element $\{\{1, 2, \ldots, n\}\}$. We call this the odd-partition poset and denote it Π_n^{odd}. This poset will come up in our work as the quotient poset of subgroup lattices under certain closure operations, as will be seen soon. For example, the diagram below illustrates Π_4^{odd}:



This poset arises in our work when considering the following closure operation on the subgroup lattice of a group G. Let H be a subgroup of G. Then

$$\overline{H} = \begin{cases} H & : \text{if } |H| \text{ is odd} \\ G & : \text{if } n \text{ is even} \end{cases}$$

It is trivial to verify that this is in fact a closure operation. Additionally, when applied to

the lattice of subgroups of the symmetric group of degree n followed by the closure operation that replaces groups by setwise stabilizers of orbits (which is equivalent to simply replacing them by their orbits themselves), one obtains the odd partition poset as the quotient poset. This is true because a group with an orbit of even length must have even order. Direct products of cyclic groups with odd orders give all partitions with only odd part size.

Computing the Möbius number of this poset for some small values of n reveals a simple pattern:

$$\begin{aligned}
\mu\left(\Pi_1^{\text{odd}}\right) &= 1 \\
\mu\left(\Pi_2^{\text{odd}}\right) &= -1 \\
\mu\left(\Pi_3^{\text{odd}}\right) &= -1 \cdot 1 \\
\mu\left(\Pi_4^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \\
\mu\left(\Pi_5^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \\
\mu\left(\Pi_6^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \cdot -5 \\
\mu\left(\Pi_7^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \cdot -5 \cdot 5 \\
\mu\left(\Pi_8^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \cdot -5 \cdot 5 \cdot -7 \\
\mu\left(\Pi_9^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \cdot -5 \cdot 5 \cdot -7 \cdot 7 \\
\mu\left(\Pi_{10}^{\text{odd}}\right) &= -1 \cdot 1 \cdot -3 \cdot 3 \cdot -5 \cdot 5 \cdot -7 \cdot 7 \cdot -9 \\
&\vdots
\end{aligned}$$

The fact that this pattern continues forever is the main result of this section:

Theorem 19 *Let Π_n^{odd} be the odd-partition poset of an n-element set. Then the Möbius number $\mu(\Pi_n^{\text{odd}})$ is given by*

$$\mu(\Pi_n^{\text{odd}}) = \begin{cases} (-1)^{(n-1)/2}\left((n-2)!!\right)^2 & : \text{if } n \text{ is odd} \\ (-1)^{n/2}(n-1)\left((n-3)!!\right)^2 & : \text{if } n \text{ is even} \end{cases}$$

where $k!!$ denotes the double-factorial, the product of all integers between 1 and k with the same parity as k.

It should be noted that the absolute value of this sequence does appear on The On-Line Encyclopedia of Integer Sequences as sequence A000246 [10] in other combinatorial settings. Our characterization of the sequence was not listed and has been submitted.

It should also be noted that this formula is stated as "known" on page 291 of [3]. However no reference is given, and even after contacting the authors, a prior proof in the literature was not found. Here we provide an original and elementary combinatorial proof simply

using generating functions, induction, the Zeilberger-Wilf Algorithm, and techniques from undergraduate calculus and differential equations.

The following well-known result will be used heavily in Section 5.1, so we state it explicitly. For a proof see [20].

Lemma 20 *[20, Proposition 3.8.2] Given posets P and Q with $(x,y) \leq_{P\times Q} (x',y')$, we have that*

$$\mu_{P\times Q}((x,y)(x',y')) = \mu_P(x,x')\,\mu_Q(y,y')$$

and in particular

$$\mu(P\times Q) = \mu(P)\cdot\mu(Q).$$

Notice that the odd partition poset in general is strictly a poset and not a lattice.

Remark 21 *The poset Π_n^{odd} is not a lattice for $n \geq 12$.*

Proof. Notice that if $n = 12$, the elements

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

and

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

have two least upper bounds:

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

and

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

For any $n > 12$ we will have a subposet of Π_n^{odd} isomorphic to this by simply adding singletons to each of these partitions. Thus none of these are lattices since lattices have unique least upper bounds. ■

Because of this, the frequently used and very powerful lattice-theoretic tools such as Crapo's Complement Theorem ([5]) will be inapplicable in this situation. We thus proceed instead with bare-knuckled enumerative combinatorics. The proof follows in four steps:

1. In Section 5.1, we write down a true but unwieldy recurrence relation for the Möbius numbers of the odd-partition posets based on the defining recurrence for Möbius numbers. This will be easy to verify but essentially impossible to work with since it will involve sums indexed over integer partitions with odd part size.

2. In Section 5.2, we emulate the product formula for the partition generating function to build two generating functions. We will show these two generating functions are equal if and only if Theorem 32 is true. The generating functions graciously handle the messiness of the sums from Section 5.1 for us.

3. In Section 5.3, we write down an Initial Value Problem and show that it has a unique solution.

4. In Section 5.4, we show the two generating functions are in fact equal by verifying that they both solve the Initial Value Problem. The crucial step in this verification is done via induction using the brilliant and powerful Zeilberger-Wilf Algorithm as documented in [14].

For notational convenience, let

$$\mu_n = \begin{cases} (-1)^{(n-1)/2}\left((n-2)!!\right)^2 & : \text{if } n \text{ is odd} \\ (-1)^{n/2}(n-1)\left((n-3)!!\right)^2 & : \text{if } n \text{ is even} \end{cases}$$

That is, μ_n is the name we are giving to the numbers themselves. We will proceed to show that these numbers are in fact the Möbius numbers of the posets.

5.1 Recurrence for the Möbius Numbers

Let $\lambda \vdash n$. That is, λ is a partition of the integer n. If $\mathcal{B}$ a partition of the set $\{1, 2, \cdots, n\}$ such that the multiset of sizes of parts of $\mathcal{B}$ is λ, we say $\mathcal{B}$ has *type* λ. For our purposes, we require λ uses only parts that have odd size or size n. Expressing λ in frequency notation, we have $\lambda = (1^{\lambda_1}3^{\lambda_3}5^{\lambda_5}\cdots(2k+1)^{\lambda_{2k+1}}n^{\lambda_n})$ be a partition of the integer n. That is, λ is a partition of n with λ_1 parts of size 1, λ_3 parts of size 3, and so on. Notice that in the odd

partition poset, the set partitions must be of this type. Additionally λ_n can only be 0 or 1, and if it is 1 then all other λ_i are 0.

We now use the Orbit-Stabilizer Theorem to count the number of set partitions of an n-element set with a fixed type $\lambda = (1^{\lambda_1}3^{\lambda_3}5^{\lambda_5}\cdots(2k+1)^{\lambda_{2k+1}}n^{\lambda_n})$. Clearly if $\lambda_n = 1$ then there is only one partition. Otherwise we have $n!$ elements of S_n acting pointwise on the elements of the set $\{1, 2, \ldots, n\}$. The stabilizer of a set partition with type λ will be a direct product of imprimitive wreath products of symmetric groups: while preserving the partition we can permute within any one of the parts or we can permute parts of the same size. Thus the stabilizer is

$$\bigotimes_{i\in\{1,3,5,\ldots,2k+1\}} S_i \wr S_{\lambda_i}$$

which has order

$$\prod_{i\in\{1,3,5,\ldots,2k+1\}} \lambda_i! \cdot i!^{\lambda_i}.$$

By the Orbit-Stabilizer Theorem, we see that Π_n^{odd} has

$$\frac{n!}{\prod_{i\in\{1,3,5,\ldots,2k+1\}} \lambda_i! \cdot i!^{\lambda_i}}$$

set partitions of type λ.

For fear of something relatively simple becoming obfuscated by excessive notation, we give an example. The set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ has many partitions of the type $(1^2 3^2)$ in Π_8^{odd}. That is, we have set partitions with two parts of size 1 and two parts of size 3. We wish to count how many such partitions it has. Letting S_8 act on the points 1 through 8, we have 8! total group elements acting. We now count how many fix such a partition. We have one copy of S_3 acting on each part of size 3. We have an S_2 that swaps the parts of size 3, and another S_2 that swaps the parts of size 1.

Thus total we have $\frac{8!}{3!^2 \cdot 2 \cdot 2}$ partitions with type $(1^2 3^2)$.

Next observe that any two partitions of the same type will have the same Möbius number, since the poset lying underneath will be isomorphic with the isomorphism given via an S_n conjugacy map.

Suppose a set partition P has type $\lambda = \{n_1, n_2, \cdots, n_m\}$ (written as a multiset). Then the subposet consisting of all elements of Π_n^{odd} less than or equal to P is isomorphic to the product poset of $\Pi_{n_1}^{\text{odd}}$, $\Pi_{n_2}^{\text{odd}}$, ..., $\Pi_{n_m}^{\text{odd}}$. Therefore by Lemma 20 we have

$$\mu(P) = \prod_{i \in \{1,2,\ldots,m\}} \mu(\Pi_{n_i}^{\text{odd}})$$

At this point, writing down the recurrence relation for the Möbius numbers amounts to just putting all the above pieces together. We know by the defining recurrence of Möbius Numbers that the Möbius number of Π_n^{odd} is the negation of the sum of the Möbius numbers of all smaller partitions in Π_n^{odd}. We can group these smaller elements according to partition type. By the above arguments, for each type, we know how many elements there are with that type and what the Möbius number is as a product of smaller Möbius numbers. Summing over all valid partitions gives us our recurrence:

Lemma 22 *Let $\mathcal{P}$ be the set of all types of partitions that occur in Π_n^{odd} except for the trivial partition consisting of just 1 part of size n. Abbreviate $m_i = \mu(\Pi_i^{\text{odd}})$. Then*

$$\mu(\Pi_n^{\text{odd}}) = -\sum_{\lambda \in \mathcal{P}} \prod_{i \in \{1,3,5,\ldots,2k+1\}} \frac{n! m_i^{\lambda_i}}{\lambda_i! \cdot i!^{\lambda_i}}$$

where $\lambda = (1^{\lambda_1} 3^{\lambda_3} 5^{\lambda_5} \cdots (2k+1)^{\lambda_{2k+1}})$.

