

## FAST FOURIER TRANSFORMS FOR THE ROOK MONOID

MARTIN MALANDRO AND DAN ROCKMORE

**ABSTRACT.** We define the notion of the Fourier transform for the rook monoid (also called the symmetric inverse semigroup) and provide two efficient divide-and-conquer algorithms (fast Fourier transforms, or FFTs) for computing it. This paper marks the first extension of group FFTs to nongroup semigroups.

### 1. INTRODUCTION

The rook monoid  $R_n$ , also called the symmetric inverse semigroup, is the set of all partial permutations of  $\{1, \dots, n\}$  under function composition; i.e., it is the semigroup of all bijections between all subsets of  $\{1, \dots, n\}$  under function composition, with the usual rule for composing partial functions. That is,  $g \circ f$  is defined for precisely the elements  $x$  for which  $x \in \text{dom}(f)$  and  $f(x) \in \text{dom}(g)$ . It is called the rook monoid because it is isomorphic to the semigroup of all  $n \times n$  matrices with the property that at most one entry in each row is 1 and at most one entry in each column is 1 (the rest being 0) under multiplication. Such matrices (called *rook matrices*) correspond to the set of all possible placements of nonattacking rooks on an  $n \times n$  chessboard. For example, consider the element  $\sigma \in R_4$  defined by

$$\sigma(2) = 1, \quad \sigma(4) = 4.$$

Then, viewed as a partial permutation,  $\sigma$  is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & 1 & - & 4 \end{pmatrix},$$

where the dash indicates that the above entry is not mapped to anything. As a rook matrix, we have

$$\sigma = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

---

Received by the editors September 25, 2007 and, in revised form, June 2, 2008.

2000 *Mathematics Subject Classification*. Primary 20C40, 20M18, 43A30; Secondary 20M30, 68W40.

*Key words and phrases.* Rook monoid, fast Fourier transform, FFT, inverse semigroup, partially ranked data.

The first author was supported by a graduate fellowship.

The second author was supported by AFOSR under grant FA9550-06-1-0027.

©2009 American Mathematical Society  
Reverts to public domain 28 years from publication

In this paper we define the notion of the *Fourier transform* for a  $\mathbb{C}$ -valued function on the rook monoid, and we address the problem of computing it efficiently. We present two distinct fast Fourier transform (FFT) algorithms, both of which make use of tools generalized from group FFT theory [29]. We assume no specialized knowledge. This paper is meant to be readable by group FFT theorists with an interest in semigroups as well as semigroup theorists with an interest in FFTs.

The history of the FFT is an interesting one, beginning, like many subjects in mathematics, with Gauss, who developed the now-classical FFT to efficiently interpolate the orbits of asteroids. This FFT was rediscovered by Cooley and Tukey [7] in 1965 to analyze seismic data. A different FFT was discovered in 1937 by Yates [35], for the analysis of data on factorial designs. The theory of FFTs for abelian groups reconciles these two FFTs. The first is an FFT on  $\mathbb{Z}/n\mathbb{Z}$ , and the second is an FFT on  $(\mathbb{Z}/2\mathbb{Z})^k$ . From this generalization also grew a theory of FFTs for nonabelian groups. For example, we now have FFTs on supersolvable groups, FFTs on the symmetric group, FFTs on compact Lie groups, and FFTs on finite groups of Lie type. For a survey of these results, see [29].

We have both theoretical and practical motivations for creating FFT algorithms for the rook monoid. From a theoretical perspective, these FFTs are significant because they are the first examples of FFTs on a nongroup semigroup. The rook monoid plays the same role for finite inverse semigroups that the symmetric group  $S_n$  does for finite groups in terms of Cayley's theorem: every finite inverse semigroup is isomorphic to a sub-semigroup of some rook monoid (see, e.g. [18], pp. 36–37), so this makes the rook monoid a natural place to begin extending the theory of FFTs to semigroups. Also, just as groups capture symmetry, inverse semigroups capture partial symmetry. See [18] for more on this idea.

