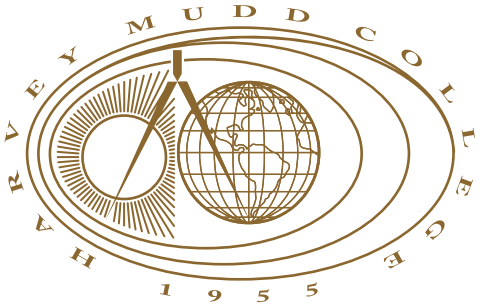
2003

An Eigenspace Approach to Isotropic Projections for Data on Binary Trees

Nate Eldredge
Harvey Mudd College



An Eigenspace Approach to Isotypic Projections for Data on Binary Trees

by
Nathaniel Eldredge
Michael E. Orrison, Advisor

Advisor: _____

Second Reader: _____

(Shahriar Shahriari)

May 2003

Department of Mathematics

HARVEY MUDD
COLLEGE

Abstract

An Eigenspace Approach to Isotypic Projections for Data on Binary Trees

by Nathaniel Eldredge

May 2003

The classical Fourier transform is, in essence, a way to take data and extract components (in the form of complex exponentials) which are invariant under cyclic shifts. We consider a case in which the components must instead be invariant under automorphisms of a binary tree. We present a technique by which a slightly relaxed form of the generalized Fourier transform in this case can eventually be computed using only simple tools from linear algebra, which has possible advantages in computational efficiency.

Table of Contents

List of Tables

Acknowledgments

My deepest thanks go to my advisor, Prof. Michael Orrison, for his constant and invaluable input into this project. I would also like to thank Prof. Shahriar Shahriari for acting as second reader. David Uminsky and Ross Richardson provided excellent advice on many issues, large and small, as well as general encouragement throughout the thesis process. Finally, John Cloutier contributed some very useful advice on a talk I gave about this project.

Chapter 1

Introduction

1.1 The Fourier transform

The Fourier transform is known to most scientists and engineers as a tool for data analysis. Given a signal, the classical Fourier transform recovers its spectrum, which describes how the signal can be broken into sines and cosines, or, equivalently, complex exponentials. In the discrete case, where the signal consists of a finite number of data points, there are well-known computational techniques for this; most notable is the discrete fast Fourier transform (FFT) algorithm due to Cooley and Tukey [4]. The FFT allows the Fourier transform to be computed efficiently, and has become an extremely important tool for digital signal processing in fields ranging from physics and engineering to electronic music.

However, complex exponentials are not the only "pieces" into which we might wish to decompose a signal. The crucial feature of functions like e^{it} is that they are in a sense invariant under translation; shifting t changes the function only by a (complex) constant multiple. So the classical Fourier transform extracts from the signal components which fit nicely into this translational structure. But there are other sorts of structure we might seek. In fact, this structure can be described by a group, and the idea of the Fourier transform generalizes to cover the case of an arbitrary group. Unfortunately, though, if computational efficiency is needed, more work must be done. Although the Cooley-Tukey FFT algorithm can be generalized to some extent (see for instance [18]), for many groups, efficient Fourier transform

algorithms are not obvious or not known.

The Fourier transform can be thought of as a change of basis; in fact, this is how it is often characterized in analysis. In essence, we are decomposing our signal space into one-dimensional subspaces, and looking at the components of the signal that lie in these subspaces. In some cases, it can be helpful if we relax this condition somewhat, and decompose the signal into larger components which nevertheless retain the important structural information we seek. This is the idea of isotypic projections, which we discuss in Chapter 2.

1.2 Eigenspaces and our approach

One disadvantage of generalizations the Cooley-Tukey FFT is that it relies heavily on algebraic facts about the group involved, making it rather complicated to implement. We shall describe an approach to isotypic projections which relies on straightforward techniques from linear algebra. In particular, it can be possible to compute isotypic projections with respect to some group via an algorithm for eigenspace projections, if the appropriate eigenspaces are used. The goal, then, is to find a "separating set" of simultaneously diagonalizable linear transformations whose eigenspaces are the subspaces we seek. Chapter 3 explains the details of this approach. Of course, finding such a set will necessarily require an algebraic understanding of the group in question; but once it is found, implementation of the projection algorithm becomes elementary.

We will be working with the automorphism groups of binary trees, to be described in Chapter 4. These groups are of interest for several tasks in signal processing; see for instance Section 4.4, as well as [9] and [25]. In addition, the decomposition of their signal spaces has interesting combinatorial properties; see Section 4.3 and [22].

1.3 Previous work

The idea of using eigenspaces to compute isotypic projections was explored in detail in [23]. Its inspiration comes from the one of the myriad properties of the Jucys-Murphy elements from the symmetric group (Section 3.5 and [6]), which can be applied for just this purpose. Generalizations of these elements exist ([6], [21], [24]), but by no means have they been generalized to all groups.

Much is known about the structure of the automorphism groups of binary trees, and wreath product groups in general (see Section 4.2). Their representation theory is examined in [16] and [17], and more recently a combinatorial approach to the more specific case of iterated wreath products of cyclic groups is in [22]. Spectral analysis on these groups has been considered in [9] and [25], with applications to signal and image processing.

Computational details about the linear algebra involved have also been considered. [23] gives bounds on the computational complexity of using separating sets for several groups. [20] presents an important optimization in the case of the symmetric group, which is generalized in [1].

1.4 Structure of this paper

In Chapter 2 we review necessary concepts and facts from the representation theory of finite groups. Chapter 3 discusses the "eigenspace approach" to isotypic projections, through which the necessary computations for isotypic projections can be done using simple linear algebra tools. Chapter 4 describes the automorphism groups with which we shall concern ourselves. Finally, Chapter 5 constructs some separating sets for small cases.

Chapter 2

Representation Theory

In this chapter we give a review of the necessary elements of representation theory that are needed to read this paper, and lay out the terminology and notation we shall use. An excellent introduction to the subject is [14]. For readers already acquainted with representation theory, the first chapter of [26] has a good concise review. [8] is a very complete reference for any unfamiliar concepts from group theory.

2.1 Group representations

Representation theory is, in essence, the idea of expressing abstract algebra in terms of linear algebra. Operations in a group are transformed into operations in a vector space.

Let G be a finite group.

Definition 2.1.1. A G**-module** or **representation** of G is a finite-dimensional complex vector space V on which G acts linearly. That is, for any $g, h \in G$, $\mathbf{v}, \mathbf{w} \in V$, and $\alpha, \beta \in \mathbb{C}$, we have:

1. $g\mathbf{v}$ is some element of V;
2. If e is the identity of G, then $e\mathbf{v} = \mathbf{v}$;
3. $g(h\mathbf{v}) = (gh)\mathbf{v}$ (1, 2, and 3 together define an action of G on V);
4. $g(\alpha\mathbf{v} + \beta\mathbf{w}) = \alpha(g\mathbf{v}) + \beta(g\mathbf{w})$ (the action respects the linear structure of V).

What we have, then, is that each $g \in G$ becomes a linear transformation of V, and these transformations compose in the same way that elements of G multiply. Since elements of G have inverses, so do these transformations. So we can also think of this correspondence as a homomorphism φ from G to $GL(V)$, the set of invertible linear transformations of V. (Many authors use the word "representation" to refer to this homomorphism instead of the corresponding module.)

Once a basis for V is fixed, each $\varphi(g)$ can be represented as an $n \times n$ matrix, where $n = \dim V$. By taking the traces of these matrices, we obtain the **character** χ corresponding to φ, defined by $\chi(g) = \operatorname{tr} \varphi(g)$. Since similar matrices have the same trace (that is, $\operatorname{tr} ABA^{-1} = \operatorname{tr} B$), we see that the character is independent of the basis chosen for V. In fact, two representations have the same character if and only if they are isomorphic. Also, $\chi(ghg^{-1}) = \operatorname{tr}[\varphi(g)\varphi(h)\varphi(g)^{-1}] = \operatorname{tr} \varphi(h) = \chi(h)$, so that χ takes the same value on conjugate elements of G. A function $f : G \to \mathbb{C}$ with this property is called a **class function**, since it can be considered a function on the set of conjugacy classes of G.

We now consider how modules decompose.

Definition 2.1.2. Let V be a G-module. A subspace $U \subset V$ is a **submodule** of V if for each $g \in G$, $\mathbf{u} \in U$, we have $g\mathbf{u} \in U$ (that is, U is closed under the action of G). We say V is **irreducible** if it has no submodules other than the trivial one $\{\mathbf{0}\}$ and itself.

Irreducible modules are the most fundamental modules, as is shown by the following central theorem.

Theorem 2.1.3 (Maschke's Theorem). *If V is a nontrivial G-module, then we can write*

$$V = W_1 \oplus \cdots \oplus W_k$$

where $W_1, \ldots, W_k$ are irreducible G-modules.

In other words, every G-module can be decomposed into irreducible modules. See [26] for a proof.

Using characters, we can say more about this decomposition.

Definition 2.1.4. Let χ and ψ be characters associated to representations of G. Define the **inner product** $\langle \chi, \varphi \rangle$ by

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}. \tag{2.1}$$

Theorem 2.1.5. *Let V be a representation of G, with associated character χ, which decomposes into irreducible submodules as*

$$V = m_1 W_1 \oplus m_2 W_2 \oplus \cdots \oplus m_k W_k$$

where $m_i W_i$ denotes the direct sum of m_i copies of W_i, and the W_i are pairwise nonisomorphic. If χ_i is the character associated with W_i, then

$$\langle \chi, \chi_i \rangle = m_i. \tag{2.2}$$

It also can be shown that irreducible characters are orthonormal with respect to this inner product. Using this fact, it is possible to show that the set of irreducible characters forms a basis for the space of all class functions on G. As the dimension of this space is equal to the number of conjugacy classes of G, we have the following theorem:

Theorem 2.1.6. *The number of irreducible representations of G is equal to the number of conjugacy classes of G.*

Now, when decomposing a representation into irreducible submodules, it may happen that some of these submodules are isomorphic to each other. In this case, the decomposition is not unique; in fact, there are infinitely many ways to write such a decomposition. To remedy this defect, we introduce the notion of an **isotypic** submodule, which is simply the direct sum of one isomorphism class of irreducible submodules of V. In other words, given one irreducible submodule, we

collect together all the irreducible submodules isomorphic to it into one larger subspace. When this is done, the decomposition is in fact unique.

Theorem 2.1.7. *If V is a nontrivial G-module, then there is a decomposition*

$$V = W_1 \oplus \cdots \oplus W_k$$

where $W_1, \ldots, W_k$ are isotypic G-modules. Furthermore, this decomposition is unique up to ordering.

2.2 Examples

Now let us see some examples of representations.

Example 2.2.1 (The permutation representation). Suppose G acts on a finite set S with n elements. Let $\mathbb{C}S$ be the set of all formal linear combinations $\sum_{i=1}^{n} a_i s_i$, where $a_i \in \mathbb{C}$, $s_i \in S$. With componentwise addition and scalar multiplication, $\mathbb{C}S$ becomes a vector space. Then we can make $\mathbb{C}S$ into a G-module by defining

$$g \sum_{i=1}^{n} a_i s_i = \sum_{i=1}^{n} a_i (g s_i).$$

This is called the **permutation representation** of G corresponding to its action on S.

Example 2.2.2 (The regular representation). If, in the previous example, we consider G acting on itself by left multiplication, we obtain the **regular representation** $\mathbb{C}G$.

Now an element of G becomes a linear transformation on $\mathbb{C}G$. Then each element of $\mathbb{C}G$ is just a linear combination of linear transformations, which is again a linear transformation. Hence each element of $\mathbb{C}G$ is itself a linear transformation of $\mathbb{C}G$, as follows:

$$\left(\sum_i a_i g_i \right) \left(\sum_j b_j h_j \right) = \sum_i \sum_j a_i b_j g_i h_j.$$

It's easy to show that this puts a multiplicative structure on $\mathbb{C}G$, and for this reason $\mathbb{C}G$ is also called the **group algebra** or **group ring** of G.

The same extension works for any G-module V. Since each element of G is a linear transformation of V, so is any element of $\mathbb{C}G$, since a linear combination of linear transformations is again a linear transformation:

$$\left(\sum_i a_i g_i\right)\mathbf{v} = \sum_i a_i(g_i\mathbf{v}).$$

For this reason, many authors prefer to think of V as actually being acted on by $\mathbb{C}G$ (since this action also respects the ring structure of $\mathbb{C}G$), and call it instead a $\mathbb{C}G$-module.

The regular representation $\mathbb{C}G$ has the important property that it contains *every* irreducible representation. In fact, if $\mathbb{C}G$ is written as a direct sum of irreducible submodules, then each irreducible representation W appears $\dim W$ times. This yields the identity

$$|G| = \dim \mathbb{C}G = \sum (\dim W)^2 \tag{2.3}$$

where the sum is taken over all non-isomorphic irreducible representations W.