5.2 Building the Generating Functions

Recall our notational shortcut: $m_i = \mu(\Pi_i^{\text{odd}})$.

Also recall the well-known infinite product formula for the generating function for partitions of sets:

$$\prod_{n \in \mathbb{N}} \frac{1}{1 - t^n} = \prod_{n \in \mathbb{N}} \sum_{i=0}^{\infty} t^{n \cdot i}$$

We observe that by slightly modifying the right-hand side of that infinite product, we can get expressions very similar to what we have in Lemma 22. First of all we throw out any even n, since these are not part sizes that will come up in the odd partition poset except for maximal elements, which we will handle separately. Additionally, the term $t^{n \cdot i}$ should be

multiplied by $\frac{m_n^i}{i!n!^i}$ to give the Möbius numbers and the Orbit-Stabilizer counts that occur in Lemma 22. Thus by applying that recurrence in each degree, we have that

$$\prod_{n \text{ odd}} \sum_{i=0}^{\infty} \frac{m_n^i}{i!n!^i} t^{n \cdot i} = 1 + t - \frac{m_2}{2!}t^2 - \frac{m_4}{4!}t^4 - \frac{m_6}{6!}t^6 - \frac{m_8}{8!}t^8 - \cdots$$

On the other hand, we can use the power series expansion for the exponential function to do a different manipulation to the same series:

$$\prod_{n \text{ odd}} \sum_{i=0}^{\infty} \frac{m_n^i}{i!n!^i} t^{n \cdot i} = \prod_{n \text{ odd}} e^{\frac{m_n}{n!}t^n} = e^{m_1 t + \frac{m_3}{3!}t^3 + \frac{m_5}{5!}t^5 + \frac{m_7}{7!}t^7 + \cdots}$$

These two expressions for the same power series provide us with our fundamental strategy for proving that the Möbius numbers m_i really are the numbers μ_i as we claim. We simply write down the same two power series with μ_i instead of m_i. The power series are equal if and only if for all i, $\mu_i = m_i$. Stated more formally:

Lemma 23 *Let*

$$L(t) = e^{\mu_1 t + \frac{\mu_3}{3!}t^3 + \frac{\mu_5}{5!}t^5 + \frac{\mu_7}{7!}t^7 + \cdots}$$

and let

$$R(t) = 1 + t - \frac{\mu_2}{2!}t^2 - \frac{\mu_4}{4!}t^4 - \frac{\mu_6}{6!}t^6 - \frac{\mu_8}{8!}t^8 - \cdots$$

Then $L(t) = R(t)$ is equivalent to Theorem 32.

The goal of the next two sections is to show that $L(t)$ is indeed equal to $R(t)$.

5.3 The Initial Value Problem

We now define an Initial Value Problem, intentionally writing down the obvious Initial Value Problem solved by $L(t)$ as defined in Lemma 23 simply using the chain rule and the derivative of the exponential.

$$\frac{dy}{dt} = y \cdot (\mu_1 + \frac{\mu_3}{2!}t^2 + \frac{\mu_5}{4!}t^4 + \frac{\mu_7}{6!}t^6 + \cdots) \qquad (*)$$
$$y(0) = 1$$

We would like to claim that $*$ has a unique solution. To do this we show:

Lemma 24 *The series* $\mu_1 + \frac{\mu_3}{2!}t^2 + \frac{\mu_5}{4!}t^4 + \frac{\mu_7}{6!}t^6 + \cdots$ *converges absolutely for* $-1 < t < 1$.

Proof. Applying the standard ratio test for convergence of power series from an undergraduate calculus course yields the desired result. ■

Clearly all involved functions are differentiable and have continuous partial derivatives. Thus the standard theorem on uniqueness of solutions to an Initial Value Problem from an undergraduate Differential Equations course applies and we get:

Lemma 25 *The Initial Value Problem* $*$ *has a unique solution.*

5.4 Verifying the Generating Functions Both Solve the Initial Value Problem

The fact that $L(t)$ satisfies the Initial Value Problem is clear. To show that $R(t)$ also satisfies the Initial Value Problem, we trivially check that the initial condition holds. We then plug $R(t)$ into both sides of the differential equation. Basic algebra shows that all terms of odd degree match. The terms of even degree are not so obvious. To show that the coefficients match on the terms of even degree is equivalent to verifying the following identity for all even n:

$$O_n = \sum_{k \in \{2,4,\ldots,n\}} O_{n-k} O_{k-1} \binom{n}{k}$$

where O_n is defined to be $|\mu_n|$. To solve this sum, we use the Zeilberger-Wilf Algorithm as explained in [14] devised for verifying such hypergeometric identities. To do this, we reformulate our sum by defining $P_n = O_{2n}$ and using the fact that $O_{2k-1} = \frac{O_{2k}}{2k-1}$. Thus our sum becomes

$$1 = \sum_k \frac{P_{n-k} P_k \binom{2n}{2k}}{(2k-1)P_n}$$

so that we are summing over all k and proving the identity for all n rather than just for even n. Following [14], we then plug in the right-hand side to Gosper's Algorithm (as implemented in Maple) to get the proof certificate. In this case the proof certificate ($R(n,k)$ in the notation of page 25 of [14]) is the function

$$\frac{(-2n-1+2k)(k-1)k}{(2n+1)(k-n-1)n}.$$

Following the proof on page 25 of [14] verifies the identity. Thus the proof of Theorem 19 is complete.

Chapter 6

The Möbius Number of the Socle

One very important normal subgroup of a group is the **socle**, the subgroup generated by all minimal normal subgroups of a group. One can show that the socle of a group is always a direct product of simple groups, see for example [6]. Thus we would like a formula for the Möbius number of a direct product of simple groups. This would allow us to compute the Möbius number of the socle of a group and get the Möbius number of the group itself if the group is not't much more complicated than its socle. In our particular case, we want to compute the Möbius numbers and thus 2-closed Möbius numbers of the transitive 2-closed groups. Here the socle is a particularly good normal subgroup to use! Often these groups are wreath products whose subgroup lattice is mostly socle -in the case of degree 18, $S_6 \wr S_3$ would be such an example since the socle would be $A_6 \times A_6 \times A_6$.

Thus a formula for the Möbius number of the socle of a group is an important step on the way to getting the Möbius numbers of the symmetric groups. In this section we provide such a formula with proof. It should be noted that the results in this section, while proven independently by the author, rather easily follow from results in [2].

6.1 Subdirect Products

We begin by classifying complements to one factor in a direct product. In order to do this we first need some basic definitions and results on subdirect products. All of this with more detail can be found in [6].

If a group G is a subgroup of $A \times B$, it has natural projection maps $\pi_A : G \to A$ and

$\pi_B : G \to B$. If $\pi_A(G) = A$ and $\pi_B(G) = B$ and the kernels of these two projection maps intersect trivially, we say that G is a **subdirect product** of A and B.

Let $H = \langle \ker(\pi_A), \ker(\pi_B) \rangle$. Clearly this is a normal subgroup of G, since both kernels are. By the First Isomorphism Theorem, we have $G/H \cong A/\pi_A(H) \cong B/\pi_B(H)$.

Thus we see that to start with groups A and B and build a subdirect product from them, they must have a common factor group. Suppose we have some $D \lhd A$ and $E \lhd B$ with $A/D \cong B/E$. Let $\zeta : A/D \to B/E$ be an isomorphism. Then we can describe the subdirect product of A with B as

$$A \curlywedge B = \{(a, b) : a \in A, b \in B, Da^{\zeta} = Eb\}$$

Notice there is not in general a unique subdirect product of A with B, different choices of D, E, and ζ will result in different subdirect products. We always have the trivial group as a common factor group; this corresponds to the fact that the direct product can always be formed.

6.2 Complements in Direct Products

In this section we work out the structure of a complement to one factor of a direct product.

Lemma 26 *Let $G = H \times K$. Let $\phi_K : G \to K$ be the projection map onto K. Let K' be a complement for H in the subgroup lattice of G. Then K' is of the form $K' = H_0 \curlywedge K$ for some $H_0 \leq H$ with H_0 isomorphic to some homomorphic image of K. Additionally, ϕ_K has trivial kernel when restricted to K'.*

Proof. Let $\phi_H : G \to H$ similarly be the projection map onto H. Let $K' \leq G$ and assume K' is a complement of H. Since $< H, K' >= G$ and $H = \ker \phi_K$, we have $\phi_K(K') = \phi_K(< H, K' >) = \phi_K(G) = K$. Let $H_0 = \phi_H(K')$. By the Second Isomorphism Theorem, K' is isomorphic to K. Thus H_0 is isomorphic to a homomorphic image of K since projection maps are homomorphisms. The image lies in H, so $H_0 \leq H$.

Thus we have that K' is a subdirect product of H_0 with K'.

Since $\ker(\phi_K) = H$, we have $\ker(\phi_K|_{K'}) = K' \cap \ker(\phi_K) = K' \cap H$ which is trivial. Thus we see that ϕ_K has trivial kernel when restricted to K'. ■

Note the condition that ϕ_K has trivial kernel when restricted to K' is intuitively saying that H_0 must be 'fully glued' to some factor of K'. This makes sense because having any 'unglued' pieces of H_0 would intersect nontrivially with H and thus K' would not be a complement.