From a practical perspective, partially ranked data occur naturally, and the rook monoid provides a nice computational framework for analyzing such data. For example, consider voting data in which some voters do not fully rank all candidates. In practice, this may well be the case. For example, in the 1980 American Psychological Association (APA) presidential election, only a third of the voters cast fully ranked ballots [9]. Say  $f(\sigma)$  is the number of voters who submitted a ballot of type  $\sigma$ . For the  $\sigma$  above,  $f(\sigma)$  would represent the number of voters who ranked candidate 2 in the first position, candidate 4 in the fourth position, and didn't bother ranking candidates 1 and 3. The values  $(\sigma, f(\sigma))$  make up the dataset. There have been previous attempts at spectral analysis for such datasets. For example, in [9], Diaconis used spectral analysis on symmetric groups to analyze the APA election mentioned above. We propose viewing  $f$  as an element of the semigroup algebra  $\mathbb{C}R_n$ , so that the spectral analysis of  $f$  involves projecting it onto the isotypic components of  $\mathbb{C}R_n$  by means of an FFT. Things are more complicated than in the group case because  $\mathbb{C}R_n$  has two natural bases. This means that there are two natural ways to view functions on  $R_n$  as elements of  $\mathbb{C}R_n$ , and therefore two different notions for the convolution of such functions. We will address both in this paper.

Partially ranked voting data is also a type of “not missing at random” (NMAR) data. Missing data in a sample is said to be NMAR if it is believed to be missing, at least in part, because of its unobserved value. In the voting example, any ballot that is not fully ranked is considered NMAR, since the voter intentionally left something on the ballot blank. Consumer survey data frequently contains NMAR data. NMAR data contrasts with randomly missing data, which, in the voting

example, can be caused by accidentally losing some of the ballots. To date, there doesn't seem to be a standard method for analyzing NMAR data. However, the concept of spectral analysis for the rook monoid immediately applies to any NMAR dataset that can be considered a collection of partial rankings. Since spectral analysis is a model-independent approach, spectral analysis for the rook monoid may go a long way towards creating a standard method for dealing with NMAR data.

This paper is organized as follows. Sections 2.1 and 2.2 contain basic definitions and background material about semigroups and the rook monoid. Section 2.3 contains a brief introduction to semigroup representation theory. Sections 2.4 and 2.5 are devoted, respectively, to two important tools in FFT theory: chain-adapted matrix representations and Schur's Lemma, adapted to semigroups.

Section 3 is devoted to basis considerations for semigroup algebras. Section 3.2 defines both natural bases for  $\mathbb{C}R_n$ , and Section 3.3 defines the notion of a Fourier basis. Section 4 defines the Fourier transform.

Section 5 shows how the semigroup algebra  $\mathbb{C}R_n$  decomposes into a product of matrix algebras over group algebras. This has far-reaching implications, some of which are explored in Section 6. Section 6.1 describes explicit matrix representations for  $R_n$ , Section 6.2 contains an explicit Fourier basis description for  $\mathbb{C}R_n$ , and Section 6.3 contains the Fourier inversion theorem for  $\mathbb{C}R_n$ .

In Section 7, we explain some of the issues that arise when choosing how to associate functions on  $R_n$  to elements of  $\mathbb{C}R_n$ . As mentioned previously, this is only an issue because  $\mathbb{C}R_n$  has two natural bases.

Section 8 contains FFT-specific considerations. Computational complexity for FFTs is defined in Section 8.1. Our algorithms for the FFT on  $R_n$  use ideas from group FFT theory, which we cover in Sections 8.2 and 8.3.

Section 9 contains our better FFT algorithm for  $R_n$ . It relies heavily on the decomposition described in Section 5 and the results in Sections 6.1 and 8.3.

Section 10 contains our other FFT algorithm for  $R_n$ . The ideas involved are mainly from Sections 2.4, 2.5, and 8.2. While it is not as efficient as the algorithm given in Section 9, it is constructed in an entirely different way. We present this algorithm because the ideas involved may be useful for constructing FFTs on other semigroups.

## 2. PRELIMINARIES

### 2.1. Definitions for general semigroups.

**Definition** (semigroup). A *semigroup* is a nonempty set  $S$  together with an associative binary operation (which we write multiplicatively).

**Definition** (inverse semigroup). An *inverse semigroup* is a semigroup  $S$  such that, for each  $x \in S$ , there is a *unique*  $y \in S$  such that

$$xyx = x \text{ and } yxy = y.$$

In this case, we write  $y = x^{-1}$ .

We remark that the condition that  $y$  be unique is necessary for this definition. An element  $x \in S$  is said to be *regular* or *Von-Neumann regular* if there is at least one  $y \in S$  satisfying  $xyx = x$  and  $yxy = y$ , and  $S$  is said to be *regular* if every element of  $S$  is regular. Consider the full transformation semigroup  $X$  on the set

$\{1, 2, \dots, n\}$ ; that is, all maps from  $\{1, 2, \dots, n\}$  to itself under composition. It is easy to see that  $X$  is regular, and that (for  $n \geq 2$ ) there exist elements  $x \in X$  for which there are *multiple* elements  $y \in X$  satisfying  $xyx = x$  and  $yxy = y$ .  $X$  is therefore not inverse. An equivalent characterization of inverse semigroups (see, e.g. [18]) is as follows.