The regular representation can also be viewed as the set of all functions $f : G \to \mathbb{C}$, with pointwise addition and scalar multiplication, and the group action $(gf)(a) = f(g^{-1}a)$ for $g, a \in G$. This can be a useful formulation for signal processing, where we may think of an element of $\mathbb{C}G$ as a signal on $|G|$ points.

2.3 Tensor products of representations

The tensor product allows us to construct representations of direct products of groups. We describe it in terms of matrices, but as we saw in Section 2.1, we could also describe it in terms of G-modules; the two formulations are completely equivalent. This material comes directly from [26] and is included here mainly for later reference.

Definition 2.3.1. Let $A = (a_{ij})$ and B be matrices. Their **tensor product** is the block matrix

$$A \otimes B = (a_{ij}B) = \begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}. \tag{2.4}$$

Now let G and H be groups, with representations $\rho : G \to GL(\mathbb{C}^n)$ and $\varphi : H \to GL(\mathbb{C}^m)$ respectively. Then their tensor product $\rho \otimes \varphi : G \times H \to \mathbb{C}^{nm}$, where we define $(\rho \otimes \varphi)(g, h) = \rho(g) \otimes \varphi(h)$, is a representation of $G \times H$. It can be shown [26] that if ρ and φ are irreducible, then so is $\rho \otimes \varphi$. Thus the representations of a direct product of two groups are completely determined by the representations of the factors.

2.4 Induced and restricted representations

It is natural to ask how the subgroup structure of a group influences its representations. In fact, if we have $H \leq G$, we can construct representations of G from those of H, and vice versa. We again use the matrix formulation of a representation. This material also comes from [26].

Definition 2.4.1. Suppose $H \leq G$, and $\rho : H \to GL(\mathbb{C}^n)$ is a representation of H. Let $t_1, \ldots, t_k$ be a set of representatives for the cosets of H in G (where $k = |G| \,/\, |H|$). Then the **induced representation** $\rho \uparrow_H^G : G \to GL(\mathbb{C}^{nk})$ maps each $g \in G$ to the block matrix

$$\rho \uparrow_H^G (g) = \begin{pmatrix} \rho(t_1^{-1}gt_1) & \rho(t_1^{-1}gt_2) & \cdots & \rho(t_1^{-1}gt_k) \\ \rho(t_2^{-1}gt_1) & \rho(t_2^{-1}gt_2) & \cdots & \rho(t_2^{-1}gt_k) \\ \vdots & \vdots & \ddots & \vdots \\ \rho(t_k^{-1}gt_1) & \rho(t_k^{-1}gt_2) & \cdots & \rho(t_k^{-1}gt_k) \end{pmatrix} \tag{2.5}$$

where $\rho(x) = 0$ for $x \notin H$.

It is shown in [26] that this actually yields a representation of G, and that any two choices of coset representatives yield isomorphic representations, so that the induced representation is well-defined.

The other direction is much simpler: given a representation ρ for G, we can produce the **restricted representation** $\rho \downarrow_H^G$ of H simply by taking the restriction of the map ρ to H. It is obvious that this remains a representation.

We should note that the induced or restricted representations of an irreducible representation are *not* necessarily themselves irreducible. See [3] for more details on when this is true.

2.5 Representation theory and the Fourier transform

Consider the case where $G = Z_n$ is the cyclic group of order n. Then $\mathbb{C}G$ consists of n-dimensional complex vectors, and the action of G cyclically permutes the components. Its irreducible submodules are all one-dimensional (this always happens for abelian groups [8]), so they will be spaces of vectors which are only scaled when their components are cyclically permuted. One such submodule is that in which all components are equal. Others are given by vectors whose components vary in some sense periodically. In fact, each irreducible submodule is spanned by a vector of the form

$$v_k = (1, e^{2\pi ik/n}, e^{4\pi ik/n}, \ldots, e^{2(n-1)\pi ik/n}) \tag{2.6}$$

Also, since these submodules are non-isomorphic, they are in fact the isotypic submodules of $\mathbb{C}G$.

So by decomposing a vector into components lying in these subspaces, we break it into parts that look like complex exponentials. If we think of vectors in $\mathbb{C}G$ as functions $f : G \to \mathbb{C}$ (where the n elements of G can be thought of as n discrete points in time), then this looks very much like a discrete Fourier transform. In

fact, expressing a vector in the basis $\{v_k\}_{k=1}^n$ yields the coefficients of the classical discrete Fourier transform on n points.

If we consider the group algebra as functions on the n elements of Z_n, then isotypic submodules will consist of functions whose values change only by a (complex) scalar when their domains are cycled.

This notion extends to arbitrary groups G ([2], [18]). Although for nonabelian groups the isotypics will not all be 1-dimensional, projections onto isotypic subspaces of $\mathbb{C}G$ (or another G-module) can still yield important information about the original vector. To give just one example, the case $G = S_n$ has been exploited to analyze ranked data [5], such as survey results and voter preferences, in much the same way as the case $G = Z_n$ is used to analyze time-series data. One particularly interesting application uses these techniques to analyze approval voting, detecting coalitions in judicial and legislative bodies [28].

The problem then becomes: how should we compute isotypic projections? Obviously, since projection onto a subspace is a linear transformation, it has a matrix representation, so we could just compute the projection directly. However, the cost of doing this is that of multiplying an $n \times n$ matrix by a vector, which in general requires $O(n^2)$ operations, since there is no reason why this matrix should be particularly "nice."

A better approach comes from an algorithm described in [1] and [23]. If we can find diagonalizable linear operators whose eigenspaces correspond well with the isotypic submodules we seek, then we can compute isotypic projections via eigenspace projections. The next chapter describes how we go about this search.

Chapter 3

Eigenspace Approaches to Isotypic Decomposition

As mentioned previously, isotypic projections can be computed via eigenspace projections, given an appropriate set of linear operators. This chapter describes the process.

3.1 Separating sets

Let us precisely state the properties we seek in our operators.

Definition 3.1.1. Let V be a G-module which decomposes into isotypic submodules as $V = W_1 \oplus \cdots \oplus W_k$. A **separating set** for V is a set $S = \{A_1, \ldots, A_m : V \to V\}$ of simultaneously diagonalizable linear operators on V satisfying the following: For each isotypic submodule W_j there exists a subset $S_j = \{A_{i_1}, A_{i_2}, \ldots\} \subset S$, and a corresponding set of eigenspaces $\{E_{i_1}, E_{i_2}, \ldots\}$, where E_{i_1} is an eigenspace of A_{i_1}, and so on. This set has the property that

$$W_j = E_{i_1} \cap E_{i_2} \cap \ldots. \tag{3.1}$$

That is, each isotypic can be written as an intersection of eigenspaces of some of the operators $A_1, \ldots, A_m$.

It should be clear that a separating set suffices to compute isotypic projections. For if $W_j = E_{i_1} \cap E_{i_2} \cap \ldots$, then to project $\mathbf{v}$ onto W_j, we need simply project it onto E_{i_1} (Section 3.3 discusses how this can be done), project the result onto E_{i_2}, and so on until we have iteratively projected onto each eigenspace. Then what we have is a projection onto their intersection; namely, W_j.

Separating sets are considered at length in [23], in which examples are given for several classes of groups.

3.2 Conjugacy classes

One particularly nice separating set for any group comes from its conjugacy classes. Let C be a conjugacy class of G, and let V be a G-module. As each $g \in C$ is a linear operator on V, so is their sum; namely, the map

$$\mathbf{v} \mapsto \sum_{g \in C} g\mathbf{v}.$$

This operator is called the **class sum** of C.

It can be shown (see for instance [23]) that all these operators are simultaneously diagonalizable, and that every irreducible submodule $W \subset V$ is contained in an eigenspace of the class sum of each C. Furthermore, if W has character χ, then the corresponding eigenvalue is given by

$$\lambda(C, W) = |C| \, \frac{\chi(C)}{\dim W} \tag{3.2}$$

where by $\chi(C)$ we mean the value of χ at any element of C (recall that characters are class functions, so it does not matter which element is used).

Notice that isomorphic irreducible submodules get the same eigenvalue, and hence reside in the same eigenspace. Thus, since an isotypic submodule is a direct sum of isomorphic irreducible submodules, each isotypic submodule also lies in an eigenspace of a class sum.

Thus, to build a separating set S out of class sums, we only require that for every pair W_1, W_2 of irreducibles, S contains some class sum c whose conjugacy class C has $\lambda(C, W_1) \neq \lambda(C, W_2)$; that is, that W_1 and W_2 lie in distinct eigenspaces of c. If this is so, then when all eigenspaces containing some W are intersected, no other irreducible W' can lie in that intersection, since for some class sum W and

W' are in distinct eigenspaces. It can be shown (see for instance [23]) that the set of *all* class sums is sufficient to form a separating set. However, in many important cases not all of them are actually needed, and a much smaller subset suffices.

Notice, in fact, that the above condition is equivalent to having some C with $\frac{\chi_i(C)}{\dim W_i} \neq \frac{\chi_j(C)}{\dim W_j}$ for each W_i, W_j (as the $|C|$'s cancel). And furthermore, since the identity ι of the group must correspond to the identity transformation on V, we have $\dim W = \chi(\iota)$ for every representation W. Thus these eigenvalues may be computed by simply examining $\chi(C)$ for each class sum C and irreducible character χ. These are given by the **character table** of G: if G has irreducible characters $\chi_1, \ldots, \chi_k$ and conjugacy classes $C_1, \ldots, C_k$, the character table is the $k \times k$ matrix whose ijth entry is $a_{ij} = \chi_i(C_j)$. The order chosen for the characters and conjugacy classes is unspecified, but usually C_1 is the conjugacy class of the identity. As such, given a character table, our eigenvalues appear as the entries of a **modified character table** whose ijth entry is $b_{ij} = a_{ij}/a_{i1}$.

Now, it might appear that this makes the problem of finding a separating set rather easy: all we have to do is generate the modified character table, and search for a set of columns (conjugacy classes) such that for every pair of rows (irreducibles), there is a column in the set in which those two rows have different entries. The number of projections required is certainly related to the number of class sums used, so it is reasonable to look for a separating set which is as small as possible. (Note, however, that the smallest separating set does not always yield the fastest projections; see Section 3.4 for an example.) Unfortunately, we have shown that finding a minimum-size separating set of class sums from the modified character table is an **NP-complete** problem; there is probably no algorithm to do this in polynomial time in the size of this table. For a further explanation and a proof of this fact, see Appendix A.

However, it is possible to approximate this problem rather well, if we require only a near-optimal solution. We could use the following **greedy algorithm**: start

by taking the conjugacy class that distinguishes the most pairs of irreducibles. If some pairs remain undistinguished, take the class that distinguishes the most of the remaining pairs. Repeat this until all pairs are distinguished.

This greedy algorithm certainly runs in polynomial time. It may be possible to show that the set thus obtained is in some sense "close" to the size of a smallest set, thereby placing bounds on how accurately the greedy algorithm approximates an optimal solution. See Appendix A for further details.

3.3 Isotypic projections via eigenspaces

Suppose, then, that we want to compute the projections of a vector $\mathbf{v}$ of dimension n onto the k eigenspaces of a diagonalizable matrix A. The naive approach is just to compute the matrix of each projection operation (which is a linear transformation) and multiply it by $\mathbf{v}$. But the projection matrix may be arbitrarily complicated, hence multiplying it by a vector requires $O(n^2)$ operations. If we have k projections to compute, we need a total of $O(kn^2)$ operations. When n is large (and for our purposes it is), this is prohibitive.

However, there is an algorithm that can take advantage of nice structure in A. If A is a general matrix, then multiplying it by an arbitrary vector takes $O(n^2)$ operations. But perhaps A is sparse, or block diagonal, or factors into smaller matrices. In this case, it can be multiplied by an arbitrary vector using fewer operations. We use A^{op} to denote this number of operations.

Theorem 3.3.1. *Given a vector* $\mathbf{v}$ *of dimension* n *and a diagonalizable* $n \times n$ *matrix* A*, the projections of* $\mathbf{v}$ *onto the* k *eigenspaces of* A *can be computed with* $O(kA^{\mathrm{op}} + k^2 n)$ *operations.*

The algorithm for this is based on a technique called the Arnoldi iteration. A description of the algorithm with a view to this application can be found in [1].

In our case, we will usually have $A^{\text{op}} = O(n)$, and $k \ll n$, so this will allow us to do projections with $O(n)$ operations.

3.4 Example: Isotypic projections for the cyclic group

Let us consider an example of the eigenspace method in action, in the case of the cyclic group. The isotypic projections we recover will correspond to the coefficients of the discrete Fourier transform, as described in Section 2.5. As Fourier transform algorithms often do, we restrict ourselves to the case where the number of "points" is a power of 2.