Also notice that this does in fact give an algorithm for constructing all complements to H in $G = H \times K$. We get one class of complements for each such H_0 (an automorphism may be applied to form the subdirect product in a different manner). Thus finding all complements simply amounts to finding all subgroups of H isomorphic to a homomorphic image of K and knowing the automorphisms of these subgroups. We use this strategy to compute the Möbius numbers of some special direct products.

Lemma 27 *Let $G = H \times K$ and assume K has no nontrivial homomorphic image isomorphic to a subgroup of H. Then $\mu(H \times K) = \mu(H)\mu(K)$.*

Proof. We look at complements to H in the subgroup lattice of G. The only possibility for H_0 as described in Lemma 26 is the trivial group, which gives K itself as the only complement. Since K is normal in G, the interval of subgroups between K and G is isomorphic to the subgroup lattice of H by the Fourth Isomorphism Theorem. Thus we can apply Crapo's Complement Theorem in the simpler form given in Corollary 10 to get that the Möbius number of G is

$$\mu(G) = \mu(K)\mu(K, G) = \mu(K)\mu(H).$$

■

Example 28 *One can easily compute (for example just from the definition of μ using GAP) that the Möbius number of S_3 is 3 and the Möbius number of A_5 is -60. Thus the Möbius number of $S_3 \times A_5$ is -180 since the only homomorphic images of A_5 are trivial or A_5 itself, and A_5 is not isomorphic to a subgroup of S_3.*

Notice that Lemma 27 has a very nice aesthetic parallel to a similar property of the number-theoretic Möbius function. Namely, for any integers n and m, if n and m are coprime then $\mu(nm) = \mu(n)\mu(m)$. Here we have a similar result for groups; it would seem that the hypothesis of Lemma 27 is a sufficient condition for whatever it means for two groups to be coprime!

Also notice that Lemma 27 does not follow from the fact that the Möbius number of a product poset is the product of the Möbius numbers of each factor. In general the lattice of subgroups of $H \times K$ will be much larger than the product lattice of the subgroups of H with the subgroups of K. The example above illustrates this: many subdirect products of S_2 (a homomorphic image of S_3) with a subgroup of A_5 isomorphic to S_2 will appear in the subgroup lattice of $S_3 \times A_5$. These subdirect products are not direct products of subgroups of each lattice.

6.3 The Homomorphic Images of a Product of Simple Groups

In order to apply Lemma 27, we will first want a classification of all possible homomorphic images of a direct product of simple groups.

Lemma 29 *Let $U_1, U_2, \ldots, U_m$ be distinct nonabelian simple groups. Let $G = U_1^{e_1} \times U_2^{e_2} \times \cdots \times U_m^{e_m}$. Then every homomorphic image of G is of the form $U_1^{f_1} \times U_2^{f_2} \times \cdots \times U_m^{f_m}$ for some natural numbers $f_i \leq e_i$ for $i \in \{1, 2, \ldots, m\}$.*

Proof. This result is equivalent to showing that any normal subgroup of G also has the above form. Let $N \lhd G$. Let π be the projection of N onto U, some factor of G. Since U is simple, $\pi(N)$ is either trivial or all of U, since intersecting a normal subgroup of G with a factor of G will produce again a normal subgroup of G. Thus since N projects trivially or fully onto each factor, N is a subdirect product powers of the U_i. Simplicity of the U_i implies that any subdirect product actually degenerates to a direct product, so N is of the required form. ■

Note that additionally for the normal subgroup, the 'gluing' in the subdirect product must be trivial, ie we cannot have any diagonal subdirect products of the simple groups in N. If we did, one could apply an inner automorphism, conjugating by an element of one of the simple groups in the diagonal subdirect product, and N would not be normal.

6.4 The Möbius Number of a Direct Power of an Abelian Simple Group

A direct power of an abelian simple group looks like $C_p^n = \underbrace{C_p \times C_p \times \cdots \times C_p}_{n}$ for some prime p and some integer n. This is clearly isomorphic to a vector space of dimension n over the field with p elements, and the subgroups of such a group will correspond to the subspaces of a such a vector space. The Möbius number of a finite vector space is well-known and can be found for example in Chapter 3 Exercises 28 and 45 of [20]. Thus we have:

Corollary 30 *The Möbius number of C_p^n is $(-1)^n p^{\binom{n}{2}}$.*

6.5 The Möbius Number of a Direct Power of a Nonabelian Simple Group

Theorem 31 *Let T be a nonabelian simple group. Let $T^n = \underbrace{T \times T \times \cdots \times T}_{n}$. Then*

$$\mu(T^n) = \prod_{j=1}^{n} (\mu(T) - (j-1)A)$$

where A is the size of the automorphism group of T.

Proof. We use Lemma 26 to enumerate all possible complements to T_1. In each case we analyze the structure of the interval of the subgroup lattice lying above the complement. Finally we apply the Complement Theorem.

Again let K' be a complement to T_1. Let $K = T_2 \times \cdots \times T_n$. Then as in the lemma, $K' = H_0 \leftthreetimes K$ for some $H_0 \leq T_1$ with H_0 a homomorphic image of K. By Lemma 29, the only homomorphic images of K are isomorphic to $1, T, T^2, T^3, \cdots, T^{n-1}$. However, only 1 and T are subgroups of T_1, so they are the only two choices for H_0.

Case 1: If $H_0 \cong 1$, $K' = K$. In this case the interval $[K, G]$ is isomorphic to the subgroup lattice of T since $G/K \cong T_1$ by the First Isomorphism Theorem.

Case 2: If $H_0 \cong T$, K' is a subdirect product of T_1 and $T_2 \times \cdots \times T_n$. In this case we claim the interval $[K', G]$ is just a totally ordered lattice with two nodes. That is, K' is maximal in G. To see this is true, assume we have a subgroup J with $K' \leq J \leq G$. Then any projection of K' has to be a subgroup of the same projection of J. That is, $\phi_{T_1}(K') = T_1$ and $\phi_K(K') = K$ implies $\phi_{T_1}(J) = T_1$ and $\phi_K(J) = K$ as well. Thus J is also a subdirect product of T_1 and K. Since $\ker(\phi_K|_J)$ must be a normal subgroup of T_1, it is either 1 or T_1. If $\ker(\phi_K|_J) = 1$ then $J = K'$. If $\ker(\phi_K|_J) = T_1$ then $J = G$. Thus K' is maximal in G. The Möbius number of such a lattice, a totally ordered lattice with two elements, is -1.

Now we just have to count how many different ways each can occur. Clearly there is only one way Case 1 can happen. However, for Case 2, in the subdirect product H_0 can be identified with any of the $n-1$ different homomorphic images of K isomorphic to T. Additionally, any automorphism of T can be applied to H_0 to identify it in a different way. Thus we have $(n-1)A$ different subdirect products in Case 2 where $A = |Aut(T)|$.

At last we apply the Complement Theorem, summing over complements of T_1. This yields

$$\mu(T^n) = \mu(T)\mu(T^{n-1}) + (n-1)A\mu(T)(-1)$$

which can be viewed as a recurrence relation with respect to n. Solving the recurrence proves the theorem.

■

6.6 The Möbius Number of a Socle

Combining Theorem 31 with Lemma 27, we get the Möbius number of any socle in terms of the Möbius numbers of the socle types.

Theorem 32 *Let G be a direct product of finite simple groups. More specifically, let $U_1, U_2, \ldots, U_m$ be distinct nonabelian simple groups and let $C_{p_1}, C_{p_2}, \ldots, C_{p_n}$ be abelian simple groups (cyclic*

groups) for some distinct primes $p_1, p_2, \ldots, p_n$. Let A_i be the size of the automorphism group of U_i for each $i \in \{1 \ldots m\}$. Let $F = \sum_{i=1}^{n} f_i$. Let

$$G = C_{p_1}^{f_1} \times C_{p_2}^{f_2} \times \cdots \times C_{p_n}^{f_n} \times U_1^{e_1} \times U_2^{e_2} \times \cdots \times U_m^{e_m}.$$

Then

$$\mu(G) = (-1)^F \prod_{i=1}^{n} p_i^{\binom{f_i}{2}} \prod_{i=1}^{m} \prod_{j=1}^{e_i} (\mu(U_i) - (j-1)A_i).$$

Proof. First assume G has no abelian direct factors. Then $G = U_1^{e_1} \times U_2^{e_2} \times \cdots \times U_m^{e_m}$ for some nonabelian simple groups $U_1, U_2, \ldots U_m$. Without loss of generality, assume $|U_1| < |U_2| < \ldots < |U_m|$. We claim that taking $H = U_1^{e_1}$ and $K = U_2^{e_2} \times \cdots \times U_m^{e_m}$ satisfies the conditions of Lemma 27. By Lemma 29, we have that the only homomorphic images of K are of the form $U_2^{f_2} \times \cdots \times U_m^{f_m}$ for some $f_i \leq e_i$. Assume such a group was isomorphic to a subgroup of H. Then we have $U_2 \leq U_2^{f_2} \times \cdots \times U_m^{f_m} \leq H$ (without loss of generality $f_2 > 0$). Consider the projection maps from H onto its factors (the copies of U_1). At least one of these projection maps must have a nontrivial image when applied to $U_2 \leq H$, otherwise U_2 would be trivial. Let $\pi : U_2 \to U_1$ be such a map with nontrivial image. Since $\ker(\pi)$ is a normal subgroup of U_2 and the image under π is nontrivial, the kernel must be trivial and $\pi(U_2) = U_2 \leq U_1$. But we cannot have $U_2 \leq U_1$ since U_2 has larger order than U_1. Thus applying Lemma 27 gives $\mu(G) = \mu(U_1^{e_1})\mu(U_2^{e_2} \times \cdots \times U_m^{e_m})$. By repeatedly applying this process next with U_2, then with U_3, and so on, we can write

$$\mu(G) = \mu(U_1^{e_1})\mu(U_2^{e_2}) \cdots \mu(U_m^{e_m})$$

and combining the above formula with Theorem 31 proves the result for the case where G has no abelian direct factors. We now must show that any abelian direct factors split off multiplicatively as well.