**Theorem 2.1** (inverse semigroup). *An inverse semigroup is a semigroup  $S$  which is regular and for which all idempotents of  $S$  commute.*

**Definition** (semigroup algebra). Let  $S$  be a finite semigroup. The *semigroup algebra*  $\mathbb{C}S$  is the formal  $\mathbb{C}$ -span of the symbols  $\{s\}_{s \in S}$ . Multiplication in  $\mathbb{C}S$ , denoted by  $*$ , is given by convolution (i.e., the linear extension of the semigroup operation via the distributive law): Suppose  $f, g \in \mathbb{C}S$ , with

$$f = \sum_{r \in S} f(r)r, \quad g = \sum_{t \in S} g(t)t.$$

Then

$$(1) \quad f * g = \sum_{r \in S} f(r)r \sum_{t \in S} g(t)t = \sum_{s \in S} \sum_{r, t \in S : rt=s} f(r)g(t)s.$$

If  $S$  is a group, then convolution may be written in the familiar way:

$$f * g = \sum_{s \in S} \sum_{r \in S} f(r)g(r^{-1}s)s.$$

Note that convolution here means convolution *in the semigroup algebra*. We hold off on defining a notion of convolution for *functions* on  $S$  until Section 7. We will use the semigroup algebra convolution to define function convolution once we have defined how to associate functions to elements of the semigroup algebra. It turns out that, unlike in the case of groups, there is in general more than one natural way to associate functions on  $S$  to elements of  $\mathbb{C}S$  because, in general,  $\mathbb{C}S$  has more than one natural basis.

## 2.2. Facts about $R_n$ .

**Definition** (rank). Given an element  $\sigma \in R_n$ , the *rank* of  $\sigma$ , denoted  $\text{rk}(\sigma)$ , is defined to be  $\text{rk}(\sigma) = |\text{dom}(\sigma)| = |\text{ran}(\sigma)|$ .

There are two main types of elements of  $R_n$ : the elements of rank  $n$  (i.e., the permutations) and the elements of rank less than  $n$ . In his analysis of the representation theory of  $R_n$ , Munn [27] introduced what he called *cycle-link notation* for the elements of  $R_n$ . As an example, consider the following element  $\sigma \in R_4$ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & - & 2 & 4 \end{pmatrix}.$$

In cycle-link notation, a cycle  $(a_1, a_2, \dots, a_k)$  means that

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_{k-1} \mapsto a_k, \text{ and } a_k \mapsto a_1,$$

and a link  $[b_1, b_2, \dots, b_k]$  means that

$$b_1 \mapsto b_2, b_2 \mapsto b_3, \dots, b_{k-1} \mapsto b_k, \text{ and } b_k \text{ goes nowhere.}$$

The element  $\sigma$ , expressed in cycle-link notation, would be  $[1, 3, 2](4)$ . Note that the cycle-link representation of a permutation always consists of cycles only, and elements of rank less than  $n$  always contain links when written in cycle-link notation.

**Theorem 2.2.**

$$|R_n| = \sum_{k=0}^n \binom{n}{k}^2 k!$$

*Proof.* For any particular rank  $k$ , there are  $\binom{n}{k}$  choices for the domain and  $\binom{n}{k}$  choices for the range of an element of  $R_n$ , and for any particular choice of domain and range, there are  $k!$  ways of mapping the domain to the range.  $\square$

We also have the recursive formula

**Theorem 2.3.** *For  $n \geq 3$ ,*

$$(2) \quad |R_n| = 2n|R_{n-1}| - (n-1)^2|R_{n-2}|.$$

*Proof.* See Section 10.3.  $\square$

**Theorem 2.4.**  *$R_n$  is an inverse semigroup.*

*Proof.* For an element  $\sigma \in R_n$ , define  $\gamma \in R_n$  by

$$\begin{aligned} \text{dom}(\gamma) &= \text{ran}(\sigma), \text{ and, for } x \in \text{dom}(\gamma), \\ \gamma(x) &= \sigma^{-1}(x). \end{aligned}$$

It is easy to see that  $\gamma\sigma\gamma = \gamma$  and  $\sigma\gamma\sigma = \sigma$ , and that  $\gamma$  is the only element of  $R_n$  satisfying both equations.  $\square$

**2.3. Semigroup representations.** Here we provide a brief introduction to the representation theory of semigroups. For a more complete introduction to this topic, see [28] and [34].