Let $G = Z_{2^n} = \{z^0, z^1, \ldots, z^{2^n-1}\}$ be the cyclic group of order 2^n with generator z, and consider the regular representation $\mathbb{C}G$. As we saw in Section 2.2, we can view this as the space of functions $f : G \to \mathbb{C}$, which we can think of as **signals** on 2^n points corresponding to the elements of G (in order). In applications, this might correspond to some sort of time-series data sampled at 2^n equally spaced points in time, so we will write the elements of $\mathbb{C}G$ as complex 2^n-tuples.

Since G is abelian, each element is its own conjugacy class. So by Theorem 2.1.6 there are 2^n distinct irreducible representations, all of which are contained in $\mathbb{C}G$. It follows that each irreducible representation has dimension 1, and appears only once in the decomposition of $\mathbb{C}G$, so in this case the isotypic submodules of $\mathbb{C}G$ are exactly the irreducible submodules.

Now each element of G is its own class sum, and hence a candidate for inclusion in a separating set. (Notice also that its matrix representation is a $2^n \times 2^n$ permutation matrix, so in this case $A^{\text{op}} = O(2^n)$). In fact, in this case the smallest separating set of class sums has only one element! The eigenspaces of the linear transformation z^1 (the generator of G) are precisely the irreducibles. Thus, if we fix ω as a primitive 2^nth root of unity, it is not difficult to see that the eigenvalues of z^1

are

$$\lambda_j = \omega^j \tag{3.3}$$

and have corresponding eigenspaces

$$E_j = \text{span}\,\{(1, \omega^j, \omega^{2j}, \ldots, \omega^{(2^n-1)j})\}, \tag{3.4}$$

for $j = 0, \ldots, 2^n - 1$. Comparing (2.6), we see that these eigenspaces are in fact the isotypic submodules of $\mathbb{C}G$.

However, this tiny (one element) separating set is not ideal for our purposes. Recall from Theorem 3.3.1 that if there are k eigenspaces, the time required to compute eigenspace projections is of order k^2, and for this element, we have $k = 2^n$. We can get better efficiency by choosing more elements with fewer eigenspaces each.

Let us consider instead the element $z^{2^{n-1}}$, which essentially interchanges the first and last "halves" of the coordinates of a vector. It has eigenvalues 1 and -1, corresponding to eigenspaces E_1, E_2 where the last half is equal to or the negative of the first half. Computing these projections thus takes $O(2^n)$ operations. Now consider the element $z^{2^{n-2}}$. It has eigenvalues $1, i, -1, -i$ (where $i = \sqrt{-1}$), and hence four eigenspaces. However, when we restrict $z^{2^{n-2}}$ to E_1, we find that the restriction has only two eigenspaces of its own; the same happens with E_2. Furthermore, E_1 and E_2 each have dimension 2^{n-1}; if we do our computations in these spaces (with an appropriate change of basis [1]), we can project onto eigenspaces of the element $z^{2^{n-2}}$ with only $O(2^{n-1})$ operations for each of E_1, E_2; again requiring a total of $O(2^n)$ operations. We have now split $\mathbb{C}G$ into 4 eigenspaces. We repeat the process with $z^{2^{n-3}}$; now we work in each of 4 eigenspaces, and require a total of $O(2^n)$ operations. Continuing the process until we reach the element z^1, we find that each of our n steps has required $O(2^n)$ operations, for a grand total of $O(n2^n)$. This may seem high, but in terms of the number of points $m = 2^n$,

[1] A significant amount of work has been swept under the rug here. However, it can be shown that an appropriate change of basis can always be computed quickly. See [1] for details.

this is only $O(m \log m)$ operations. In fact, what we have described is in essence an algorithm for the fast Fourier transform. It is equivalent [23] to the so-called Gentleman-Sande FFT [12].

By using a divide-and-conquer approach, we can achieve the same results in far less time. This is a common theme in Fourier transform algorithms.

We observe in passing that that our "better" separating set actually contains the first one! The key is that we use it last, after the space is already mostly decomposed, rather than trying to use its full power right at the beginning of the process. This demonstrates that in considering a separating set, we must also consider the order in which the elements are to be applied. Had we used our "better" separating set in the reverse order, it would have been no improvement at all.

3.5 Jucys-Murphy elements

In the example of Section 3.4, we saw a separating set for which the intersections of the eigenspaces were exactly the isotypic submodules we sought. We do not actually need the full strength of this condition. It is perfectly all right for a separating set to decompose the space more finely than the isotypics. In particular, it suffices that the intersections of the eigenspaces are merely all *contained* in the isotypic submodules, since if this holds, we can compute our eigenspace projections and merely add up all the projections which lie in a single isotypic submodule.

As we noted in Section 3.2, this will never be necessary when our separating set consists of class sums. However, there are other possibilities. For instance, we could intersect conjugacy classes with subgroups of our group G, and take our elements to be the sums of the resulting sets. In the symmetric group S_n, a particularly nice set of this kind is supplied by the so-called Jucys-Murphy elements.

Definition 3.5.1. For $2 \leq j \leq n$, the jth **Jucys-Murphy element** of $\mathbb{C}S_n$ is given by

the sum of transpositions

$$R_j = (1\ j) + (2\ j) + \cdots + ((j-1)\ j). \tag{3.5}$$

Recalling [8] that two elements of S_n are conjugate if and only if they have the same cycle type, we see that the set of all transpositions in S_n form a conjugacy class $K_{(2)}$. Furthermore, for $j \leq n$, we have $S_j \leq S_n$ in a very natural way (if S_n is the group of permutations of $\{1, \ldots, n\}$, then consider S_j as the subgroup consisting of permutations which fix $j+1, j+2, \ldots, n$). Then R_j is simply the sum of the subset $(K_{(2)} \cap S_j) - S_{j-1}$ of S_n.

It can be shown [23] that we can get the separating set we desire by taking all of the Jucys-Murphy elements; namely, the set $\{R_j \,|\, 2 \leq j \leq n\}$. Moreover, their matrix representations in the standard basis for $\mathbb{C}S_n$ are quite simple: there are only j nonzero entries in each row and column (and these are 1s). As $j \leq n \ll n! = \dim \mathbb{C}S_n$, these matrices are computationally very inexpensive to multiply, which is desirable in view of Theorem 3.3.1.

A further, extremely useful property of the Jucys-Murphy elements appears when we consider them as acting on $\mathbb{C}S_n$ not only by *left* multiplication, but also by *right* multiplication. Then the right action of R_j gives rise to a different linear transformation on $\mathbb{C}S_n$, which we may call R'_j. As mentioned by [23] (with reference to [7] and [19]), if we include these right-acting elements in our set (to obtain $\{R_j, R'_j \,|\, 2 \leq j \leq n\}$), the resulting decomposition is so fine that all of the (nontrivial) eigenspace intersections are 1-dimensional. As such, computing the projections of a vector onto these intersections amounts to a change of basis—much as the Fourier transform in the Z_n case. In fact, what we recover is exactly the discrete Fourier transform on S_n.

Much work has been done on generalizing these elements to other groups; see [6], [21], and [24]. However, we are not aware of any analogue of the Jucys-Murphy elements for the groups in which we shall be interested (see Chapter 4).

Chapter 4

Automorphism Groups of Binary Trees

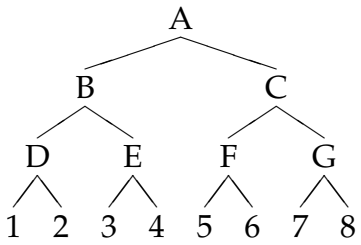
4.1 Binary trees

For the rest of this thesis, we shall be interested in the following class of groups.

Definition 4.1.1. W_n is the group of all automorphisms (or symmetries) of a complete binary tree T_n of height $n+1$.

As seen in the following example, an automorphism of such a tree corresponds to a permutation of its leaves, and this correspondence is one-to-one. In this sense, W_n is isomorphic to a subgroup of the symmetric group S_{2^n}.

Example 4.1.2. Consider the following tree T_3:



We can see that the permutation $(1\ 2)$ (written in cycle notation) corresponds to an automorphism of T_3, but that $(1\ 3)$ does not.

We can get automorphisms of G by swapping the subtrees of any of the non-leaf nodes A–G, and all automorphisms can be obtained by composing these. In fact, the group W_3 of all automorphisms of T_3 is generated by the elements $(1\ 2)$, $(1\ 3)(2\ 4)$, $(1\ 5)(2\ 6)(3\ 7)(4\ 8)$, which correspond respectively to swaps at D, B and A.

The recursive structure of these groups is obvious. In particular, notice that T_n consists of two copies of T_{n-1} under a root node. Any automorphism of T_n can be written as a product (composition) of an automorphism of the left-hand T_{n-1}, an automorphism of the right-hand T_{n-1}, and possibly a swap of the two copies. Thus we see that $|W_n| = 2\,|W_{n-1}|^2$, and since $|W_1| = 2$, we have by induction that $|W_n| = 2^{(2^n-1)}$. This extremely rapid growth of the group with respect to n is the fundamental cause of computational difficulties: the group is just too big.

4.2 Wreath products

A nice description of W_n can be given in terms of wreath products, which we now define.

Definition 4.2.1. Let G be a finite group, and let $H \leq S_n$ be a permutation group. Let $G^n = G \times \cdots \times G$ (n times) be the set of ordered n-tuples of elements of G. The **wreath product** $G \wr H$ of G with H is the set $G^n \times H$ with the following multiplication:

$$(g, \sigma)(h, \pi) = (gh^\sigma, \sigma\pi) \tag{4.1}$$

$$= ((g_1 h_{\sigma^{-1}(1)}, \ldots, g_n h_{\sigma^{-1}(n)}), \sigma\pi) \tag{4.2}$$

where $g = (g_1, \ldots, g_n), h = (h_1, \ldots, h_n)$ are in G^n, and σ and π are in H.

To understand this, imagine that the components of h are "twisted" by σ before being multiplied by g.

It is easy to show that $G \wr H$ is a group under this multiplication. It is also not hard to show that the wreath product is associative, but generally not commutative. Furthermore, it is apparent that the wreath product is a semidirect product $G^n \rtimes H$.

In our case, we take $G = W_{n-1}$ and $H = Z_2$. Then $W_{n-1} \wr Z_2$ consists of two copies of W_{n-1} which can be "twisted" together. These copies of W_{n-1} correspond

to automorphisms of two copies of T_{n-1}, and the twisting corresponds to the possibility of interchanging the copies of T_{n-1}, as if they were subtrees of a root node. In fact, what we obtain is all automorphisms of T_n, and we have $W_n = W_{n-1} \wr Z_2$. Since $W_1 = Z_2$, we can write

$$W_n = Z_2 \wr \cdots \wr Z_2 \quad (n \text{ times}). \tag{4.3}$$

In general, the group of all automorphisms of a complete regularly branching r-ary tree of height $n+1$ is given by $S_r \wr \cdots \wr S_r$ (n times). By choosing at each step some subgroup of S_r, we obtain a more restricted set of automorphisms. [9] describes applications of the group $W_{n,r} = Z_r \wr \cdots \wr Z_r$ (n times), with particular interest in the case $r = 4$, in which a "wreath product transform" for image processing can be obtained.

4.3 Representation theory

Given the recursive structure of W_n, it should come as no surprise that its representations arise recursively. This section follows a construction from [22], which generalizes to wreath products of arbitrary cyclic groups; a discussion of the representation theory of wreath product groups in general may be found in [16]. The process of constructing representations of a semidirect product is the purview of Clifford theory [3]; a good source on the subject is [15]. Tensor products $\rho \otimes \varphi$ of representations are defined in Section 2.3; induced representations $\rho \uparrow_H^G$ are defined in Section 2.4.

We start with the irreducible representations $\{\rho_i\}$ of W_{n-1}, and consider the normal subgroup $W_{n-1} \times W_{n-1} \trianglelefteq W_n$ which corresponds to automorphisms of T_n which do not swap the right and left subtrees of the root. As shown in Section 2.3, the irreducible representations of $W_{n-1} \times W_{n-1}$ are of the form $\rho_i \otimes \rho_j$.

If $i = j$, then $\rho_i \otimes \rho_i$ is actually an irreducible representation of W_n which simply disregards the swap at the root. To take this swap into account, we tensor an irre-

ducible representation of Z_2. There are two of these—the trivial representation φ_0 and the alternating representation φ_1—and thus we obtain irreducible representations for W_n of the form $\rho_i \otimes \rho_i \otimes \varphi_k$.

If $i \neq j$, then $\rho_i \otimes \rho_j$ is not a representation of W_n. However, since $W_{n-1} \times W_{n-1} \leq W_n$, we can induce this representation of the former to a representation of the latter, as described in Section 2.4. It can be shown that the resulting representation $\rho_i \otimes \rho_j \uparrow^{W_n}_{W_{n-1} \times W_{n-1}}$ of W_n is irreducible. Furthermore, the representations which arise from $\rho_i \otimes \rho_j$ and $\rho_j \otimes \rho_i$ are isomorphic to one another, so that the ordering of i and j can be ignored.

We summarize this construction in the following theorem, which is proved in [22].