Once again let $G = C_{p_1}^{f_1} \times C_{p_2}^{f_2} \times \cdots \times C_{p_n}^{f_n} \times U_1^{e_1} \times U_2^{e_2} \times \cdots \times U_m^{e_m}$. Taking $H = C_{p_1}^{f_1} \times C_{p_2}^{f_2} \times \cdots \times C_{p_n}^{f_n}$ and $K = U_1^{e_1} \times U_2^{e_2} \times \cdots \times U_m^{e_m}$ satisfies the conditions of Lemma 27, since an abelian group could not possibly have a subgroup isomorphic to a homomorphic image of a direct product of nonabelian simple groups (since Lemma 29 shows that any such

homomorphic image is nonabelian). Thus $\mu(G) = \mu(H)\mu(K)$, so the abelian part does indeed split off multiplicatively.

At last we compute the Möbius number of the abelian part. Again Lemma 27 implies that

$$\mu\left(C_{p_1}^{f_1} \times C_{p_2}^{f_2} \times \cdots \times C_{p_n}^{f_n}\right) = \mu\left(C_{p_1}^{f_1}\right)\mu\left(C_{p_2}^{f_2}\right)\cdots\mu\left(C_{p_n}^{f_n}\right)$$

since no power of a cyclic group C_p could have a subgroup isomorphic to the homomorphic image of an abelian group that does not have elements of order p. Applying Corollary 30 to each factor proves the result.

■

Example 33 *The Möbius number of C_2 is -1. The Möbius number of A_5 is -60 and its automorphism group has size 120. The Möbius number of A_6 is 720 and its automorphism group has size 1440. Thus we have*

$\mu(C_2 \times A_5^3 \times A_6^2) = -1 * -60 * (-60 - 120) * (-60 - 2 * 120) * 720 * (720 - 1440) = -1,679,616,000,000.$

This is a computation that would clearly not be feasible by any brute force enumeration of the subgroup lattice! Notice that this is in fact divisible by the order of the derived subgroup of $A_5^3 \times A_6^2$ which has order $60^3 * 360^2$ (equal to the group order). Thus we are in agreement with Theorem 4 [11].

It should be noted that there is an ongoing project by Joe Bohanon to compute the Möbius numbers of all sporadic simple groups that has computed the Möbius numbers of sporadic groups Ru and Suz [1]. Additionally [18] has the Möbius numbers of some infinite families of simple groups, including linear groups of dimension two.

Chapter 7

Möbius Numbers of Wreath Products and Some Low-Index Subgroups Towards Computing $\mu(S_{18})$

In this section we compute the Möbius numbers of several infinite families of wreath products. This is useful when using Shareshian's closure operation which reduces computation of $\mu(S_n)$ to computation of the Möbius numbers of transitive subgroups, since most transitive subgroups are wreath products and subgroups of wreath products. In particular we will apply these results to obtain the Möbius number of the symmetric group of degree 18, pending the completion of a large computer calculation currently running.

7.1 The Möbius Number of $S_2 \wr S_m$

Theorem 34 $\mu(S_2 \wr S_m) = \begin{cases} 0 & \text{if } m \text{ is even} \\ 2^m \mu(S_m) & \text{if } m \text{ is odd} \end{cases}$

We prove Theorem 34 by using Crapo's Complement Theorem on the base group of the wreath product. In order to do this, we will find representatives of conjugacy classes of complements to S_2^m in the subgroup lattice of $S_2 \wr S_m$, compute the sizes of these conjugacy classes, and determine the lattice that lies above any such conjugate.

7.1.1 Classifying Complements to the Base Group

First note that any complement to the base group must be isomorphic to S_m since the base group is a normal subgroup and $S_2 \wr S_m / S_2^m \cong S_m$. We claim there are two conjugacy classes

of complements, a class of transitive complements and a class of intransitive complements. We write K_T for a representative of the class of transitive complements and K_I for a representative of the class of intransitive complements. We first construct K_I, then construct K_T, and then prove that there are no further conjugacy classes.

7.1.2 The Intransitive Complement K_I

To construct an intransitive complement, we simply write down generators:

$$K_I = \langle (1,3)(2,4), (1,3,5,\ldots,2m-1)(2,4,6,\ldots,2m) \rangle$$

We can see that this group has trivial intersection with S_2^m since K_I acts trivially within the blocks but S_2^m acts only within the blocks. Together with S_2^m it generates all of $S_2 \wr S_m$ since it provides any way to act upon the blocks and S_2^m provides any way to act within the blocks. Thus K_I is a complement to the base group and is intransitive with orbits $\{1,3,5,...,2m-1\}$ and $\{2,4,6,\ldots,2m)\}$.

7.1.3 The Transitive Complement

To construct the transitive complement K_T, consider S_m in its usual action on m points. A point stabilizer is isomorphic to S_{m-1}. This point stabilizer has a unique index two subgroup, namely the alternating group on $m-1$ points, A_{m-1}. Let S_m now act on cosets of A_{m-1}. This will produce an action of S_m on $2m$ points. The action will be transitive since acting on the cosets of a subgroup is always transitive. This action will also have a block system with blocks of size 2 since A_{m-1} is not a maximal subgroup of S_m but instead is an index two subgroup of a maximal subgroup of S_m. This process of taking a point stabilizer and then acting on the cosets of a subgroup of the point stabilizer to yield an imprimitive action of larger degree is called taking an **inflation**. For example, the regular representation of S_3 is an inflation of the action of S_3 on 3 points. See [8] for more details. This inflation of S_m acting on m points to an action on $2m$ points is our complement K_T.

To see that K_T is a complement, notice that it acts as the full symmetric group on the

blocks. Thus S_2^m and K_T do together generate $S_2 \wr S_m$. Also, K_T can't have any nonidentity elements which fix all blocks, since then the action on the blocks would have a nontrivial kernel but the image of this action is isomorphic to $S_m \cong K_T$. Thus K_T intersects trivially with S_2^m.

7.1.4 Proving There Aren't More Complements

We now show that any complement must be conjugate to either K_I or K_T.

Theorem 35 *As constructed above, K_I and K_T are representatives for the only two conjugacy classes of complements to S_2^m in $S_2 \wr S_m$.*

Proof. Let K be a complement to S_2^m in $S_2 \wr S_m$. We do a proof by cases based on whether K is transitive or intransitive.

First assume K is intransitive. Since K is transitive on the blocks, it must have an orbit of length m. Since it preserves the m blocks of size 2, one orbit of length m implies that K must in fact have two orbits of length m. Conjugating K with a permutation such that one of the orbits is $\{1, 3, 5, \ldots, 2m-1\}$ will produce K_I.

Next assume K is transitive. Considering the action of K on the blocks as permutation isomorphic to S_m acting on m points shows that K is an inflation of this action. By Lemma 3.1 in [8], there is only one conjugacy class of such permutation groups, since there is only one $Aut(S_m)$-class of A_{m-1} subgroups in S_m. ■

7.1.5 Counting Numbers of Conjugates

It turns out both conjugacy classes of subgroups are of size 2^{m-1}.

Lemma 36 *Both K_T and K_I have 2^{m-1} conjugates in $S_2 \wr S_m$.*

Proof. Let $K \in \{K_T, K_I\}$. By the Orbit-Stabilizer Theorem, the number of conjugates of K is $n_K = [S_2 \wr S_m : N(K)]$ the index of the normalizer of K. The element $(1,2)(3,4)(5,6)\cdots(2m-1, 2m)$ is in the center of $S_2 \wr S_m$ and not in K, so the normalizer of K is strictly larger than K by a factor of at least 2. Thus $n_K \leq 2^{m-1}$.

We now construct 2^{m-1} conjugates to prove that n_K is in fact equal to 2^{m-1}. Consider an element $g \in K$ with order m. As a permutation, g must be a double m-cycle since it preserves the block system with m blocks of size 2. Without loss of generality, $g = (1, 3, 5, \ldots, 2m-1)(2, 4, 6, \ldots, 2m)$. This double m-cycle corresponds to a partition of the $2m$ points into two sets of size m, namely $\{\{1, 3, 5, \ldots, 2m-1\}, \{2, 4, 6, \ldots, 2m\}\}$. Assume K has a different element h of order m that acts on the blocks in the same manner as g. Then gh^{-1} would be a nontrivial element of $K \cap S_2^m$ which contradicts K being a complement to S_2^m. Thus we can identify conjugates of K with the partition of the points into two sets of size m coming from the element tht acts on the blocks in the same manner as g.

We now count such partitions. Assume the point 1 is in the first set. Then 2 must be in the second set. For each of the $m-1$ remaining blocks, we have two choices, to put the first point with 1 and the second point with 2 or vice-versa. Thus there are 2^{m-1} such partitions which gives 2^{m-1} different conjugates of K. ■

7.1.6 The Lattice of Subgroups Lying Above a Complement

We apply the following theorem from Shareshian [19].

Theorem 37 *Let $G = NK$ with $N \lhd G$ and K a complement for N. Let $\mathcal{L}$ be the lattice of subgroups of N normalized by K. Then the lattice of subgroups between K and G is isomorphic to $\mathcal{L}$.*

Thus we only need to figure out what subgroups of S_2^m are normalized by a complement K. The answer turns out not to be dependent on the conjugacy class of complements K is chosen from but actually only on the parity of m.