In this paper, we adopt the convention that all maps act on the left of sets, and we only consider left modules. We also only concern ourselves with finite semigroups. For the rest of the paper, every semigroup discussed is understood to be finite. Let  $S$  be a semigroup. If  $S$  does not have identity, then let  $S^1$  denote  $S$  with an identity element added. If  $S$  does have identity, then let  $S^1 = S$ .

**Definition** (semigroup representation). A *representation* of  $S$  is a finite dimensional  $\mathbb{C}$ -vector space  $V$  together with a homomorphism  $\rho$  from  $S$  into the semigroup  $\text{End}(V)$  under composition.

*Remark.* If  $S$  is a group, this definition does not agree with the usual group definition, which requires  $\rho(e) = 1 \in \text{End}(V)$ . Such representations are called *unital*. However, there is only a trivial difference between a representation and a unital representation of  $S^1$ : a representation is called *null* if  $\rho(s) = 0$  for all  $s \in S$ , and every representation of  $S^1$  is either unital, null, or a direct sum of a unital and a null representation ([28], Fact 1.10).

**Definition** (semigroup matrix representation). A *matrix representation* of  $S$  is a representation of  $S$  with respect to a particular choice of basis for  $V$ ; i.e., it is a homomorphism from  $S$  into the semigroup of  $\dim(V) \times \dim(V)$  matrices with entries in  $\mathbb{C}$  under multiplication.

**Definition** (representation module). A *representation module* for  $S$  is a  $\mathbb{C}S$ -module that is also a finite dimensional  $\mathbb{C}$ -vector space.

**Definition** (matrix representation of  $\mathbb{C}S$ ). A *matrix representation* of the semi-group algebra  $\mathbb{C}S$  is an algebra homomorphism  $\rho$  from  $\mathbb{C}S$  into the matrix algebra  $M_{d_\rho}(\mathbb{C})$ .

Given a representation  $\rho$  of  $S$ , we may create a representation module for  $S$  by viewing the underlying vector space  $V$  as a  $\mathbb{C}S$ -module, where the action of  $S$  on  $V$  is given by  $\rho$ , and the action of  $\mathbb{C}S$  on  $V$  is given by the linear extension of  $\rho$ . In this case, we call  $V$  (as a  $\mathbb{C}S$ -module) the *representation module for  $\rho$* . Conversely, given a  $\mathbb{C}S$ -module  $V$  which is also a finite dimensional  $\mathbb{C}$ -vector space, we may define a representation  $\rho : S \rightarrow \text{End}(V)$  by  $\rho(s) \cdot v = s \cdot v$  for all  $s \in S$  and  $v \in V$ . In this case, we call  $\rho$  the *representation associated to  $V$* . Furthermore, a matrix representation of  $\mathbb{C}S$  defines a matrix representation of  $S$  by restricting to a basis, and any matrix representation of  $S$  extends linearly to a matrix representation of  $\mathbb{C}S$ . Matrix representations of  $S$  and of  $\mathbb{C}S$  are therefore in one-to-one correspondence, and the notions of representations, matrix representations, and representation modules for  $S$  are equivalent. We shall move between these notions freely as needed.

Also, we will often abuse the language and simply refer to a representation or matrix representation  $\rho$  of  $S$ , where the underlying vector space  $V$  is understood.

**Definition** (irreducible representation). A nonnull representation  $\rho$  of  $S$  is said to be *irreducible* if the representation module for  $\rho$  is nonnull and simple. In other words, with respect to no basis does  $\rho$  have the form

$$\rho = \begin{pmatrix} \phi_1 & 0 \\ g & \phi_2 \end{pmatrix}$$

for some representations  $\phi_1, \phi_2$  and some matrix-valued function  $g$ .

A matrix representation of  $\mathbb{C}S$  is irreducible if and only if the corresponding matrix representation of  $S$  is irreducible.

**Definition** (equivalence of representations). Given two matrix representations  $\rho_1$  and  $\rho_2$  of  $S$  (or of  $\mathbb{C}S$ ),  $\rho_1$  is said to be *equivalent* to  $\rho_2$  if there exists an invertible matrix  $A$  such that  $A\rho_1(s)A^{-1} = \rho_2(s)$  for all  $s \in S$ . Equivalently, two representations of  $S$  are equivalent if their representation modules are isomorphic (as  $\mathbb{C}S$ -modules).