Theorem 4.3.1. *Suppose $\{\rho_i\}$ are all the irreducible representations of W_{n-1}. Let φ_0 and φ_1 be the trivial and alternating representations of Z_2. Then every irreducible representation of W_n takes exactly one of the following forms:*

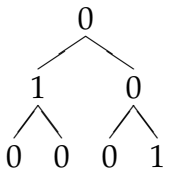
1. $\rho_i \otimes \rho_i \otimes \varphi_k$, *or*

2. $\rho_i \otimes \rho_j \uparrow^{W_n}_{W_{n-1} \times W_{n-1}}$, *for $i < j$.*

This gives us a nice recursive way to index irreducible representations of W_n, using labeled trees of height n. For $W_1 \cong Z_2$, there are only two irreducible representations, the trivial representation ρ_0 and the alternating representation ρ_1. To these, we associate trees of height 1, whose single node is labeled 0 for trivial or 1 for alternating. Otherwise, an irreducible representation of W_n is associated with a labeled tree consisting of a root and two subtrees, each of which correspond to an irreducible representation of W_{n-1}. If the two subtrees are the same, the root may be labeled with a 0 or a 1 (this corresponds to the first case of Theorem 4.3.1). Otherwise, if they are different, the root must be labeled 0 (this corresponds to the second case). Notice that isomorphic trees yield isomorphic representations. [22]

calls these trees 2**-trees** (a special case of r-trees for iterated wreath products of any Z_r), and we shall follow this terminology.

Example 4.3.2. The 2-tree



corresponds to the following irreducible representation for W_3:

$$(\rho_0 \otimes \rho_0 \otimes \varphi_1) \otimes (\rho_0 \otimes \rho_1 \uparrow_{W_1 \times W_1}^{W_2}) \uparrow_{W_2 \times W_2}^{W_3} .$$

This bijection between 2-trees and irreducible representations lets us count the irreducible representations of W_n. In fact, the following recurrence is easy to see:

Theorem 4.3.3. *Let k_n be the number of irreducible representations of W_n. Then $k_1 = 2$, and*

$$k_{n+1} = 2k_n + \binom{k_n}{2} = \frac{k_n^2 + 3k_n}{2}. \tag{4.4}$$

Proof. We count the 2-trees of height $n+1$. Given an 2-tree, suppose its root is labeled with $a = 0$ or 1, and the two subtrees of the root are the 2-trees A and B of height n. We have the following possibilities:

1. $A = B$; that is, the two subtrees are equivalent. Then there are k_n choices for the subtree $A = B$, and the root may be labeled with either a 0 or a 1. This gives us $2k_n$ possibilities.

2. $A \neq B$. The root is then forced to be labeled with a 0. Since order does not matter, there are $\binom{k_n}{2}$ choices for A, B.

As these cases are disjoint and cover every 2-tree of height $n+1$, (4.4) follows. □

We are not aware of any closed-form solution of this recurrence. However, since for $n \geq 2$ we have $k_n > 3$, it follows that $k_{n+1} < k_n^2$, and so $k_n \leq 2^{2^{n-1}}$. In fact, it seems empirically that the growth is rather slower than this.

4.4 Permutation representation and Haar wavelets

As we saw, each element of W_n induces a permutation on the 2^n leaves of T_n (see Section 4.1). This gives rise to a group action of W_n on the set of leaves L, and as discussed in Section 2.2, this action in turn gives rise to a permutation representation of W_n. The permutation representation can be thought of as the vector space $\mathbb{C}L$ of linear combinations of L, or alternatively as complex-valued functions $f : L \to \mathbb{C}$. In either case it can be viewed as a space of signals, and the structure of the representation gives us a way to decompose these signals. In particular, we are interested in their isotypic projections.

It can be shown [9] that these projections correspond to the 1-D discrete Haar wavelet transform of the signal. This transform essentially involves decomposing the signal as a sum of smaller and smaller square waves. One particular advantage of the Haar wavelet transform is that it can very effectively "zoom in" on short-term, transient parts of the signal, without losing the signal's overall shape. Further details can be found in [29], which discusses applications including compression and denoising of signals.

4.5 Conjugacy classes

In the course of this work, we found it useful to explicitly derive some results about the conjugacy classes of $G \wr Z_2$, of which $W_n = W_{n-1} \wr Z_2$ is a special case. We record them here.

Let G be a finite group with identity ι and $Z_2 = \{0, 1\}$ be the cyclic group of order 2. We write elements of $G \wr Z_2$ as ordered triples (a, b, z) where $a, b \in G$ and $z \in Z_2$.

For readers who prefer to think of trees, think of $G = W_{n-1}$. Then (a, b, z) corresponds to an automorphism of T_n constructed as follows:

1. Apply the automorphism a to the left-hand subtree of the root (this subtree is a copy of T_{n-1}).

2. Apply the automorphism b to the right-hand subtree.

3. If z is the generator of Z_2, exchange the two subtrees; if z is the identity of Z_2, do nothing.

Recall that in general for wreath product groups $G \wr H$ where $H \leq S_n$, multiplication is given by $(a, \pi) \cdot (b, \sigma) = (ab^{\pi}, \pi\sigma)$ (where $a, b \in G^n$ and b^{π} denotes permuting the "coordinates" of b according to π). It follows that inverses are given by $(a, \pi)^{-1} = ((a^{-1})^{\pi^{-1}}, \pi^{-1})$, and conjugation by $(a, \pi)(b, \sigma)(a, \pi)^{-1} = (ab^{\pi}(a^{-1})^{\sigma}, \pi\sigma\pi^{-1})$. Notice that when H is abelian (as in our case), the last coordinate of an element is unchanged by conjugation.

Let $\sim$ denote the conjugacy relation (i.e. $a \sim b$ if $a = xbx^{-1}$ for some x).

Proposition 4.5.1. *$(a, b, 0) \sim (c, d, 0)$ if and only if $a \sim c$ and $b \sim d$, or $a \sim d$ and $b \sim c$.*

Proof. Suppose $(a, b, 0) \sim (c, d, 0)$. There are two cases:

1. $(x, y, 0)(a, b, 0)(x, y, 0)^{-1} = (c, d, 0)$. Expanding, $(xax^{-1}, yby^{-1}, 0) = (c, d, 0)$. Thus $xax^{-1} = c$, $yby^{-1} = d$, and we have $a \sim c$ and $b \sim d$.

2. $(x, y, 1)(a, b, 0)(x, y, 1)^{-1} = (c, d, 0)$. Expanding, $(xbx^{-1}, yay^{-1}, 0) = (c, d, 0)$. Thus $xbx^{-1} = c$, $yay^{-1} = d$, and we have $b \sim c$ and $a \sim d$.

Note that each step is reversible, so the converse is also established. □

Proposition 4.5.2. *$(a, \iota, 1) \sim (c, d, 1)$ if and only if $a \sim cd$.*

Proof. ($\Rightarrow$) Suppose $(a, \iota, 1) \sim (c, d, 1)$. There are two cases:

1. $(x, y, 0)(a, \iota, 1)(x, y, 0)^{-1} = (c, d, 1)$. Expanding, $(xay^{-1}, yx^{-1}, 1) = (c, d, 1)$. Thus $c = xay^{-1}$, $d = yx^{-1}$, and then $cd = xax^{-1}$, so that $a \sim cd$.

2. $(x, y, 1)(a, \iota, 1)(x, y, 1)^{-1} = (c, d, 1)$. Expanding, $(xy^{-1}, yax^{-1}, 1) = (c, d, 1)$. Thus $c = xy^{-1}, d = yax^{-1}$, and then $cd = xax^{-1}$, so that again $a \sim cd$.

($\Leftarrow$) Suppose $a \sim cd$, so that $a = z(cd)z^{-1}$ for some $z \in G$. Let $x = z^{-1}$, $y = dz^{-1}$. Then

$$\begin{aligned}(x, y, 0)(a, \iota, 1)(x, y, 0)^{-1} &= (xay^{-1}, yx^{-1}, 1) \\ &= ((z^{-1})(zcdz^{-1})(zd^{-1}), (dz^{-1})z, 1) \\ &= (c, d, 1).\end{aligned}$$

Thus $(a, \iota, 1) \sim (c, d, 1)$. □

Corollary 4.5.3. *Every element of $G \wr Z_2$ is conjugate to an element of the form $(a, b, 0)$ or $(a, \iota, 1)$ (and never both).*

This gives us a way to count the conjugacy classes of $G \wr Z_2$.

Proposition 4.5.4. *If G has k conjugacy classes, then $G \wr Z_2$ has $\binom{k}{2} + 2k$ conjugacy classes.*

Proof. Let $\{c_1 = \iota, c_2, \ldots, c_k\}$ be a complete set of representatives for the conjugacy classes of G. Given Corollary 4.5.3 and the fact that $(c_i, c_j, 0) \sim (c_j, c_i, 0)$ (from Proposition 4.5.1), we find that a complete set of representatives for the conjugacy classes of $G \wr Z_2$ is given by

$$\{(c_i, c_j, 0) \mid i < j\} \cup \{(c_i, c_i, 0)\} \cup \{(c_i, \iota, 1)\}. \tag{4.5}$$

The first set contains $\binom{k}{2}$ elements, while the second and third contain k elements each. As the union is obviously disjoint, the conclusion follows. □

In the case $G = W_{n-1}$, the fact that the number of conjugacy classes equals the number of irreducible representations means that Proposition 4.5.4 gives an alternate proof of Theorem 4.3.3. On the other hand, comparing the set of class

representatives given in Proposition 4.5.4 with the 2-tree construction given in Section 4.3 shows us that 2-trees correspond in a very natural way with conjugacy classes. So there are natural bijections between 2-trees, irreducible representations, and conjugacy classes.

We can now compute the sizes of the conjugacy classes of $G \wr Z_2$. For $g \in G$, let C_g denote the conjugacy class of g in G.

Proposition 4.5.5. *1. The conjugacy class of an element $(a, b, 0)$, where $a \sim b$, has size $|C_a|^2$.*

2. The conjugacy class of an element $(a, b, 0)$, where $a \nsim b$, has size $2\,|C_a|\,|C_b|$.

3. The conjugacy class of an element $(a, \iota, 1)$ has size $|C_a|\,|G|$.

Proof. 1. If $(c, d, 0) \sim (a, b, 0)$, where $a \sim b$, by Proposition 4.5.1 $a \sim c$ and $d \sim b \sim a$. Hence c and d may each be any element of C_a, so there are a total of $|C_a|$ elements conjugate to $(a, b, 0)$.

2. If $(c, d, 0) \sim (a, b, 0)$, where $a \nsim b$, by Proposition 4.5.1 either $a \sim c$ and $b \sim d$, or $a \sim d$ and $b \sim c$. In the former case there are $|C_a|$ possibilities for c and $|C_b|$ possibilities for d, for a total of $|C_a|\,|C_b|$. In the latter case there are $|C_a|$ possibilities for d and $|C_b|$ possibilities for c, again for a total of $|C_a|\,|C_b|$. Furthermore, as $a \nsim b$, these cases must be disjoint. Hence there are a total of $2\,|C_a|\,|C_b|$ elements conjugate to $(a, b, 0)$.

3. If $(c, d, 1) \sim (a, \iota, 1)$, then by Proposition 4.5.2 we have $a \sim cd$. Choose an element $a' \in C_a$; we want to have $cd = a'$. Now d may be any element of G, but then we are forced to have $c = a'd^{-1}$. As there are $|C_a|$ choices for a' and $|G|$ choices for d, there must be a total of $|C_a|\,|G|$ elements conjugate to $(a, \iota, 1)$.

□

Chapter 5

Separating Sets

5.1 Regular representations

5.1.1 Separating sets for $\mathbb{C}W_n$

Using the techniques described in Section 3.2, we have computed separating sets of class sums for the regular representation of W_n, $n \leq 4$. The relevant program code is contained in Appendix B. We used character tables generated by the GAP software package for computational algebra [10], modified as described in Section 3.2. The results are summarized in Table 5.1.

The reason for the cutoff at $n = 4$ is that W_5 is so large that GAP was unable to compute its character table in a reasonable amount of time. Running for 12 hours on a 1.2 GHz Pentium III workstation resulted in no apparent progress.

n	$\lvert W_n \rvert$	Irreducibles	Minimal set size	Method
1	2	2	1	Trivial
2	8	5	2	Inspection
3	128	20	4	Brute force
4	32768	230	≤ 9	Greedy algorithm

Table 5.1: Separating set sizes for the regular representation of W_n, $n \leq 4$

The sizes of separating sets appear to us to grow suspiciously like powers of 2. This suspicion would be strengthened if we were able to find a separating set of

size 8 for W_4; unfortunately, the greedy algorithm only yields one of size 9, and the number of representations is so large as not to be susceptible to brute force techniques. Nevertheless, based on the recursive nature of these groups, we would not be surprised if W_{n+1} should have a separating set of twice the size of the smallest one for W_n. Specifically:

Conjecture 5.1.1. W_n has a separating set consisting of 2^n class sums.