Lemma 38 *Let K be a complement for S_2^m in $S_2 \wr S_m$. Let $\mathcal{L}$ be the lattice of subgroups inbetween K and $S_2 \wr S_m$. Then* $\mu(\mathcal{L}) = \begin{cases} 0 & \text{if } m \text{ is even} \\ 1 & \text{if } m \text{ is odd} \end{cases}$

Proof. Notice that S_2^m is in fact an m-dimensional vector space over the field with 2 elements. Thus any subgroup of S_2^m can be identified with the solutions of some linear equations in m variables $x_1, x_2, \ldots, x_m$. The action of K on such a subgroup via conjugation can be seen

as permuting the indices on these variables. Thus for a subgroup to be normalized by K, the system of equations must be completely invariant under any permutation of the indices. There are exactly four systems of equations with this property:

- No equations.
- $x_1 + x_2 + \cdots + x_m = 0$
- For all $i, j \in \{1, 2, \ldots, m\}$, $x_i + x_j = 0$
- For all $i \in \{1, 2, \ldots, m\}$, $x_i = 0$

Clearly the first and fourth correspond respectively to the maximal and minimal elements of this lattice. Additionally, the third is contained in the second if and only if m is even. Thus if m is even we have a totally ordered lattice with Möbius number zero, while if m is odd we have a Möbius number of 1.

■

7.1.7 Applying Crapo's Complement Theorem

We now apply Crapo's Complement Theorem to prove Theorem 34.

Proof. Let $\mathcal{K}$ be the set of all complements to the base group in $S_2 \wr S_m$. Applying Crapo's Complement Theorem to the subgroup S_2^m in $S_2 \wr S_m$ yields

$$\sum_{K \in \mathcal{K}} \mu(K)\mu(K, S_2 \wr S_m).$$

Notice that $\mu(K) = \mu(S_m)$ since $K \cong S_m$. By Lemma 38 $\mu(K, S_2 \wr S_m)$ is 0 or 1 depending on whether m is even or odd, respectively. By Lemma 36 and Lemma 35 there are exactly 2^m terms in the sum. Thus plugging directly into Crapo's Complement Theorem proves the result. ■

7.2 The Möbius Number of $S_3 \wr S_m$

Theorem 39 $\mu(S_3 \wr S_m) = \begin{cases} 0 & \text{if } m \text{ is even} \\ -6^m \mu(S_m) & \text{if } m \text{ is odd} \end{cases}$

We follow basically the same approach as to the proof of Theorem 34, however this time classifying complements is too complicated to do by studying orbits. Instead we use techniques from cohomology.

7.2.1 Classifying Complements to the Socle

There is one obvious complement to the socle. We use the following permutation representation:

$$S_3 \wr S_m = \left\langle \begin{array}{l} (1,2,3),(1,2),(1,4)(2,5)(3,6),(4,7)(5,8)(6,9),\ldots, \\ (2m-5,2m-2)(2m-4,2m-1)(2m-3,2m) \end{array} \right\rangle$$

We get corresponding representation for the socle:

$$C_3^m = \langle (1,2,3),(4,5,6),(7,8,9),\ldots,(2m-2,2m-1,2m) \rangle$$

We now construct a complement and count how many conjugates it has.

Lemma 40 *The following subgroup of $S_3 \wr S_m$ is a complement for the socle:*

$$S_2 \wr S_m = \left\langle \begin{array}{l} (1,2),(1,4)(2,5)(3,6),(4,7)(5,8)(6,9),\ldots, \\ (2m-5,2m-2)(2m-4,2m-1)(2m-3,2m) \end{array} \right\rangle$$

This group has exactly 3^m distinct conjugates, each of which is a complement.

Proof. An S_2 acting on each component will intersect trivially with the C_3 that acts on each component. The socle acts trivially on the blocks, so the full S_m acting on the blocks also intersects trivially with the socle. Thus $C_3^m \cap S_2 \wr S_m$ is trivial.

Together the S_2 and the C_3 generate all of S_3 on each component. Thus $\langle C_3^m, S_2 \wr S_m \rangle = S_3 \wr S_m$

Notice that $N_{S_3 \wr S_m}(S_2 \wr S_m) = S_2 \wr S_m$ since any element with a three-cycle on one of the blocks will conjugate an S_2 to a distinct two-cycle. The number of conjugates is the index of the normalizer which is $|S_3 \wr S_m|/|S_2 \wr S_m| = (6^m * m!)/(2^m * m!) = 3^m$.

■

We now use cohomology to show that there are no more conjugacy classes of complements. For a more detailed exposition regarding the following process, see Section IV.4 of [9]

We have the following homomorphism with the socle $= C_3^m$ as the kernel:

$$(1,2,3) \mapsto ()$$

$$(1,2) \mapsto (1,2)$$

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

$$(4,7)(5,8)(6,9) \mapsto (4,7)(5,8)(6,9)$$

$$\vdots$$

$$(2m-5,2m-2)(2m-4,2m-1)(2m-3,2m) \mapsto (2m-5,2m-2)(2m-4,2m-1)(2m-3,2m)$$

We have that $(S_3 \wr S_m)/C_3^m = S_2 \wr S_m$. We use the Coxeter presentation of this group: $S_2 \wr S_m = \langle x_1, x_2, x_3, \ldots, x_m : R \rangle$ where R consists of the following relators:

- x_i^2 for each $i \in \{1, 2, \ldots, m\}$
- $(x_1 x_2)^4$
- $(x_1 x_i)^2$ for each $i \in \{3, 4, \ldots, m\}$
- $(x_i x_j)^2$ for each $i \in \{2, 3, \ldots, m-2\}$ and $j \in \{i+2, i+3, \ldots, m\}$
- $(x_i x_{i+1})^3$ for each $i \in \{2, 3, \ldots, m-1\}$

$(1,2,3)$ is mapped to the identity so we don't need to consider it. However, we now consider all possible ways of pairing the other generators with elements from the normal subgroup. We give generators names:

$$x_1 = (1,2)$$

$$x_2 = (1,4)(2,5)(3,6)$$

$$x_3 = (4,7)(5,8)(6,9)$$

$$\vdots$$

$$x_m = (2m-5, 2m-2)(2m-4, 2m-1)(2m-3, 2m)$$

and note that any complement will be generated by elements of the form $x_1n_1, x_2n_2, x_3n_3, \ldots x_mn_m$ for some $n_1, n_2, \ldots n_m$ in the socle. Note also that the socle is a vector space. In particular we make the following identification:

$$(1,2,3) = [1,0,0,0,\ldots,0]$$

$$(4,5,6) = [0,1,0,0,\ldots,0]$$

$$(7,8,9) = [0,0,1,0,\ldots,0]$$

$$\vdots$$

$$(2m-2, 2m-1, 2m) = [0,0,0,\ldots,1]$$

Thus we get $m \times m$ matrices corresponding to the actions of $x_1, x_2, x_3, \ldots, x_m$ on the socle by conjugation:

$$x_1 \mapsto \begin{bmatrix} -1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$x_2 \mapsto \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$x_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$$

$$\vdots$$

$$x_m \mapsto \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}$$

We now use the fact that $x_1n_1, x_2n_2, x_3n_3, \ldots x_mn_m$ must satisfy the same relators that $x_1, x_2, x_3, \ldots x_m$ do to get restrictions on the possibilities for $n_1, n_2, n_3, \ldots n_m$. Call

$$n_1 = [n_{1,1}, n_{1,2}, n_{1,3}, \ldots, n_{1,m}]$$

$$n_2 = [n_{2,1}, n_{2,2}, n_{2,3}, \ldots, n_{2,m}]$$

$$n_3 = [n_{3,1}, n_{3,2}, n_{3,3}, \ldots, n_{3,m}]$$

$$\vdots$$

$$n_m = [n_{m,1}, n_{m,2}, n_{m,3}, \ldots, n_{m,m}]$$

First relator: x_1^2

$$(x_1n_1)^2 = x_1n_1x_1n_1 = x_1^2n_1^{x_1+1} = ()$$

which implies $[n_{1,1}, n_{1,2}, n_{1,3}, \ldots, n_{1,m}] \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 2 & 0 & \cdots & 0 \\ 0 & 0 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 2 \end{bmatrix} = [0, 0, 0, \ldots, 0]$

and thus we have that $n_2 = n_3 = \cdots = n_m = 0$.

Second through m^{th} relator: x_i^2 for $i \in \{2, 3, \ldots, m\}$

$$(x_in_i)^2 = x_in_ix_in_i = x_i^2n_i^{x_i+1} = ()$$

which implies $[n_{i,1}, n_{i,2}, \ldots, n_{i,m}] \begin{bmatrix} 2 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 2 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 2 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 & 2 \end{bmatrix} = [0, 0, \ldots, 0]$

so also

$$[2n_{i,1}, 2n_{i,2}, \ldots, 2n_{i,i-1}, n_{i,i} + n_{i,i+1}, n_{i,i} + n_{i,i+1}, \ldots, 2n_{i,m}] = [0, 0, \ldots, 0]$$

and thus we have that $n_{i,i+1} = -n_{i,i}$ and $n_{i,j} = 0$ for all other values of j.

Note at this point there are exactly m free variables, so the system can have at most 3^m solutions. Above we constructed 3^m complements, so we knew there were at least 3^m solutions. Thus the remaining relators impose no further restrictions on our solutions, and the only complements are exactly the 3^m complements we constructed above.

7.2.2 The Lattice of Subgroups Lying Above a Complement

We again apply Theorem 37.