**Theorem 2.5** (decomposing representations). *Suppose that  $\mathbb{C}S$  is semisimple. That is, as a  $\mathbb{C}S$ -module,  $\mathbb{C}S$  is isomorphic to a direct sum of simple  $\mathbb{C}S$ -modules. Then every representation of  $S$  (or of  $\mathbb{C}S$ ) is equivalent to a direct sum of irreducible and null representations of  $S$  (resp.  $\mathbb{C}S$ ). Furthermore, there are only finitely many inequivalent, irreducible representations of  $S$  (resp.  $\mathbb{C}S$ ).*

*Proof.* This is [28], Theorem 1.18 and Proposition 1.19.  $\square$

**Theorem 2.6** (Wedderburn-Artin). *Let  $\mathbb{C}S$  be semisimple, and let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations for  $S$ . For each  $\rho \in \mathcal{Y}$ ,  $\rho : S \rightarrow M_{d_\rho}(\mathbb{C})$ , extend  $\rho$  linearly to  $\tilde{\rho} : \mathbb{C}S \rightarrow M_{d_\rho}(\mathbb{C})$ . Then the family  $\{\tilde{\rho}\}$  defines an isomorphism of algebras*

$$(3) \quad \mathbb{C}S \rightarrow \bigoplus_{\rho \in \mathcal{Y}} M_{d_\rho}(\mathbb{C}).$$

Explicitly,

$$\sum_{s \in S} f(s)s \mapsto \bigoplus_{\rho \in \mathcal{Y}} \tilde{\rho} \left( \sum_{s \in S} f(s)s \right) = \bigoplus_{\rho \in \mathcal{Y}} \left( \sum_{s \in S} f(s)\rho(s) \right).$$

*Proof.* See, for example, [8], [28], [30], or [12, p. 50, exercise 18].  $\square$

**Corollary 2.7** (sum of the squares of the dimensions). *Let  $S$  be a semigroup such that  $\mathbb{C}S$  is semisimple, and let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations for  $S$ . Then*

$$(4) \quad |S| = \sum_{\rho \in \mathcal{Y}} d_{\rho}^2.$$

*Proof.* The formula (4) is just the  $\mathbb{C}$ -dimensionality of the algebras appearing in (3).  $\square$

**Theorem 2.8** (Munn [26], Theorem 3.1).  *$\mathbb{C}R_n$  is semisimple.*

More generally, we have the following extension of Maschke's theorem.

**Theorem 2.9** (Munn [27], Theorem 4.4). *If  $S$  is an inverse semigroup, then  $\mathbb{C}S$  is semisimple.*

**2.4. Adapted representations.** Let  $X_0 < X_1 < \dots < X_n$  be a chain of semigroups whose semigroup algebras  $\mathbb{C}X_i$  are semisimple. Even if a matrix representation of  $X_i$  is irreducible, its restriction to  $X_{i-1}$  will typically not be. However, it will be equivalent to (though not necessarily *equal* to) a direct sum of irreducible and null matrix representations of  $X_{i-1}$ .

**Definition** (adapted representations). Let  $\mathcal{Y}_i$  be a set of inequivalent, irreducible matrix representations for  $X_i$ . The collection  $\{\mathcal{Y}_i\}_{i=0}^n$  is said to be *chain-adapted to the chain*  $X_0 < X_1 < \dots < X_n$  if, for every  $i \geq 1$  and every  $\rho \in \mathcal{Y}_i$ ,  $\rho|_{X_{i-1}}$  is *equal* to a direct sum of null representations and matrix representations in  $\mathcal{Y}_{i-1}$ . Note that this definition forces the irreducible representations appearing in such a restriction to be equal whenever they are equivalent.

Induction shows that a representation from a chain-adapted set of representations may be restricted further down the chain with the same equality results. In particular, if  $\{\mathcal{Y}_i\}_{i=0}^n$  is chain-adapted to  $X_0 < X_1 < \dots < X_n$ , then  $\{\mathcal{Y}_{j_i}\}_{i=1}^k$  is chain-adapted to  $X_{j_1} < X_{j_2} < \dots < X_{j_k}$  for any nonempty subset  $\{j_1 < j_2 < \dots < j_k\}$  of  $\{0, \dots, n\}$ .

We shall often simply ask that a complete set of irreducible representations  $\mathcal{Y}_n$  for  $X_n$  be adapted to the chain  $X_0 < X_1 < \dots < X_n$ . In this case, the choices of the  $\mathcal{Y}_i$  are understood (and, in fact, are often completely determined) by the choice of  $\mathcal{Y}_n$ .

*Remark.* Adapted representations are very important in the construction of FFTs (see [21], for example), but the requirement that a set of representations be adapted is in no way limiting. Given any chain  $X_0 < X_1 < \dots < X_n$  of semigroups whose semigroup algebras  $\mathbb{C}X_i$  are semisimple, a straightforward induction argument shows that a complete set of inequivalent, irreducible, chain-adapted matrix representations always exists. Explicitly describing such sets, however, is frequently a challenging endeavor.