We have examined the structure of the separating sets we found in hopes of finding a pattern, but have so far been unsuccessful. We list here the separating sets we have found.

5.1.2 Separating sets for $\mathbb{C}W_2$

There are 3 separating sets of class sums of size 2 for W_2. They can easily be found by inspection of the character table. Inspection also shows that there is no separating set of size 1, and thus the separating sets of size 2 are minimal.

First, Table 5.2 lists the conjugacy classes of W_2, in the order used by GAP. We list a representative for each, in cycle notation, and the corresponding 2-tree (see Section 4.5).

Given the indexing of Table 5.2, Table 5.3 lists all 3 separating sets of size 2 for the regular representation of W_2.

5.1.3 Separating sets for $\mathbb{C}W_3$

Again, we begin by listing the conjugacy classes of W_3, in Table 5.4. Using its indexing, Table 5.5 gives all 40 separating sets of class sums of size 4 for the regular representation of W_3. There are none of size 3, so these are minimal. These separating sets were obtained by brute force search of a character table generated by GAP [10].

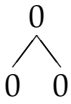
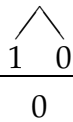
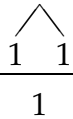
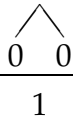
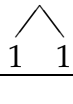
Index	Representative	2-tree
1	ι	
2	$(1\,2)$	
3	$(1\,2)(3\,4)$	
4	$(1\,3)(2\,4)$	
5	$(1\,4\,2\,3)$	

Table 5.2: Conjugacy classes of W_2

$\{2,4\}$	$\{2,5\}$	$\{4,5\}$

Table 5.3: Minimal separating sets for $\mathbb{C}W_2$

Table 5.4: Conjugacy classes of W_3

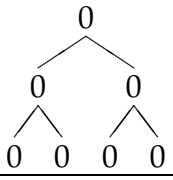
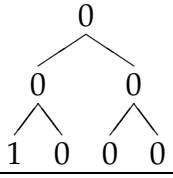
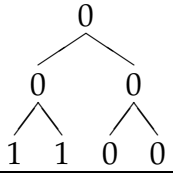
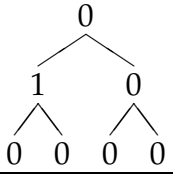
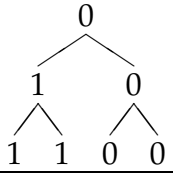
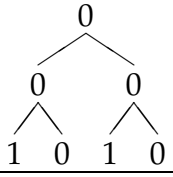
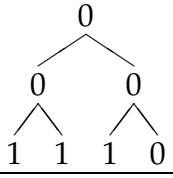
Index	Representative	2-tree
1	ι	
2	$(1\,2)$	
3	$(1\,2)(3\,4)$	
4	$(1\,3)(2\,4)$	
5	$(1\,4\,2\,3)$	
6	$(1\,2)(5\,6)$	
7	$(1\,2)(3\,4)(5\,6)$	

Table 5.4: Conjugacy classes of W_3 (continued)

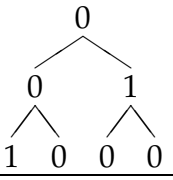
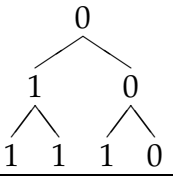
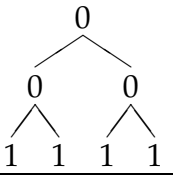
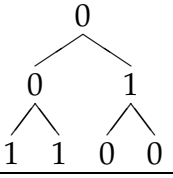
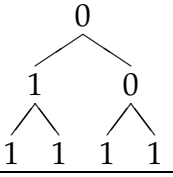
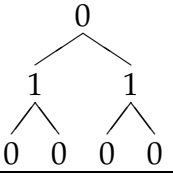
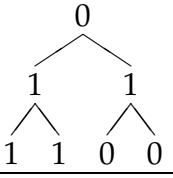
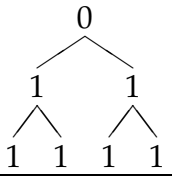
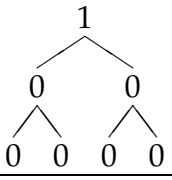
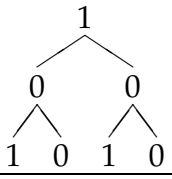
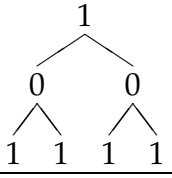
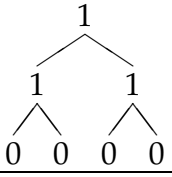
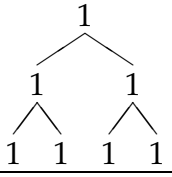
Index	Representative	2-tree
8	$(1\,2)(5\,7)(6\,8)$	
9	$(1\,4\,2\,3)(5\,6)$	
10	$(1\,2)(3\,4)(5\,6)(7\,8)$	
11	$(1\,2)(3\,4)(5\,7)(6\,8)$	
12	$(1\,4\,2\,3)(5\,6)(7\,8)$	
13	$(1\,3)(2\,4)(5\,7)(6\,8)$	
14	$(1\,4\,2\,3)(5\,7)(6\,8)$	

Table 5.4: Conjugacy classes of W_3 (continued)

Index	Representative	2-tree
15	$(1\,4\,2\,3)(5\,8\,6\,7)$	
16	$(1\,5)(2\,6)(3\,7)(4\,8)$	
17	$(1\,6\,2\,5)(3\,7)(4\,8)$	
18	$(1\,6\,2\,5)(3\,8\,4\,7)$	
19	$(1\,7\,3\,5)(2\,8\,4\,6)$	
20	$(1\,8\,4\,6\,2\,7\,3\,5)$	

5.1.4 Separating set for $\mathbb{C}W_4$

Table 5.6 gives a separating set of size 9 of class sums for the regular representation of W_4. This was obtained by greedily searching the character table of W_4, as

$\{2,4,5,16\}$	$\{2,4,5,18\}$	$\{2,4,8,16\}$	$\{2,4,8,18\}$
$\{2,4,12,16\}$	$\{2,4,12,18\}$	$\{2,5,9,16\}$	$\{2,5,9,18\}$
$\{2,5,11,16\}$	$\{2,5,11,18\}$	$\{2,8,11,16\}$	$\{2,8,11,18\}$
$\{2,9,12,16\}$	$\{2,9,12,18\}$	$\{2,11,12,16\}$	$\{2,11,12,18\}$
$\{4,5,7,16\}$	$\{4,5,7,18\}$	$\{4,5,14,16\}$	$\{4,5,14,18\}$
$\{4,7,8,16\}$	$\{4,7,8,18\}$	$\{4,7,12,16\}$	$\{4,7,12,18\}$
$\{4,12,14,16\}$	$\{4,12,14,18\}$	$\{5,7,9,16\}$	$\{5,7,9,18\}$
$\{5,7,11,16\}$	$\{5,7,11,18\}$	$\{5,11,14,16\}$	$\{5,11,14,18\}$
$\{7,8,11,16\}$	$\{7,8,11,18\}$	$\{7,9,12,16\}$	$\{7,9,12,18\}$
$\{7,11,12,16\}$	$\{7,11,12,18\}$	$\{11,12,14,16\}$	$\{11,12,14,18\}$

Table 5.5: Minimal separating sets for $\mathbb{C}W_3$

described in Section 3.2. As such, this set is *not* known to be minimal; in fact, we conjecture (5.1.1) that it has one of size 8. It is also presumably not the only set of size 9. Unfortunately, brute force search is infeasible for checking this.

As W_4 has 230 conjugacy classes, we do not list all of them; only those involved in the separating set. As before, we index them as returned by GAP [10].

Table 5.6: Separating set for $\mathbb{C}W_4$

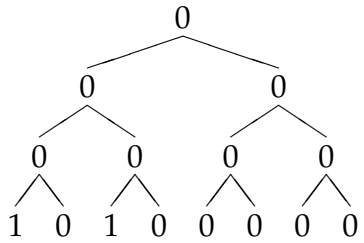
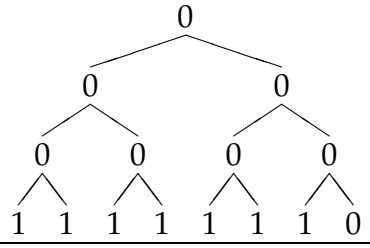
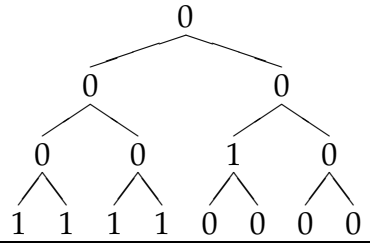
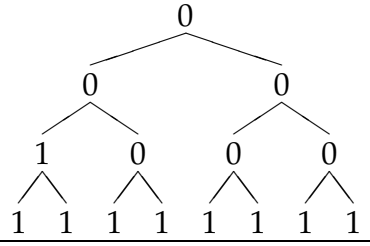
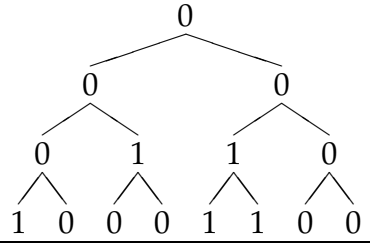
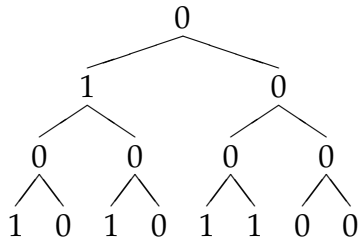
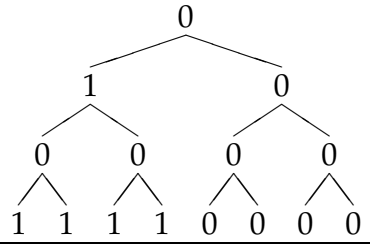
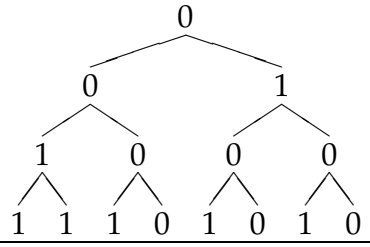
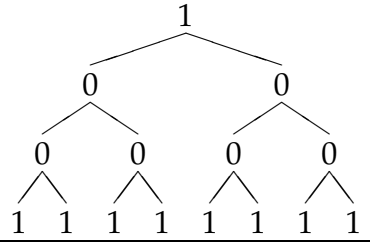
Index	Representative	2-tree
4	$(1\ 2)(5\ 6)$	
20	$(1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12)(13\ 14)$	
32	$(1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 11)(10\ 12)$	
57	$(1\ 4\ 2\ 3)(5\ 6)(7\ 8)(9\ 10)(11\ 12)(13\ 14)(15\ 16)$	
62	$(1\ 2)(5\ 7)(6\ 8)(9\ 12\ 10\ 11)$	

Table 5.6: Separating set for $\mathbb{C}W_4$ (continued)

Index	Representative	2-tree
128	$(1\,6\,2\,5)(3\,7)(4\,8)(9\,10)(11\,12)$	
133	$(1\,6\,2\,5)(3\,8\,4\,7)$	
158	$(1\,4\,2\,3)(5\,6)(9\,14\,10\,13)(11\,15)(12\,16)$	
216	$(1\,10\,2\,9)(3\,12\,4\,11)(5\,14\,6\,13)(7\,16\,8\,15)$	

5.2 Permutation representations

In Section 4.4 we described a permutation representation for W_n, derived from the action of W_n on the leaves of T_n. We shall use V_n to denote this representation. We now describe separating sets of class sums for V_n.

Notice that $\dim V_n = 2^n$, so this representation is quite small compared to the

group itself. Furthermore, the number of irreducibles into which it decomposes is even smaller. It can be shown in general [9] that V_n is the direct sum of $n+1$ nonisomorphic irreducible submodules, and each appears in the sum with multiplicity 1. Since there are fewer submodules to be separated, separating sets are much easier to find, and much smaller.

The algorithm for finding these separating sets is much as before, except the table we use contains only the characters for those irreducible representations which make up V_n. These can easily be found using the inner product relation described in Theorem 2.1.5. The character for V_n is easy to compute: since a permutation matrix contains a 1 on the diagonal for each fixed point, the character of an element g is equal to the number of leaves of T_n which it fixes. Once we have identified the irreducible representations involved, which correspond to rows in the character table, we can remove all other rows and perform a brute force or greedy search on the remaining table.

Table 5.7 lists some separating sets for these permutation representations. Due to their small size, they were all found using brute-force search. As there are usually many, we do not list them all. We give only an example or two for each. The numbers refer to our previous indexing of conjugacy classes, and the following column lists where this indexing can be found.

n	$\dim V_n$	Number of isotypic subspaces	Minimal set size	Number of sets	Example	See table
2	4	3	1	2	$\{4\}, \{5\}$	5.2
3	8	4	2	60	$\{2, 16\}$	5.4
4	16	5	2	1940	$\{32, 216\}$	5.6
n	2^n	$n+1$	?	?	—	—

Table 5.7: Separating sets for the permutation representation of W_n, $n \leq 4$

Chapter 6

Conclusion

6.1 Closing remarks

This area of mathematics has proven for us to be a very intriguing one, uniting elements of algebra and combinatorics from "pure" mathematics with "applied" ideas from spectral analysis, algorithms, and computational linear algebra. We hope that our exposition and results can spur, in some small way, further interest in the field.