Lemma 41 *Let K be a complement for C_3^m in $S_3 \wr S_m$. Let $\mathcal{L}$ be the lattice of subgroups inbetween K and $S_3 \wr S_m$. Then $\mu(\mathcal{L}) = -1$.*

Proof. Recall that C_3^m is in fact an m-dimensional vector space over the field with 3 elements. Thus any subgroup of C_3^m can be identified with the solutions of some linear equations in m variables $x_1, x_2, \ldots, x_m$. The action of K on such a subgroup via conjugation can be seen as permuting the indices on these variables (from the action of the S_m) and negating the variables (from the action of the S_2^m). Thus for a subgroup to be normalized by K, the system of equations must be completely invariant under any permutation of the indices and negation of variables. There are exactly two systems of equations with this property:

- No equations.
- For all $i \in \{1, 2, \ldots, m\}$, $x_i = 0$

These respectively correspond to all of C_3^m and the identity subgroup. Thus we have a Möbius number of -1.

■

7.2.3 Applying Crapo's Complement Theorem

We now apply Crapo's Complement Theorem to prove Theorem 39.

Proof. Let $\mathcal{K}$ be the set of all complements to the socle in $S_3 \wr S_m$. Applying Crapo's Complement Theorem to the subgroup C_3^m in $S_3 \wr S_m$ yields

$$\sum_{K \in \mathcal{K}} \mu(K)\mu(K, S_2 \wr S_m).$$

Notice that $\mu(K) = \mu(S_2 \wr S_m)$ since $K \cong (S_3 \wr S_m)/C_3^m \cong S_2 \wr S_m$. By Lemma **??** $\mu(K, S_2 \wr S_m)$ is -1. By Lemma 40 and Lemma 41 there are exactly 3^m identical terms in the sum. Theorem 34 computes the value of $\mu(S_2 \wr S_m)$. Plugging directly into Crapo's Complement Theorem proves the result. ■

7.3 Groups with Socle A_n^2

Notice that $S_n \wr S_2$ is isomorphic to $A_n^2 \rtimes D_8$. The groups between A_n^2 and $S_n \wr S_2$ thus correspond to the subgroups of D_8. In order for such a group to be transitive on $2n$ points (the kind we're interested in for computing the Möbius number of S_{2n}), it must contain the involution from D_8 that swaps the two copies of A_n. Only four subgroups of D_8 contain such an involution. Of those four, one of them is simply $A_n^2 \rtimes D_8 \cap A_{2n}$. Any subgroup contained in the alternating group gets thrown out of our computation by the trick presented to eliminate the alternating group in [12]. Thus there are only three relevant subgroups with above socle. These three subgroups are the subgroups we handle in the three subsections below.

7.3.1 The Möbius Number of $S_n \wr S_2$

We again apply Crapo's Complement Theorem to compute the Möbius Number of $S_n \wr S_2$ (Corollary 43), though this time in a simpler fashion. We prove a more general result where we produce a subgroup that has no complement in the subgroup lattice of $G \wr S_2$ for $G \leq S_m$ and $G \not\leq A_m$. This yields an empty sum in Crapo's Complement Theorem, giving the answer of zero.

Theorem 42 *Let $G \leq S_m$ and $G \not\leq A_m$. Then $\mu(G \wr S_2) = 0$.*

Proof. We show that $G \wr S_2$ has a subgroup H with no complement in $\mathcal{L}(G \wr S_2)$ and then apply Crapo's Complement Theorem.

Let $B_1 = \{1, 2, \ldots, m\}$ and $B_2 = \{m+1, m+2, \ldots, 2m\}$. Let G_1 be the first copy of G in the wreath product and G_2 be the second copy of G in the wreath product, where G_1 permutes B_1 and G_2 permutes B_2. Thus every element of $G \wr S_2$ can be written as $g_1 g_2 g$ where $g_1 \in G_1$, $g_2 \in G_2$, and $g \in \{(), (1, m+1)(2, m+2)\cdots(m, 2m)\}$. That is, $\langle g \rangle$ is the S_2 being used in the wreath product. Let

$$H = \{g_1 g_2 : g_1 \in G_1,\ g_2 \in G_2,\ \text{and}\ \operatorname{sgn}(g_1) = \operatorname{sgn}(g_2)\}.$$

We see that H is a subgroup of $G \wr S_2$, since if $g_1 g_2,\ h_1 h_2 \in H$, then $\operatorname{sgn}(g_1) = \operatorname{sgn}(g_2)$ and $\operatorname{sgn}(h_1) = \operatorname{sgn}(h_2)$ so $\operatorname{sgn}(g_1 h_1) = \operatorname{sgn}(g_1) + \operatorname{sgn}(h_1) = \operatorname{sgn}(g_2) + \operatorname{sgn}(h_2) = \operatorname{sgn}(g_2 h_2)$. Alternatively, one can see that $H \leq G \wr S_2$ by noticing that $H = (G_1 \times G_2) \cap A_{2n}$. Readers familiar with subdirect products will notice that H is simply the subdirect product of G with itself with respect to the epimorphism $\operatorname{sgn} : G \to S_2$.

Assume $K \leq G \wr S_2$ and K complements H in $\mathcal{L}(G \wr S_2)$. That is, $HK = G \wr S_2$ and $H \cap K = \langle() \rangle$. First notice that since $K \leq G \wr S_2$, every element of K is of the form $k_1 k_2 k$, where $k_1 \in G_1, k_2 \in G_2$, and $k \in \{(), (1, m+1)(2, m+2)\cdots(m, 2m)\}$. We now make the key claim in the proof:

$$\exists k_1 k_2 k \in K,\ \operatorname{sgn}(k_1) \neq \operatorname{sgn}(k_2)\ \text{and}\ k \neq () \tag{7.1}$$

To prove this claim, first assume $\forall g_1 g_2 g \in K,\ \mathrm{sgn}(g_1) = \mathrm{sgn}(g_2)$. Then $\forall g_1 g_2 g \in HK,\ \mathrm{sgn}(g_1) = \mathrm{sgn}(g_2)$. However, since $G_1 \not\leq A_m$, $\exists r \in G_1$ with r odd. Also, $() \in G_2$ and $()$ is even. Thus $r() = r \in G \wr S_2$ but $\mathrm{sgn}(r) \neq \mathrm{sgn}()$. Therefore $r \notin HK$, so $HK \neq G \wr S_2$, which contradicts K being a complement to H. Thus $\exists g_1 g_2 g \in K,\ \mathrm{sgn}(g_1) \neq \mathrm{sgn}(g_2)$.

Next assume $\forall h_1 h_2 h \in K$, $h = ()$. Then $K \leq G_1 \times G_2$ so $HK \leq G_1 \times G_2$, so $HK \neq G \wr S_2$, which contradicts K being a complement to H. Thus $\exists h_1 h_2 h \in K,\ h \neq ()$.

Case 1: $\mathrm{sgn}(h_1) \neq \mathrm{sgn}(h_2)$. In this case, the element $h_1 h_2 h$ satisfies (7.1).

Case 2: $g \neq ()$. In this case, the element $g_1 g_2 g$ satisfies (7.1).

Case 3: $\mathrm{sgn}(h_1) = \mathrm{sgn}(h_2)$ and $g = ()$. In this case, the element $g_1 g_2 g h_1 h_2 h = g_1 g_2 h_1 h_2 h = (g_1 h_1)(g_2 h_2) h$ satisfies (7.1), since $\mathrm{sgn}(h_1) = \mathrm{sgn}(h_2)$ and $\mathrm{sgn}(g_1) \neq \mathrm{sgn}(g_2)$ implies that $\mathrm{sgn}(g_1 h_1) \neq \mathrm{sgn}(g_2 h_2)$, and $h \neq ()$.

Thus in every case, we have that $\exists k_1 k_2 k \in K,\ \mathrm{sgn}(k_1) \neq \mathrm{sgn}(k_2)$ and $k \neq ()$. Now consider $U = \left\langle (k_1 k_2 k)^2 \right\rangle$. Clearly $U \leq K$ since $(k_1 k_2 k)^2 \in K$. Notice that $k = k^{-1}$ and $k k_1 k \in G_2$ and $k k_2 k \in G_1$, since we are conjugating by k. Thus we compute

$$\begin{aligned}
(k_1 k_2 k)^2 &= k_1 k_2 k k_1 k_2 k \\
&= k_1 k_2 k k_1 (kk) k_2 k \\
&= k_1 k_2 (k k_1 k)(k k_2 k) \\
&= (k_1 (k k_2 k))(k_2 (k k_1 k)).
\end{aligned}$$

We see that $k_1 (k k_2 k) \in G_1$ is odd, since $\mathrm{sgn}(k_1) \neq \mathrm{sgn}(k_2)$, and similarly $k_2 (k k_1 k) \in G_2$ is odd. Thus $\mathrm{sgn}(k_1 (k k_2 k)) = \mathrm{sgn}(k_2 (k k_1 k))$, so $(k_1 k_2 k)^2 \in H$.

Thus $U \leq H \cap K$. However, since $k_1 (k k_2 k) \in G_1$ and $k_2 (k k_1 k) \in G_2$ are odd, $(k_1 k_2 k)^2 \neq ()$. Thus U is a nontrivial subgroup of $H \cap K$, which is a contradiction.

Therefore H does not have a complement in $\mathcal{L}(G \wr S_2)$, so $\mu(G \wr S_2) = 0$. ■

Thus as a corollary we have:

Corollary 43 *$\mu(S_n \wr S_2) = 0$ for all $n \geq 1$.*

7.3.2 The Möbius Number of $A_n \wr S_2$

Here we compute the Möbius number of $A_n \wr S_2$, an important index 4 subgroup of $S_n \wr S_2$. It is very surprising that the values are nonzero and do not depend on the Möbius number of A_n, but rather it is a simple explicit formula in terms of n. No such simple formula is known for the Möbius number of A_n.