*Remark.* Chain-adapted representations are also sometimes referred to as *seminormal* or *Gelfand-Tsetlin* representations.

**2.5. Schur's Lemma.** Schur's Lemma appears in many forms, the most widely recognized probably being the one below.

**Lemma 2.10** (Schur's Lemma). *Let  $R$  be a ring and let  $M, N$  be simple  $R$ -modules. Then every  $R$ -module homomorphism  $\phi : M \rightarrow N$  is either 0 or an isomorphism. See, e.g., [12], pp. 30-32.*

For computational purposes, the following (also called Schur's Lemma) is a very useful consequence of Lemma 2.10.

**Lemma 2.11** (Schur's Lemma). *Suppose that  $A < B < C$  are semigroups, that  $\mathcal{Y}_A$ ,  $\mathcal{Y}_B$ , and  $\mathcal{Y}_C$  are complete sets of inequivalent, irreducible matrix representations for  $A, B, C$ , respectively, adapted to the chain, and that  $\mathbb{C}A$ ,  $\mathbb{C}B$ , and  $\mathbb{C}C$  are semisimple. Let  $\rho \in \mathcal{Y}_C$ . Say  $\rho|_B = \rho^1 \oplus \cdots \oplus \rho^k$  (with each  $\rho^j$  either in  $\mathcal{Y}_B$  or, without loss of generality, null of dimension 1) and  $\rho^j|_A = \rho_1^j \oplus \cdots \oplus \rho_{g(j)}^j$  (with each  $\rho_i^j$  either in  $\mathcal{Y}_A$  or, again without loss of generality, null of dimension 1). Let  $\sigma \in B$  such that  $\sigma$  commutes with every element of  $A$ . Then  $\rho(\sigma)$  is a block matrix*

$$\rho(\sigma) = \begin{pmatrix} \rho^1(\sigma) & 0 & 0 & \cdots & 0 \\ 0 & \rho^2(\sigma) & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \rho^k(\sigma) \end{pmatrix},$$

where, for  $1 \leq j \leq k$ , the block  $\rho^j(\sigma)$  is itself a block matrix, with blocks indexed by all ordered pairs from  $\{\rho_1^j, \dots, \rho_{g(j)}^j\}$ :

$$\rho^j(\sigma) = \begin{pmatrix} \rho_1^j & \rho_2^j & \cdots & \rho_{g(j)}^j \\ \rho_1^j & \begin{pmatrix} \lambda_{1,1}^j I & \lambda_{1,2}^j I & \cdots & \lambda_{1,g(j)}^j I \\ \lambda_{2,1}^j I & \lambda_{2,2}^j I & \cdots & \lambda_{2,g(j)}^j I \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{g(j),1}^j I & \lambda_{g(j),2}^j I & \cdots & \lambda_{g(j),g(j)}^j I \end{pmatrix} \end{pmatrix},$$

where the  $\lambda_{a,b}^j$  are scalars,  $I$  is the appropriately-sized identity matrix for the block in which it appears, and the block in position  $\rho_a^j, \rho_b^j$  is nonzero only if  $\rho_a^j$  and  $\rho_b^j$  are equivalent representations of  $A$ .

*Proof.* To prove this, we need only show that  $\rho^j(\sigma)$  has the block form indicated above. Let  $V^j$  be the representation module for  $\rho^j$  on  $B$ . Viewing  $V^j$  as a  $\mathbb{C}A$ -module, we have  $V^j = V_1^j \oplus \cdots \oplus V_{g(j)}^j$ , and the  $V_i^j$  are simple  $\mathbb{C}A$ -modules, where the module action on  $V_i^j$  is given by  $\rho_i^j$ . Note that a basis  $\mathcal{B}$  of  $V^j$  has already been chosen by virtue of the fact that  $\rho^j$  is in matrix form, and likewise, bases  $\mathcal{B}_i$  for the  $V_i^j$  are given since  $\rho_i^j$  is in matrix form. Since  $\rho^j$  is adapted, we have that  $\mathcal{B}_i \subseteq \mathcal{B}$  for all  $i$ ,  $\mathcal{B}_i \cap \mathcal{B}_k = \emptyset$  for  $i \neq k$ , the  $\mathcal{B}_i$  are ordered as subsets of  $\mathcal{B}$ , and  $\bigcup \mathcal{B}_i = \mathcal{B}$ .