6.2 Future work

Our research in this area has raised many more questions than it has answered. We will list several problems which we feel are worthy of future investigation.

6.2.1 Conjecture 5.1.1

A proof of Conjecture 5.1.1 would be very nice to have, especially if it is constructive. Armed with separating sets for all W_n, we would immediately have an isotypic projection algorithm.

It would also be useful to find a bound for the sizes of minimal separating sets for the permutation representation of W_n, as described in Section 5.2.

6.2.2 *Other separating sets*

We considered only separating sets consisting of class sums. Although these have many nice properties, they are not necessarily optimal. Other possibilities should be considered. In particular, thinking of the Jucys-Murphy elements for S_n (see Section 3.5), one could consider conjugacy classes intersected with subgroups, or some similar construction. It is especially suggestive that $S_1 \leq S_2 \leq \ldots \leq S_n$ and $W_1 \leq W_2 \leq \ldots \leq W_n$ both have a strongly recursive structure. Also, the Jucys-Murphy elements separate representations into finer pieces than isotypic submodules, and can even be used to compute a genuine discrete Fourier transform; it would be very helpful to be able to duplicate these properties for W_n.

6.2.3 *Computational bounds*

We concentrated on finding minimal-size separating sets. However, as we saw in Section 3.4, minimal size is not always best when we actually want to compute projections. In fact, in order to say anything about the computational properties of the separating sets we found, we would have to look at how the eigenspaces of our elements interact, considering the dimensions of their intersections as they decompose the space. Once computational bounds are established for isotypic projections using our separating sets, we could evaluate them with respect to other possible separating sets to find one with the best computational properties.

6.2.4 *Greedy algorithm*

In Section 3.1, we described a greedy algorithm for quickly finding separating sets from a character table. It would be useful to know how optimal its results are. As mentioned in Appendix A, a greedy algorithm for a related problem (MINIMUM TEST COLLECTION) has been well studied, and it seems likely that these results could be brought to bear on the separating set problem. Since this method bounds

separating set sizes, it is possible that we could thus obtain a (nonconstructive) proof for Conjecture 5.1.1.

6.2.5 Extensions to iterated wreath products of cyclic groups

We have only examined the group $W_n = Z_2 \wr \cdots \wr Z_2$. More generally, the groups $W_{n,r} = Z_r \wr \cdots \wr Z_r$ are also of great interest. Many of our results about the groups extend to this case (especially when r is prime); see also [22] and [9]. In particular, the case $r = 4$ gives rise to a so-called "wreath product transform" with useful applications in image processing (see [9]).

Appendix A

NP-Completeness of Finding Separating Sets of Class Sums From Character Tables

We mentioned in Section 3.2 that a separating set of class sums for any given group can be found by examining a modified character table. The problem, precisely stated, is the following.

Problem (SEPARATING SET)

Given an $n \times m$ matrix (b_{ij}) (in our case, the table of eigenvalues) and an integer k, do there exist integers $1 \leq c_1, \ldots, c_k \leq m$ such that for every pair $1 \leq i_1, i_2 \leq n$, there exists $1 \leq j \leq k$ such that $b_{i_1 c_j} \neq b_{i_2 c_j}$? In other words, can we tell any two rows apart by looking only in columns $c_1, \ldots, c_k$?

This problem boils down to "does there exist a separating set of size k?" If we can solve this problem efficiently, we can find a minimal-size separating set by attempting it for ever-increasing k until we find one that works.

Unfortunately, we will show that SEPARATING SET is NP-complete. This means that if it has a polynomial-time solution, then so does every other problem in the class NP of problems whose solutions can be verified in polynomial time. This would imply that NP is equal to P, the class of problems with polynomial-time solutions. It is universally believed (though not proven, remaining a famous open conjecture) that this is not the case. For more details on the theory of NP-completeness, see [11].

Our proof of this assertion is by reduction from a problem called MINIMUM

TEST COLLECTION, which we describe here.

Problem (MINIMUM TEST COLLECTION)

Given a finite set A, a collection $C \subset \mathcal{P}(A)$, and a number $J \leq |A|$, does there exist a subcollection $C' \subset C$ with $|C'| \leq J$ such that for every pair $a_1, a_2 \in A$, there exists a set $S \in C'$ such that S contains exactly one of a_1 and a_2 (in other words, $|\{a_1, a_2\} \cap S| = 1$)?

This problem can be considered as one of medical diagnosis: imagine A is a set of diseases, and C is a collection of tests, each of which will return "positive" in the presence of some diseases, and "negative" for the rest. As such, each test may be associated with the set of diseases for which it returns "positive." The question is, do k tests suffice to narrow the diagnosis to a single disease?

It is shown in [11] (page 71) that MINIMUM TEST COLLECTION is NP-complete. We now show that SEPARATING SET is as well.

Theorem A.0.1. *SEPARATING SET is NP-complete.*

Proof. First, it is obvious that SEPARATING SET is in NP, since a solution can be verified in polynomial time. Given the integers $c_1, \ldots, c_k$, we can test that any pair of rows i_1, i_2 is "separated" by looking at the k pairs $a_{i_1 c_j}, a_{i_2 c_j}$ for $1 \leq j \leq k$. Repeating this for each of the $\binom{n}{2} \leq n^2$ pairs of rows and noticing that $k \leq m$, we find that verification requires only $O(n^2 m)$ time.

Now, suppose we have an instance $(A = \{a_1, \ldots, a_n\}, C = \{C_1, \ldots, C_m\}, J)$ of MINIMUM TEST COLLECTION. We can convert it in polynomial time to an instance of SEPARATING SET. Construct a $n \times m$ matrix (b_{ij}) where

$$b_{ij} = \begin{cases} 1, & a_i \in C_j \\ 0, & a_i \notin C_j \end{cases}.$$

Set $k = J$. We show that our instance of SEPARATING SET has a solution if and only if our instance of MINIMUM TEST COLLECTION did.

Suppose that the constructed instance of SEPARATING SET has a solution $c_1, \ldots, c_k$. Then for any pair $1 \leq i_1, i_2 \leq n$, there is some $1 \leq j \leq k$ such that $b_{i_1 c_j} \neq b_{i_2 c_j}$. Suppose without loss of generality that $b_{i_1 c_j} = 0$ and $b_{i_2 c_j} = 1$. Then $a_{i_1} \in C_{c_j}$ and $a_{i_2} \notin C_{c_j}$. As we can do the same for every pair i_1, i_2, it follows that the set $C' = \{C_{c_1}, \ldots, C_{c_k}\}$ is of size $k = J$ and satisfies the conditions required by MINIMUM TEST COLLECTION.

Suppose that the given instance of MINIMUM TEST COLLECTION has a solution $C' = \{S_{c_1}, \ldots, S_{c_J}\}$. Then for every pair $a_{i_1}, a_{i_2} \in A$, there exists some $S_{c_j} \in C'$ such that (without loss of generality) $a_{i_1} \in S_{c_j}$ but $a_{i_2} \notin S_{c_j}$. Then we have $b_{i_1 c_j} = 1 \neq 0 = b_{i_2 c_j}$. As this is true for every pair i_1, i_2, the set $c_1, \ldots, c_J$ is of size $J = k$ and satisfies the conditions required by SEPARATING SET.

Thus, a polynomial-time solution for SEPARATING SET would immediately yield one for MINIMUM TEST COLLECTION, and thus (since MINIMUM TEST COLLECTION is NP-complete) for every other problem in NP. Hence, since SEPARATING SET is also in NP, we have that SEPARATING SET is NP-complete. □

Notice that we do *not* claim that a minimal separating set can never be found in polynomial time. For one thing, we have assumed nothing about the structure of the table (b_{ij}). It is possible that when (b_{ij}) is actually a modified character table for some group, it has properties which could allow us to find a separating set more efficiently. Also, there may be other ways to find a separating set besides simply examining the character table.

It is mentioned in [13] that MINIMUM TEST COLLECTION has a greedy approximation algorithm which produces a collection within $1 + 2 \ln |S|$ of optimal. It is further shown that improving upon this approximation is NP-complete. In Section 3.1 we mention a greedy algorithm for SEPARATING SET; it would be in-

teresting to consider whether a similar bound can be shown to apply for it.

Appendix B

Program for Computing r-trees and Separating Sets for W_n

B.1 `sepset.cc`

Given a character table, computes separating sets. Contains functions for computation by either brute force or a greedy algorithm.

```
#include <bitset>
#include <vector>
#include <iostream>
#include <stdio.h>
#include <algorithm>
#include <sys/time.h>

#if (__GNUC__ < 3)
#error g++ 2.x miscompiles bitset!
#endif

// #define QUIET

using namespace std;

// Due to limitations of the bitset class, the size of the character
// table must be defined at compile time.

#define CLASSES 5
#define REPS 5

#define CHOOSE2(n) (((n)*((n)-1))/2)

int table[REPS][CLASSES];

typedef bitset<CHOOSE2(REPS)> bs;

bs seps[CLASSES];

int get_int(istream& is) {
  while (is) {
    char c;
    is.get(c);
    switch (c) {
    case '0' ... '9' :
    case '+':
    case '-':
    case '.':
      is.putback(c);
      goto done;
      break;
```

```
    default:
      break;
    }
  }
 done:
  int i;
  is >> i;
  return i;
}

void get_table (void) {
  for (int i = 0; i < REPS; i++)
    for (int j = 0; j < CLASSES; j++)
      table[i][j] = get_int(cin);
}

int gcd(int a, int b) {
  if (b == 0)
    return a;
  else
    return gcd(b, a % b);
}

int lcm(int a, int b) {
  return a * b / gcd(a,b);
}

int get_lcm (void) {
  int k = 1;
  for (int i = 0; i < REPS; i++)
    k = lcm(k,table[i][0]);
  return k;
}

void make_eigenvalues (void) {
  int k = get_lcm();
#ifndef QUIET
  printf("LCM = %d\n", k);
#endif
  for (int i = 0; i < REPS; i++) {
    int dim = table[i][0];
    assert(k % dim == 0);
    for (int j = 0; j < CLASSES; j++) {
      table[i][j] *= (k / dim);
    }
  }
}

void make_seps (void) {
  for (int cl = 0; cl < CLASSES; cl++) {
    int serial = 0;
    seps[cl].reset();
    for (int i = 0; i < REPS; i++) {
      for (int j = i + 1; j < REPS; j++) {
        assert(serial < seps[cl].size());
        seps[cl].set(serial++, table[i][cl] == table[j][cl]);
      }
    }
  }
}

void find_sep_set_2 (void) {
  for (int a = 0; a < CLASSES; a++) {
```

```
    for (int b = a+1; b < CLASSES; b++) {
      bs x = seps[a] & seps[b];
      if (x.none()) {
        printf("Found %d,%d\n",a+1,b+1);
        //cout << x << endl;
      }
    }
  }
}

// brute force for a 3-size set

void find_sep_set_3 (void) {
  for (int a = 0; a < CLASSES; a++) {
    for (int b = a+1; b < CLASSES; b++) {
      for (int c = b+1; c < CLASSES; c++) {
        bs x = seps[a] & seps[b] & seps[c];
        if (x.none()) {
          printf("Found %d,%d,%d\n",a+1,b+1,c+1);
          //cout << x << endl;
        }
      }
    }
  }
}

void find_sep_set_4 (void) {
  int i = 0;
  for (int a = 0; a < CLASSES; a++) {
    for (int b = a+1; b < CLASSES; b++) {
      for (int c = b+1; c < CLASSES; c++) {
        for (int d = c+1; d < CLASSES; d++) {
          bs x = seps[a] & seps[b] & seps[c] & seps[d];
          if (x.none()) {
            printf("$\\{ %d,%d,%d,%d \\}$",a+1,b+1,c+1,d+1);
            if (++i % 4 == 0)
              printf(" \\\\ \\hline\n");
            else
              printf(" &\n");
          }
        }
      }
    }
  }
}

bs already_got;

bool bs_comp(const bs *a, const bs *b) {
  if (!a)
    return false;
  if (!b)
    return true;
  bs aa = ~*a & already_got;
  bs bb = ~*b & already_got;
  return aa.count() > bb.count();
}



int greedy(void) {
  bs *s[CLASSES];
  int sepset[CLASSES];
```

```
  int sepsetsize = 0;
  int size = 0;
  for (int i = 0; i < CLASSES; i++) s[i] = &seps[i];
  already_got.set();
  while (already_got.any()) {
    sort(s, s + CLASSES, bs_comp);
    assert(s[0]);
    bs **p = &s[0];
    while (!*p) p++;

    already_got &= **p;
    sepset[sepsetsize++] = *p - seps;
    printf("Using number %d\n", *p - seps + 1);
    cout << "Added\t\t" << **p << endl;
    cout << "Now have\t" << already_got << endl;
    cout << "Any left:\t" << already_got.any() << endl;
    *p = NULL;
    size++;
  }
  printf("Found separating set of size %d:", size);
  for (int j = 0; j < sepsetsize; j++)
    printf(" %d", sepset[j]+1);
  printf("\nRelevant columns:\n");
  for (int i = 0; i < REPS; i++) {
    for (int j = 0; j < sepsetsize; j++)
      printf("%2d ", table[i][sepset[j]]);
    printf("\n");
  }
  return sepsetsize;
}

int main(void) {
  get_table();
#ifndef QUIET
  for (int i = 0; i < REPS; i++) {
    for (int j = 0; j < CLASSES; j++)
      printf("%2d ", table[i][j]);
    printf("\n");
  }
  printf("\n");
#endif
  make_eigenvalues();
#ifndef QUIET
  for (int i = 0; i < REPS; i++) {
    for (int j = 0; j < CLASSES; j++)
      printf("%2d ", table[i][j]);
    printf("\n");
  }
#endif
  make_seps();
  for (int cl = 0; cl < CLASSES; cl++) {
    //cout << cl << ":\t\t" << seps[cl] << endl;
  }
  find_sep_set_2();
  //greedy();
  return 0;
}
```