We begin by classifying complements to the socle. We find there is a unique conjugacy class of complements with $n!/2$ complements.

Lemma 44 *There is a unique conjugacy class of complements to $A_n \times A_n$ in $A_n \wr S_2$ isomorphic to S_2. There are $n!/2$ complements in this conjugacy class.*

Proof.

Since $A_n \times A_n$ is normal in $A_n \wr S_2$, every complement is isomorphic to the quotient, which is just S_2. We take the obvious permutation representation on $2n$ points, where elements a_1 and a_2 generate A_n on $\{1, 2, \ldots n\}$ and

$$g = \langle (1, n+1)(2, n+2) \cdots (n, 2n) \rangle$$

so we have

$$A_n \wr S_2 = \langle a_1, a_2, g \rangle$$

.

Clearly $\langle g \rangle$ is a complement. Consider another complement K. It must be generated by some element k with:

$$k = \langle (1, a_{n+1})(2, a_{n+2}) \cdots (n, a_{2n}) \rangle$$

where

$$\{a_{n+1}, a_{n+2}, \ldots a_{2n}\} = \{n+1, n+2, \ldots 2n\}$$

since k must be of order 2 and swap the blocks. Thus k is conjugate to g by some element of S_n acting on $\{n+1, n+2, \ldots 2n\}$. Call this conjugating element c. Thus we have $c^{-1}kc = g$. By closure under conjugation, kg must be in $A_n \wr S_2$. Notice

$$kg = kc^{-1}kc = (kc^{-1}k)c$$

which is in the base group. Thus c is in A_n and not just S_n, so any two complements are conjugate.

Notice the element g is centralized by g itself as well as any element of the form aa^g for $a \in A_n$. Thus we have that the centralizer of g has $2n!/2$ elements, and thus this centralizer has index $n!/2$ since the group order is $2n!^2$. Thus there are exactly that many complements.

■

Next we study the sublattice of $A_n \times A_n$ normalized by the S_2 described above. We write $A_n \underset{\phi}{\wr} A_n$ as a shorthand for the diagonal subdirect product of A_n with itself, constructed using ϕ as the automorphism. We write $A_n \underset{g}{\wr} A_n$ as a shorthand for the diagonal subdirect product of A_n with itself, constructed using conjugation by $g \in S_n$ as the automorphism.

Lemma 45 *Let $A_n \underset{\phi}{\wr} A_n$ be a diagonal subdirect product contained in $A_n \times A_n$. Let S_2 be the complement to the base group in the wreath product described above. Then $A_n \underset{\phi}{\wr} A_n$ is normalized by S_2 if and only if ϕ has order 2.*

Proof. Note that $A_n \underset{\phi}{\wr} A_n = \left\{\left(g, g^\phi\right) : g \in A_n\right\}$. Assume $A_n \underset{\phi}{\wr} A_n$ is in fact normalized by S_2. Conjugation by the generator of S_2 swaps the coordinates of $A_n \times A_n$ and any of its subgroups. Thus we have

$$\left\{\left(g, g^\phi\right) : g \in A_n\right\} = \left\{\left(g^\phi, g\right) : g \in A_n\right\}$$

Since ϕ permutes the elements of A_n, we can reindex the set on the right, replacing g by g^ϕ.

$$\left\{\left(g, g^\phi\right) : g \in A_n\right\} = \left\{\left(g^{\phi\circ\phi}, g^\phi\right) : g \in A_n\right\}$$

which shows we must in fact have $\phi \circ \phi$ equal to the identity map.

■

Additionally, the following combinatorial lemma from [20] will prove useful.

Lemma 46 *[20] If the intersection of all maximal elements of a lattice is not the minimum element of the lattice, the lattice Möbius number is zero.*

We are now ready to prove the theorem.

Theorem 47 $\mu(A_n \wr S_2) = \begin{cases} 6!^2/2 & \text{if } n = 6 \\ (-1)^n \frac{n!^2}{4} & \text{if } n \neq 6 \end{cases}$

Proof.

We apply Crapo's Complement Theorem to the socle. Lemma 44 classifies the complements. An easy computation shows $\mu(S_2) = -1$. Thus we have

$$\mu(A_n \wr S_2) = (-1)\frac{n!}{2}\mu(S_2, A_n \wr S_2)$$

Applying Theorem 37, we can compute $\mu(S_2, A_n \wr S_2)$ by computing the Möbius number of the sublattice of $A_n \times A_n$ normalized by S_2. For notational convenience, for any subgroup H of $A_n \times A_n$, write $\mathcal{L}_N(H)$ to denote the sublattice of H normalized by S_2. Rephrasing above, we have $\mu(S_2, A_n \wr S_n) = \mu(\mathcal{L}_N(A_n \times A_n))$.

To do this, we apply a closure operation to $\mathcal{L}_N(A_n \times A_n)$. Let π_1 and π_2 be the projection maps onto the first and second factors, respectively. Then our closure operation is $\overline{H} = \pi_1(H) \times \pi_2(H)$. That is, we map to the direct product of the projections onto each factor.

We apply the closure theorem to this operation. The quotient lattice consists of the subgroups that were already just direct products. Since these subgroups had to be normalized by the S_2, they must be the same on each factor. Thus we have that the quotient lattice is isomorphic to the subgroup lattice of A_n. We also must analyze what gets mapped to the full group $A_n \times A_n$ under this closure operation. Of course $A_n \times A_n$ itself does. Besides this, for a subgroup to get mapped to the top requires that the projections onto each factor are isomorphic to A_n, so the group must be a diagonal subdirect product of A_n with itself.

We now enumerate based on different cases of diagonal subdirect products of A_n with itself, as the automorphism used in building the subdirect product will affect the outcome. Notice that the automorphism must be of order one or two as explained by Lemma 45.

i) Identity: Here the sublattice consists of diagonal subdirect products of every subgroup of A_n. Thus the lattice is isomorphic to the sublattice of A_n.

ii) Conjugation by a two-cycle: In this case, we again apply a closure operation. The two points swapped by the two cycle must lie in the same orbit. Thus if we apply the closure operation that replaces a permutation group by its orbits, we get the partition lattice on $n-1$ points as the quotient lattice. This has Möbius number $(-1)^{n-2}(n-2)!$ by the formula for the Möbius number of the partition lattice (see for example [20, Example 3.10.4] or [12]. Nothing gets mapped to$A_n \times A_n$ under this closure operation except itself. Thus in this case $\mathcal{L}_N(A_n \underset{g}{\curlywedge} A_n) = (-1)^{n-2}(n-2)!$.

iii) Conjugation by an element of order two that is a product of multiple disjoint two-cycles: Let g be the element of order two that we are conjugating by. Then in $\mathcal{L}_N(A_n \underset{g}{\curlywedge} A_n)$, the intersection of all the maximal elements contains $< g >$. This is because if we have some $H \in \mathcal{L}_N(A_n \underset{g}{\curlywedge} A_n)$ that does not contain g, then H is a proper normal subgroup of $< H, g >$, which cannot be equal to A_n since A_n is simple. Thus this has Möbius number zero by Lemma 46.

Thus $\mathcal{L}_N(A_n \times A_n) = \frac{n!}{2}$, which completes the proof. ■

7.3.3 The Möbius Number of $\frac{1}{2}\left[S_n^2\right]2$ for Even n

The group $\frac{1}{2}\left[S_n^2\right]2$, is an index 2 subgroup of $S_n \wr S_2$ defined as follows. Let h_1 and h_2 generate A_n on $\{1, 2, \ldots, n\}$, and let

$$h_3 = (1, n+1, 2, n+2)\,(3, n+3)\,(4, n+4)\cdots(n, 2n)\,.$$

Then we define $\frac{1}{2}\left[S_n^2\right]2 = \langle h_1, h_2, h_3 \rangle$, an index 2 subgroup of $S_n \wr S_2$. Notice that this group is just a direct product of A_n with itself, except every time the components are switched using the element h_3, the sign of the permutation of the second component is also switched.

Theorem 48 *If n is even, $\mu\left(\frac{1}{2}\left[S_n^2\right]2\right) = 0$.*

Proof. We show that $\frac{1}{2}\left[S_n^2\right]2$ satisfies the hypothesis of Lemma 11 for even n.

Let $h = (1, n+1)(2, n+2)(3, n+3)(4, n+4)\cdots(n, 2n)$. Thus h is even, so h_3 is odd since $h_3 = (n+1, n+2)\,h$. Thus $\frac{1}{2}\left[S_n^2\right]2 \not\leq A_{2n}$.