Since  $\sigma$  commutes with  $A$ , we have that, for all  $v \in V^j$  and  $x \in A$ ,

$$\rho^j(\sigma) \cdot x \cdot v = \rho^j(\sigma x) \cdot v = \rho^j(x\sigma) \cdot v = x \cdot \rho^j(\sigma) \cdot v;$$

i.e.,  $\rho^j(\sigma)$  is a  $\mathbb{C}A$ -linear map from  $V^j$  to itself. Hence

$$\rho^j(\sigma) \in \text{Hom}_{\mathbb{C}A}(V^j, V^j) = \text{Hom}_{\mathbb{C}A}(V_1^j \oplus \cdots \oplus V_{g(j)}^j, V_1^j \oplus \cdots \oplus V_{g(j)}^j).$$

According to our basis  $\mathcal{B}$  for  $V^j$ , we have

$$\rho^j(\sigma) \in \begin{pmatrix} \text{Hom}_{\mathbb{C}A}(V_1^j, V_1^j) & \text{Hom}_{\mathbb{C}A}(V_2^j, V_1^j) & \cdots & \text{Hom}_{\mathbb{C}A}(V_{g(j)}^j, V_1^j) \\ \text{Hom}_{\mathbb{C}A}(V_1^j, V_2^j) & \text{Hom}_{\mathbb{C}A}(V_2^j, V_2^j) & \cdots & \text{Hom}_{\mathbb{C}A}(V_{g(j)}^j, V_2^j) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Hom}_{\mathbb{C}A}(V_1^j, V_{g(j)}^j) & \text{Hom}_{\mathbb{C}A}(V_2^j, V_{g(j)}^j) & \cdots & \text{Hom}_{\mathbb{C}A}(V_{g(j)}^j, V_{g(j)}^j) \end{pmatrix}.$$

Let  $X \in \text{Hom}_{\mathbb{C}A}(V_a^j, V_b^j)$  be given in matrix form with respect to the bases  $\mathcal{B}_a$ ,  $\mathcal{B}_b$ . By Lemma 2.10,  $X$  is either 0 or an isomorphism (i.e.,  $X$  is either 0 or  $\rho_a^j$  and  $\rho_b^j$  are equivalent representations of  $A$ ). Suppose then that  $X$  is an isomorphism. The goal, then, is to show that  $X$  is a diagonal matrix. Since  $X$  is  $\mathbb{C}A$ -linear, for every  $x \in \mathbb{C}A$ ,  $v \in V_a^j$  we have

$$Xx \cdot v = x \cdot Xv.$$

With respect to  $\mathcal{B}_a$ ,  $\mathcal{B}_b$  this is

$$X\rho_a^j(x)v = \rho_b^j(x)Xv,$$

and hence for every  $x \in \mathbb{C}A$ ,

$$X\rho_a^j(x) = \rho_b^j(x)X.$$

Since  $\rho_a^j$  and  $\rho_b^j$  are equivalent, and are either null or part of an adapted set of matrix representations, we have  $\rho_a^j = \rho_b^j$ , and thus

$$(5) \quad X\rho_a^j(x) = \rho_a^j(x)X$$

for all  $x \in \mathbb{C}A$ .

Now, either  $\rho_a^j$  is null of dimension 1 (in which case so is  $\rho_b^j$ ), which means that  $X$  is 1-dimensional and we're done, or  $\rho_a^j$  is an irreducible representation of  $A$ . So, suppose  $\rho_a^j$  is irreducible. Then by Burnside's theorem (Theorem 1.14 of [28]), we have

$$\rho_a^j(\mathbb{C}A) = M_{|\mathcal{B}_a|}(\mathbb{C}),$$

and therefore (5) says that  $X$  is in the center of  $M_{|\mathcal{B}_a|}(\mathbb{C})$ , i.e.  $X$  is diagonal.  $\square$

*Remark/Notation.* Schur's Lemma says that adapted representations cause the matrix  $\rho(\sigma)$  to be sparse and structured. Under the same hypotheses as above, let  $\mathcal{M}(B, A)$  be the maximum multiplicity of an irreducible or dimension-1 null representation of  $A$  occurring in the restriction, from  $B$  to  $A$ , of an irreducible representation of  $B$ . Since  $\rho(\sigma)$  is a block matrix of the form

$$\rho(\sigma) = \begin{pmatrix} \rho^1(\sigma) & 0 & 0 & \cdots & 0 \\ 0 & \rho^2(\sigma) & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & \rho^k(\sigma) \end{pmatrix},$$