B.2 Makefile

Controls compilation of all other files.

```
CXX = g++32
CFLAGS = -Wall -g -W -I /usr/local/include # -pg
LDFLAGS = -L /usr/local/lib -lgmp

PROGS = gen_rtrees count_rtrees conjclasses_main

all : $(PROGS)

sepset : sepset.o
        $(CXX) -o $@ $> $(LDFLAGS)

#compute_reps : compute_reps.o rtree.o wreath.o conjclasses.o
#       $(CXX) -o $@ $> $(LDFLAGS)

gen_rtrees : gen_rtrees.o rtree.o wreath.o
        $(CXX) -o $@ $> $(LDFLAGS)

count_rtrees : count_rtrees.o rtree.o wreath.o
        $(CXX) -o $@ $> $(LDFLAGS)

conjclasses_main : conjclasses_main.o conjclasses.o rtree.o wreath.o
        $(CXX) -o $@ $> $(LDFLAGS)


clean :
        rm -f $(PROGS) *.o

deps : *.cc *.h
        $(CXX) -MM *.cc >deps

.include "deps"
```

B.3 wreath.h

Header file for wreath product-related utility functions.

```
#ifndef WREATH_H
#define WREATH_H

#include <vector>

using namespace std;

extern const int primes[];
extern const int nprimes;
extern const int maxprime;
bool isprime(int n);
int gcd(int a, int b);
int lcm(int a, int b);
int compute_mu(int n);

void compute_mus(int maxn);
int mu(int n);
```

```
#endif
```

B.4 wreath.cc

Utility routines related to wreath products.

```
#include <assert.h>
#include <vector>
#include "wreath.h"

const int primes[] = {
  2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,
  61,67,71,73,79,83,89,97,101,103,107,109,113,127,
  131,137,139,149,151,157,163,167,173,179,181,191,
  193,197,199
};

const int nprimes = sizeof(primes);
const int maxprime = 199;

static vector<int> mu_values;

void compute_mus(int maxn)
{
  for (int n = mu_values.size(); n <= maxn; n++)
    mu_values.push_back(compute_mu(n));
}

int mu(int n)
{
  compute_mus(n);
  return mu_values[n];
}


int compute_mu(int n)
{
  assert(n <= maxprime);
  int t = 0;
  for (int i = 0; primes[i] <= n; i++)
    {
      if (n % primes[i] == 0)
        {
          n /= primes[i];
          if (n % primes[i] == 0) // has two factors of primes[i]
            return 0;
          else
            t++;
        }
    }
  return (t % 2 == 0) ? 1 : -1;
}

bool isprime(int n)
{
  switch (n) {
  case 2:
```

```
  case 3:
  case 5:
  case 7:
  case 11:
  case 13:
  case 17:
  case 19:
  case 23:
  case 29:
  case 31:
  case 37:
    return true;
  default:
    if (n % 2 == 0)
      return false;
    for (int i = 3; i*i <= n; i += 2) {
      if (n % i == 0)
        return false;
    }
    return true;
  }
}

int gcd(int a, int b) {
  if (b == 0)
    return a;
  else
    return gcd(b, a % b);
}

int lcm(int a, int b) {
  return a * b / gcd(a,b);
}
```

B.5 `rtree.h`

Header file for r-tree computation routines.

```
#ifndef RTREE_H
#define RTREE_H

#include <assert.h>

#include <string>
#include <iostream>
#include <vector>
#include <deque>
#include <set>

#include "wreath.h"

using namespace std;

#include <gmpxx.h>

inline ostream & operator<<(ostream &o, mpz_srcptr z)
{
  char *s = mpz_get_str(NULL, 10, z);
```

```
  ostream& r = (o << s);
  free(s);
  return r;
}

template<class It> ostream& dump_range(It i, It end, ostream& os)
{
  for (; i != end; ++i)
    os << *i << ' ';
  os << endl;
  return os;
}

template<class Cont> ostream& dump(const Cont& c, ostream& os)
{
  return dump_range(c.begin(), c.end(), os);
}



// number of r-trees

typedef mpz_class bint;

inline bint bpow(const bint& b, unsigned int e)
{
  bint r;
  mpz_pow_ui(r.get_mpz_t(), b.get_mpz_t(), e);
  return r;
}

bint count_rtrees(int n, int r);

// rtree stuff

struct rtree {
  int r;
  vector<rtree *> kids;
  mutable int d;
  int root;
  mutable bint dim;

  rtree (int r_) : r(r_), kids(r_, (rtree *)0), d(0), root(0), dim(0) { };

  bool isleaf () const { return !kids[0]; }

  void makeleaf (int root_) { assert(isleaf()); root = root_; dim = 1; }

  friend bool rpequal(const rtree *a, const rtree *b);
  int get_d () const;
  const bint& get_dim () const;
  ostream& print(ostream&) const;
  ostream& print_parsetree (ostream&) const;
  int get_height() const {
    if (isleaf())
      return 0;
    else
      return kids[0]->get_height() + 1;
  }
};

bool rpequal (const rtree* a, const rtree* b);
```

```
inline bool operator== (const rtree& a, const rtree& b)
{
  return rpequal(&a, &b);
}

inline bool operator!= (const rtree& a, const rtree& b)
{
  return !(a == b);
}

inline ostream& operator<< (ostream& os, const rtree& rt) {
  return rt.print(os);
}

extern const int max_depth;

extern vector<rtree> all_rtrees[];

extern int all_r; // all_rtrees depends on r, so it only makes sense for r to be fixed

void clear_all_rtrees(void);

void generate_all_rtrees(int depth, int r);

bint wr_order(int n, int r);

#endif
```

B.6 rtree.cc

Computes all r-trees of desired height and r.

```
#include <assert.h>

#include <string>
#include <iostream>
#include <vector>
#include <deque>
#include <set>

#include "wreath.h"
#include "rtree.h"

using namespace std;

#include <gmpxx.h>

bint count_rtrees(int n, int r)
{
  if (n == 0)
    return r;
  bint lastk = count_rtrees(n-1, r);
  bint sum;
  for (int c = 1; c <= r; c++)
    {
      if (r % c != 0)
        continue;
      for (int d = 1; d <= c; d++)
        {
```

```
          if (c % d != 0)
            continue;
          sum += bpow(lastk, r/c) * (mu(c/d)*d*d);
        }
    }
  return sum / r;
}

bool rpequal (const rtree* a, const rtree* b)
{
  if (a == b)
    return true;
  if (!a || !b)
    return false; // one is null, hence other is not
  if (a->r != b->r || a->root != b->root)
    return false;
  for (int i = 0; i < a->r; i++)
    {
      if (!rpequal(a->kids[i], b->kids[i]))
        return false;
    }
  return true;
}

int rtree::get_d () const
{
  if (d)
    return d;
  for (int i = 1; i < r; i++)
    {
      if (r % i != 0)
        continue;
      // attempt to cycle by i
      bool ok = true;
      for (int j = 0; j < r - i; j++)
        {
          if (!rpequal(kids[j], kids[j+i]))
            {
              ok = false;
              break;
            }
        }
      if (ok)
        {
          // the subgroup of Z/rZ generated by i is isomorphic to Z/(r/i)Z
          d = r/i;
          return d;
        }
    }
  // Z/1Z ~= <1> trivially stabilizes, and no other one worked.
  d = 1;
  return d;
}

const bint& rtree::get_dim () const
{
  if (dim != 0)
    return dim;
  if (isleaf())
    {
      dim = 1;
      return dim;
    }
```

```
  dim = 1;
  for (int i = 0; i < r; i++)
    {
      assert(kids[i]);
      dim *= kids[i]->get_dim(); // tensored
    }
  // induce: index of G wr Z_d in G wr Z_r is r/d
  dim *= (r/d);
  return dim;
}

ostream& rtree::print(ostream& os) const
{
  if (isleaf())
    os << "(" << root << ")";
  else
    {
      os << "(" << root;
      for (int i = 0; i < r; i++)
        {
          assert(kids[i]);
          os << " ";
          kids[i]->print(os);
        }
      os << ")";
    }
  return os;
}

ostream& rtree::print_parsetree (ostream& os) const
{
  if (isleaf())
    os << " ." << root << ". ";
  else
    {
      os << "( ." << root << ". ";
      for (int i = 0; i < r; i++)
        {
          assert(kids[i]);
          os << " ";
          kids[i]->print_parsetree(os);
        }
      os << ") ";
    }
  return os;
}

// want to iterate over all length l vectors of {0,1,...,n-1} which are not
// cyclic permutations of each other.

typedef deque<int> cvec;

template<class T> static void cycle_right(T& v)
{
  v.push_back(v.front());
  v.pop_front();
}

template<class T> static void cycle_left(T& v)
{
  v.push_front(v.back());
  v.pop_back();
}
```

```
class cvec_gen {
  int n;
  int len;
  bool alldone;
  cvec v;
  set<cvec> seen;

public:
  cvec_gen (int n_, int len_)
    : n(n_), len(len_), alldone(false), v(len,0) { };

  ~cvec_gen () { };

  const cvec& get (void) const
  {
    return v;
  }

  bool done (void) const
  {
    return alldone;
  }

public:
  void next (void);
};

// return true if overflow
static bool incv (cvec::iterator i, cvec::iterator end, int base)
{
  if (i == end)
    return true;
  assert(*i < base);
  if (++*i >= base)
    {
      *i = 0;
      return incv(++i, end, base);
    }
  else
    return false;
}

void cvec_gen::next (void)
{
  // save what we've seen
  seen.insert(v);

  while (!(alldone = incv(v.begin(), v.end(), n)))
    {
      cvec v1(v);
      bool ok = true;
      for (int i = 0; i < len; i++)
        {
          if (seen.find(v1) != seen.end())
            {
              ok = false;
              break;
            }
          cycle_left(v1);
        }
      if (ok)
        break;
```

```
    }
}


size_t estimate_rtree_size(int r) {
  return sizeof(rtree) + r * sizeof(rtree *);
}

// rtree generation

const int max_depth = 10;

vector<rtree> all_rtrees[max_depth];

int all_r; // all_rtrees depends on r, so it only makes sense for r to be fixed

void clear_all_rtrees(void)
{
  for (int i = 0; i < max_depth; i++)
    all_rtrees[i].clear();
}

#if 0
// base r addition.  lsb stored first
// return true if carry out

bool inc_base_r(int *num, int len, int base)
{
  assert(len >= 1);
  assert(base >= 2);
  int carry = 1;
  for (int i = 0; i < len && carry; i++)
    {
      assert(num[i] < base);
      num[i] += carry;
      if (num[i] == base)
        {
          num[i] = 0;
          carry = 1;
        }
      else
        carry = 0;
    }
  return carry;
}
#if 0
bool inc_base_r(int *num, int len, int base)
{
  assert(base >= 2);
  if (len == 0)
    return true;
  else
    {
      assert(*num < base);
      if (++*num >= base)
        return inc_base_r(num+1, len-1, base);
      else
        return false;
    }
}
#endif
#endif
```

```
void generate_all_rtrees(int depth, int r)
{
  if (r != all_r)
    {
      clear_all_rtrees();
      all_r = r;
    }
  if (!all_rtrees[depth].empty())
    return; // already done
  if (depth == 0)
    {
      for (int i = 0; i < r; i++)
        {
          rtree rt(r);
          rt.makeleaf(i);
          all_rtrees[depth].push_back(rt);
        }
    }
  else
    {
      generate_all_rtrees(depth - 1, r);

      bint needed = count_rtrees(depth, r);
      bint done = 0;

      cerr << "Generating " << needed << " rtrees with n=" << depth
           << ", r=" << r << endl;
      cerr << "This will take about " << needed * estimate_rtree_size(r)
           << " bytes" << endl;

      int n_subtrees = all_rtrees[depth - 1].size();
      for (cvec_gen cvg(n_subtrees, r); !cvg.done(); cvg.next())
        {
          rtree rt(r);
          const cvec& v = cvg.get();
          for (int i = 0; i < r; i++)
            rt.kids[i] = &all_rtrees[depth - 1][v[i]];
          int d = rt.get_d();
          for (int j = 0; j < d; j++)
            {
              rt.root = j * (r/d);
              all_rtrees[depth].push_back(rt);
              if (++done % 100 == 0)
                cerr << "Done with " << done << " of " << needed << "    \r";
            }
        }
      cerr << endl;
    }
}

bint wr_order(int n, int r)
{
  if (n == 1)
    return r;
  else
    return bpow(wr_order(n-1, r), r) * r;
}
```