We now must show that $\frac{1}{2}\left[S_n^2\right]2$ does not contain an odd involution. First notice $\frac{1}{2}\left[S_n^2\right]2 \leq S_n \wr S_2$, since $\{h_1, h_2, h_3\} \subseteq S_n \wr S_2$. Thus every element of $\frac{1}{2}\left[S_n^2\right]2$ can be written in the form $g_1 g_2 g$ where g_1 permutes $\{1, 2, \ldots, n\}$, g_2 permutes $\{n+1, n+2, \ldots, 2n\}$, and $g \in \{h, ()\}$. That is, $\langle g\rangle$ is the S_2 being used in the wreath product. Define the following sets:

$$\begin{aligned} A &= \left\{ g_1 g_2 g \in \frac{1}{2}\left[S_n^2\right]2 : \operatorname{sgn}(g_1) = \operatorname{sgn}(g_2) \text{ and } g = () \right\} \\ B &= \left\{ g_1 g_2 g \in \frac{1}{2}\left[S_n^2\right]2 : \operatorname{sgn}(g_1) \neq \operatorname{sgn}(g_2) \text{ and } g = h \right\} \end{aligned}$$

Notice that $h_3 \in B$ and $\{(), h_1, h_2\} \subseteq A$. For any $a \in A$, $ah_1 \in A$, $ah_2 \in A$, and $ah_3 \in B$. For any $b \in B$, $bh_1 \in B$, $bh_2 \in B$, and $bh_3 \in A$. Thus $\frac{1}{2}\left[S_n^2\right]2 \subseteq A \cup B$. If $g_1 g_2 g \in A$, then $g_1 g_2 g = g_1 g_2$ so $g_1 g_2 g$ is even since $\operatorname{sgn}(g_1) = \operatorname{sgn}(g_2)$. Thus A cannot contain an odd involution. If $g_1 g_2 g \in B$, then $g_1 g_2 g = g_1 g_2 h$. Thus

$$\begin{aligned} \left(g_1 g_2 h\right)^2 &= g_1 g_2 h g_1 g_2 h \\ &= g_1 g_2 \left(h g_1 h\right)\left(h g_2 h\right) \\ &= g_1 \left(h g_2 h\right) g_2 \left(h g_1 h\right). \end{aligned}$$

Since $\operatorname{sgn}(g_1) \neq \operatorname{sgn}(g_2)$, we have $g_1\left(h g_2 h\right)$ and $g_2\left(h g_1 h\right)$ are odd elements acting on $\{1, 2, \ldots, n\}$ and $\{n+1, n+2, \ldots, 2n\}$ respectively. Thus $\left(g_1 g_2 h\right)^2 \neq ()$, so $g_1 g_2 h$ is not an involution, so B cannot contain an odd involution. Since $\frac{1}{2}\left[S_n^2\right] 2 \subseteq A \cup B$ and neither A or B contain an odd involution, $\frac{1}{2}\left[S_n^2\right]2$ doesn't contain an odd involution. ■

Note that in the proof above, $\frac{1}{2}\left[S_n^2\right]2$ is in fact equal to $A \cup B$.

Also note that we do not yet have a general description of what happens in this case for odd n. Such a theorem would be very useful for future Möbius number computations.

7.4 A Corollary Regarding Complementation in Subgroup Lattices

Corollary 49 *For the following families of groups, every subgroup of those has a complement.*

$$S_2 \wr S_m$$
$$S_3 \wr S_m$$
$$A_n \wr S_2$$

where m is any odd positive integer and n is any positive integer.

Corollary 49 follows immediately from Theorem 34 and Crapo's Complement Theorem, since if there existed a subgroup $H \leq S_2 \wr S_m$ without a complement, applying Crapo's Complement Theorem would imply $\mu(S_2 \wr S_m) = 0$. However for m odd, it is not zero.

Chapter 8

Towards the Möbius Number of S_{18}

As stated above, to compute the Möbius Number of S_{18}, we need only to look at the proper transitive subgroups via Equation (1) in Section 4.1. Primitive groups (including A_{18}) are easily handled separately. Among the transitive subgroups of degree 18, we can look at things case-by-case, broken up according to block size. Any group of block size 2 or 3 has a solvable radical and can be handled in the same manner as the theorems presented in Sections 7.1 and 7.2. A group with block size 9 has at most an S_2 acting on the blocks, which greatly simplifies the structure of such a group. Thus ad-hoc techniques including the ones used in Section 7.3 can handle these groups. What remains are the groups with block size 6. All of these are subgroups of $S_6 \wr S_3$. A computer computation is underway to compute all subgroups of this group. Once this terminates, it will be possible to get the Möbius numbers of the remaining subgroups. At this point we will have the Möbius number of S_{18}, which is the smallest currently unknown value.

Chapter 9

Future Work

Though explained in the other sections, here is a short summary of the major goals of the research, the techniques proposed, and why these look promising.

The ultimate goal would be to compute $\mu(S_n)$ for all n. This would fully settle this problem which Pahlings, Stanley, and Shareshian have worked on. These new techniques proposed here may yield some infinite families, which would be significant progress. At the very least, some more small values of n for which $\mu(S_n)$ has not been computed will certainly fall, for example $n = 18, 20, 24, 28, 30, \ldots$. All of this would be new work; since Shareshian's infinite families there has been no further progress on this question.

We first use the socle formula as a stepping stone to get Möbius numbers of wreath products (eventually we need the 2-closed Möbius numbers, but once we have the Möbius numbers we should be able to obtain the 2-closed Möbius numbers via the Closure Theorem on the 2-closure operation). This should be feasible since typically a wreath product is "mostly" socle.

Next, we continue to classify transitive 2-closed wreath products by figuring out what subgroups of wreath products can be 2-closed as well as showing that a wreath product of two 2-closed groups is again 2-closed, proving Conjecture 17. This should yield a description of what transitive 2-closed groups can occur for various degrees. Given how many of the transitive 2-closed subgroups of S_{18} fit into this category, it is reasonable that this approach will describe many or all of the transitive 2-closed subgroups for other degrees as well.

We then continue to compute 2-closed Möbius numbers of the transitive 2-closed groups.

Many more results like Theorem 18 should be feasible, especially since GAP computations and current results seem to indicate that the 2-closed Möbius numbers seem to come out "easier" than Möbius numbers. The family of groups in Theorem 18 are a perfect example; no formula is known for their Möbius numbers but the 2-closed Möbius numbers just come out to be zero.

With the above values of 2-closed Möbius numbers, we can compute the 2-closed Möbius number of the symmetric group of degree n for as many n as possible via the Closure Theorem on the 1-closure operation being applied to the lattice of 2-closed subgroups. This will certainly happen for some previously intractable small values and hopefully for infinite families or even all n.

We then obtain the Möbius numbers of the doubly-transitive groups that arise, and determine where the doubly-transitive groups occur. Since these are fully classified, knowing which doubly-transitive groups occur in what degree will not be an issue. Computing the Möbius numbers should be feasible as well, at least in some cases. For example in degree 18, $PSL(2,13)$ and $PGL(2,13)$ are the only two doubly-transitive groups that are not symmetric or alternating. Both of these groups are linear groups of dimension two, which have already had their Möbius numbers computed in [18].

Finally, we use the 2-closed Möbius number of S_n along with the Möbius numbers of the doubly-transitive groups to compute the Möbius number of S_n via the Closure Theorem on the 2-closure operation (though $\mu(A_n)$ will come up as well, we can handle A_n in a manner similar to S_n or use some ad-hoc arguments to deal with it).

Additionally, future progress is possible without the use of 2-closures. This is the direction of Section 7. By obtaining the Möbius numbers of large families of imprimitive groups using the complement theorem, one may get more milage out of simply reducing to transitive groups instead of doubly-transitive. There are currently some large computations running that when coupled with the results of Section 7 will soon yield the Möbius number of S_{18}, as discussed at the end of Section 7.

REFERENCES

[1] Joe Bohanon. Personal communication.

[2] Kenneth S. Brown. The coset poset and probabilistic zeta function of a finite group. *J. Algebra*, 225:989–1012, 1999.

[3] A. R. Calderbank, P. Hanlon, and R. W. Robinson. Partitions into even and odd block size and some unusual characters of the symmetric groups. In *Proc. London Math. Soc*, pages 288–320, 1986.

[4] Peter J. Cameron. Finite permutation groups and finite simple groups. *Bull. London Math. Soc.*, 13(1):1–22, 1981.

[5] Henry H. Crapo. The Möbius function of a lattice. *J. Combinatorial Theory*, 1:126–131, 1966.

[6] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[7] Philip Hall. The eulerian functions of a group. *Quart. J.Math*, 7:134–151, 1936.

[8] Alexander Hulpke. Constructing transitive permutation groups. *J. Symbolic Comput.*, 39(1):1–30, 2005.

[9] Alexander Hulpke. *Notes on Computational Group Theory.* http://www.math.colostate.edu/ hulpke/CGT/cgtnotes.pdf. 2010.

[10] OEIS Foundation Inc. The on-line encyclopedia of integer sequences. *oeis.org*, 2011.

[11] Charles Kratzer and Jacques Thévenaz. Fonction de Möbius d'un groupe fini et anneau de Burnside. *Comment. Math. Helv.*, 59(3):425–438, 1984.

[12] Kenneth M Monks. The Möbius number of the symmetric group of degree 12. Master's thesis, Colorado State University, 2008.

[13] H. Pahlings. Character polynomials and the Möbius function. *Arch. Math. (Basel)*, 65(2):111–118, 1995.

[14] Marko Petkovsek, Donald E. Knuth, Doron Zeilberger, and Herbert Wilf. *A=b*. 1997.

[15] Cheryl E. Praeger and Jan Saxl. On the orders of Primitive Permutation Groups. *Bull. London Math. Soc.*, 12(4):303–307, 1980.

[16] L. Pyber. Asymptotic results for permutation groups. In L. Finkelstein and W. M. Kantor, editors, *Groups and computation: Proceedings of the DIMACS Workshop held at Rutgers University. New Brunswick, United States of America, 07/Oct/1991-10/Oct/1991*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science; 11, pages 197–219. American Mathematical Society, 1991.

[17] L. Pyber and A. Shalev. Asymptotic results for primitive permutation groups. *Journal of Algebra*, 188(1):103 – 124, 1997.

[18] John Shareshian. *Combinatorial Properties of Subgroup Lattices of Finite Groups*. PhD thesis, Rutgers University, 1996.

[19] John Shareshian. On the Möbius number of the subgroup lattice of the symmetric group. *Journal of Combinatorial Theory, Series A*, 78(2):236 – 267, 1997.

[20] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[21] Helmut Wielandt. *Mathematical Works: Permutation groups through invariant relations and invariant functions*, volume 1, 237 – 296. de Gruyter 1998, taken from Lecture Notes from Ohio State University 1969.