B.7 gen_rtrees.cc

Driver program to generate and print out rtrees.

```
// FIXME: indexing here sucks

#include "rtree.h"

int main(int argc, char *argv[])
{
  assert(argc >= 3);
  int n = atoi(argv[1]);
  int r = atoi(argv[2]);
  generate_all_rtrees(n-1, r); // n is 1-based but depth is 0-based
  for (int i = 0; i < n; i++)
    {
      cout << all_rtrees[i].size() << " rtrees of height " << i
           << " (should be " << count_rtrees(i, r) << ")" << endl;
      bint dimsum = 0;

      for (unsigned j = 0; j < all_rtrees[i].size(); j++)
        {
          all_rtrees[i][j].print(cout);
          const bint& dim = all_rtrees[i][j].get_dim();
          cout << " [dim=" << dim << "]" << endl;
          dimsum += dim * dim;
        }
      bint real_dim = wr_order(i+1, r);
      cout << "Total dimension is " << dimsum << " (should be "
           << real_dim << ")" << endl;
    }
  return 0;
}
```

B.8 conjclasses.cc

Computes conjugacy class representatives and sizes for corresponding r-trees.

```
#include <sstream>
#include <iostream>
#include <string>
#include "rtree.h"
#include "conjclasses.h"



// hack: string(n, 'A' + i) doesn't work
static inline string dup_char(int n, char c)
{
  return string(n,c);
}


// Compute a representative of the conjugacy class corresponding
// to the given rtree.  Returns a string giving a product of
// generators A..Z and their inverses a..z.
```

```
string class_rep(const rtree& rt) {
  assert(isprime(rt.r)); // for now
  int n = rt.get_height();
  int r = rt.r;
  int d = rt.get_d();
  if (n == 0)
    return dup_char(rt.root, 'A' + 0);
  else
    {
      string s;

      if (rt.root == 0) {
        for (int i = 0; i < r; i++) {
          // look at kids.  Conjugate each to shift it into position.
          s += dup_char(i, 'A' + n)
            + class_rep(*rt.kids[i])
            + dup_char(i * (r-1), 'A' + n); // inverse
          // really dup_char(i, 'a' + n);
          // for non-prime case we'd have something
          // involving dup_char((r/d)*root % r, 'A' + n)
        }
      } else {
        assert(d == r);
        // all kids are the same.  Take one copy, in first position,
        // and z^k is tacked on the back
        s = class_rep(*rt.kids[0]) + dup_char(rt.root, 'A' + n);
        // non-prime case again will have r/d
      }
      return s;
    }
}

bint class_size(const rtree& rt) {
  assert(rt.r == 2);
  if (rt.get_height() == 0) // i.e. an element of W_1,r
    return 1;
  if (rt.root == 0) {
    const rtree kid0 = *(rt.kids[0]), kid1 = *(rt.kids[1]);
    if (kid0 == kid1) {
      bint k0size = class_size(kid0);
      return k0size * k0size;
    } else {
      return 2 * class_size(kid0) * class_size(kid1);
    }
  } else {
    assert(rt.root == 1);
    // all kids are same
    return class_size(*rt.kids[0]) * wr_order(rt.get_height(), rt.r);
  }
}

static string gen_to_cycle(char c) {
  ostringstream ost;
  int n = c - 'A';
  int ts = (1 << n); // leaves on this subtree
  for (int i = 1; i <= ts; i++) {
    ost << "(" << i << "," << (i + ts) << ")";
  }
  return ost.str();
}

string gens_to_cycle(const string& gens) {
  ostringstream ost;
```

```
  for (string::const_iterator i = gens.begin(); i != gens.end(); ++i) {
    if (i != gens.begin())
      ost << "*";
    ost << gen_to_cycle(*i);
  }
  return ost.str();
}
```

B.9 conjclasses_main.cc

Driver program to print out conjugacy class representatives.

```
#include <string>
#include <iostream>
#include "conjclasses.h"
#include "rtree.h"

int main(int argc, char *argv[]) {
  assert(argc >= 2);
  int n = atoi(argv[1]);
  generate_all_rtrees(n-1, 2);
  vector<rtree>& treelist = all_rtrees[n-1];
  for (vector<rtree>::iterator i = treelist.begin();
       i != treelist.end(); ++i) {
#if 1
    cout << " & \\begin{parsetree} ";
    i->print_parsetree(cout);
    cout << "\\end{parsetree} \\quad \\quad \\\\ \\hline" << endl;
#endif
#if 0
    cout << ": " << gens_to_cycle(class_rep(*i))
         << " [size=" << class_size(*i) << "]" << endl;
    cout << gens_to_cycle(class_rep(*i)) << ", ";
#endif
  }
  cout << endl;
  return 0;

}
```

Bibliography

[1] Ruben Arenas, Nathaniel Eldredge, and Michael E. Orrison. Efficient eigenspace projections with compression. Technical report, Harvey Mudd College, 2002. In progress. Develops an efficient algorithm for repeately projecting vectors onto eigenspaces of diagonalizable operators in large-dimensional vector spaces.

[2] Michael Clausen and Ulrich Baum. *Fast Fourier Transforms*. BI-Wissenschaftsverlag, Mannheim, 1993. Describes various fast Fourier transform algorithms, from Cooley-Tukey to the present, including the underlying algebra, complexity analysis, and extensions to various nonabelian groups, including S_n.

[3] A.H. Clifford. Representations induced in an invariant subgroup. *Ann. of Math. (2)*, 38(3):533–550, July 1937. The paper which founded Clifford theory. Describes the process of inducing representations from invariant (i.e. normal) subgroups, and proves theorems about when they are irreducible.

[4] J.W. Cooley and J.W. Tukey. An algorithm for machine calculation of complex Fourier series. *Math. Comp.*, 19:297–301, 1965. The paper which initially presented the revolutionary fast Fourier transform algorithm.

[5] Persi Diaconis. A generalization of spectral analysis with application to ranked data. *Ann. Statist.*, 17(3):949–979, 1989. Uses isotypic projections in representations of the symmetric group to analyze ranked data, with special emphasis on election results.

[6] Persi Diaconis and Curtis Greene. Applications of Murphy's elements. Technical Report 335, Dept. of Statistics, Stanford University, 1989. Describes several important properties of the Jucys-Murphy elements, including that they are diagonal in the seminormal basis, and that they can generate class sums. Includes a method for constructing analogues in other groups.

[7] Y. Drozd and V. Kirichenko. *Finite-dimensional algebras*. Springer-Verlag, 1994.

[8] David S. Dummit and Richard M. Foote. *Abstract Algebra*. Prentice Hall, second edition, 1999. An excellent general algebra text.

[9] Richard Foote, Gagan Mirchandani, Daniel N. Rockmore, Dennis Healy, and Tim Olson. A wreath product group approach to signal and image processing. I. Multiresolution analysis. *IEEE Trans. Signal Process.*, 48(1):102–132, 2000. An application of wreath product Fourier transforms to image processing. An image can be thought of as a signal on a tree on which an iterated wreath product of cyclic groups acts, and the Fourier transform of this signal picks out details of the image which appear at different resolutions.

[10] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.3*, 2002. `(http://www.gap-system.org)`. An advanced software package for computational discrete algebra. Particularly useful when working with permutation groups.

[11] Michael R. Garey and David S. Johnson. *Computers and intractability*. W. H. Freeman and Co., San Francisco, Calif., 1979. An invaluable text on NP-completeness. Contains a complete discussion of the theory, and an extensive dictionary of NP-complete problems.

[12] W. Gentleman and G. Sande. Fast Fourier transforms for fun and profit. In

Proc. AFIPS, Joint Computer Conference, volume 29, pages 563–578, 1966. Describes the Gentleman-Sande FFT.

[13] Bjarni V. Halldórsson, Magnús M. Halldórsson, and R. Ravi. On the approximability of the minimum test collection problem. In Friedhelm Meyer auf der Heide, editor, *Algorithms — ESA 2001*, volume 2161 of *Lecture Notes in Computer Science*, pages 158–169. Springer, 2001. Shows that the greedy algorithm for MINIMUM TEST COLLECTION yields the best possible polynomial-time approximation, together with other results about the problem.

[14] Gordon D. James and Martin W. Liebeck. *Representations and characters of groups*. Cambridge University Press, 1993. A quite elementary introduction to representation theory, assuming only the most basic abstract algebra.

[15] G. Karpilovsky. *Clifford Theory for Group Representations*. Number 156 in North-Holland Mathematics Studies. Elsevier, 1989. Of particular interest is the last chapter, which describes how representations of a group can be induced from normal subgroups; this is useful for us in constructing the representations of a wreath product from its (normal) factors.

[16] Adalbert Kerber. *Representations of Permutation Groups I*. Number 240 in Lecture Notes in Mathematics. Springer-Verlag, 1971. An entire book on the representation theory of wreath products. Contains constructions of representations, combinatorial results, and all manner of useful facts about these groups.

[17] Adalbert Kerber. *Representations of Permutation Groups II*. Number 495 in Lecture Notes in Mathematics. Springer-Verlag, 1975. Continuation of [16].

[18] David K. Maslen and Daniel N. Rockmore. The Cooley-Tukey FFT and group theory. *Notices Amer. Math. Soc.*, 48(10):1151–1160, 2001. Written for general

scientific readers, this paper describes the Fourier transform in terms of group theory. Discusses the Cooley-Tukey fast Fourier transform algorithm and how it can be generalized to other groups, including the symmetric group.

[19] G. Murphy. The idempotents of the symmetric group and Nakayama's conjecture. *J. Algebra*, 69(2):287–297, 1981.

[20] Elizabeth Norton. Data compression on the symmetric group. Technical report, Harvey Mudd College, 2002. Senior thesis outlining a technique for compressing data vectors in S_n-modules by eliminating linearly dependent components.

[21] Andrei Okounkov and Anatoly Vershik. A new approach to representation theory of symmetric groups. *Selecta Math. (N.S.)*, 2(4):581–605, 1996. This paper constructs the representation theory of the symmetric group using Jucys-Murphy elements from the ground up. Suggests generalizations to other groups.

[22] R.C. Orellana, M.E. Orrison, and D.N. Rockmore. Rooted trees and iterated wreath products of cyclic groups. In progress. Describes quite concretely the representation theory of iterated wreath products $Z_r \wr \cdots \wr Z_r$, particulary as symmetry groups of r-ary trees., 2002.

[23] Michael E. Orrison. *An Eigenspace Approach to Decomposing Representations of Finite Groups*. PhD thesis, Dartmouth College, 2001. Describes the technique of decomposing group representations as direct sums of eigenspaces which are the irreducible representations. Considers operators yielding these eigenspaces in several groups, including symmetric, hyperoctahedral, and general linear groups.

[24] Arun Ram. Seminormal representations of Weyl groups and Iwahori-Hecke algebras. *Proc. London Math. Soc. (3)*, 75(1):99–133, 1997. Generalizes the Jucys-Murphy elements to several types of Weyl groups.

[25] Daniel N. Rockmore. Fast Fourier transforms for wreath products. *Appl. Comput. Harmon. Anal.*, 2(3):279–292, 1995. Construct a Cooley-Tukey style FFT algorithm on general wreath product groups $G \wr S_n$.

[26] Bruce E. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Number 203 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 2001. A very readable book with an excellent review of representation theory, and construction of the Specht modules as irreducible representations of the symmetric group.

[27] Michael Sipser. *Introduction to the Theory of Computation*. PWS Publishing Company, 1997. A useful elementary text, explaining issues of computational decidability, intractability, NP-completeness, and so on.

[28] David Uminsky. Generalized spectral analysis on large sets of approval voting data. Technical report, Harvey Mudd College, 2002. Senior thesis describing techniques for detecting voter coalitions via spectral analysis with respect to the symmetric group.

[29] James S. Walker. Fourier analysis and wavelet analysis. *Notices Amer. Math. Soc.*, 44(6):658–670, 1997. Contains an expository overview of the theory of wavelets as it relates to Fourier analysis. A good introduction to the topic.