and the block  $\rho^j(\sigma)$  is of the form

$$\rho^j(\sigma) = \begin{pmatrix} \rho_1^j & \rho_2^j & \cdots & \rho_{g(j)}^j \\ \rho_1^j & \lambda_{1,1}^j I & \lambda_{1,2}^j I & \cdots & \lambda_{1,g(j)}^j I \\ \rho_2^j & \lambda_{2,1}^j I & \lambda_{2,2}^j I & \cdots & \lambda_{2,g(j)}^j I \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \rho_{g(j)}^j & \lambda_{g(j),1}^j I & \lambda_{g(j),2}^j I & \cdots & \lambda_{g(j),g(j)}^j I \end{pmatrix},$$

where  $\lambda_{a,b}^j \neq 0$  implies that  $\rho_a^j$  and  $\rho_b^j$  are equivalent representations of  $A$ , we see that the matrix  $\rho(\sigma)$  contains at most  $\mathcal{M}(B, A)$  nonzero entries per row and column. The computational implication of Schur's Lemma, then, is that for an arbitrary  $d_\rho \times d_\rho$  matrix  $H$ , it requires no more than  $\mathcal{M}(B, A)d_\rho^2$  complex multiplications and additions to perform each of the matrix multiplications  $\rho(\sigma)H$  and  $H\rho(\sigma)$ , as opposed to the upper bound of  $d_\rho^3$  multiplications and additions that would be necessary if  $\rho(\sigma)$  were arbitrary.

### 3. BASIS CONSIDERATIONS FOR $\mathbb{C}S$

#### 3.1. The poset structure of an inverse semigroup.

**Definition** (poset structure of  $S$ ). Let  $S$  be a finite inverse semigroup. For  $s, t \in S$ , define

$$\begin{aligned} s \leq t &\iff s = et \text{ for some idempotent } e \in S \\ &\iff s = tf \text{ for some idempotent } f \in S. \end{aligned}$$

For  $R_n$ , the idempotents are the restrictions of the identity map. If  $S$  is a group, then its poset structure is trivial.

If  $P$  is a finite poset, then the *zeta function*  $\zeta$  of  $P$  is given by

$$\begin{aligned} \zeta : P \times P &\rightarrow \{0, 1\}, \\ \zeta(x, y) &= \begin{cases} 1 & \text{if } x \leq y, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Given a poset  $P$ , one may define an *incidence algebra* for  $P$  over any ring with identity. The element  $\zeta$  is invertible in the incidence algebra, and its inverse is called the *Möbius function*  $\mu$ . There is a general theory of Möbius inversion for incidence algebras. We will not go into the details here. Rather, we will record only the results that we need. Details may be found in [34].

The Möbius function for  $R_n$  (over  $\mathbb{C}$ ) is well known ([32], [34]). It is, for  $x \leq y$ ,

$$\mu(x, y) = (-1)^{\text{rk}(y) - \text{rk}(x)}.$$

**3.2. Natural bases for  $\mathbb{C}S$ .** Let  $S$  be an inverse semigroup. There are two natural bases for  $\mathbb{C}S$  (if  $S$  is not a group). The first basis is of course  $\{s\}_{s \in S}$ , and multiplication in  $\mathbb{C}S$  with respect to this basis is just the linear extension of the multiplication in  $S$ . To motivate the second basis, recall that every (finite) inverse

semigroup is isomorphic to a subsemigroup of a rook monoid and can therefore be viewed as a collection of partial functions. There is another model for composing partial functions: only allow the composition if the range of the first function “lines up” with the domain of the second. For example, if

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & - & 1 & - \end{pmatrix}, \quad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & - & - \end{pmatrix},$$

then the idea is that the composition  $\pi \circ \sigma$  is

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & - & 4 & - \end{pmatrix},$$

and the composition  $\sigma \circ \pi$  is disallowed. The *groupoid basis* for  $\mathbb{C}S$  encodes this.

**Definition** (groupoid basis). Let  $S$  be an inverse semigroup. Define, for each  $s \in S$ , the element  $[s] \in \mathbb{C}S$  by

$$[s] = \sum_{t \in S: t \leq s} \mu(t, s)t.$$

**Theorem 3.1.** *The collection  $\{[s]\}_{s \in S}$  is a basis for  $\mathbb{C}S$ . Multiplication in  $\mathbb{C}S$  relative to this basis is given by the linear extension of*

$$(6) \quad [s][t] = \begin{cases} [st] & \text{if } \text{dom}(s) = \text{ran}(t), \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, the change of basis to the  $\{s\}_{s \in S}$  basis of  $\mathbb{C}S$  is given by Möbius inversion:

$$(7) \quad s = \sum_{t \in S: t \leq s} [t].$$

*Proof.* This is [34], Lemma 4.1 and Theorem 4.2, using our convention that maps act on the left of sets.  $\square$

The viewpoint then is that we have two natural bases for  $\mathbb{C}S$ , the basis  $\{s\}_{s \in S}$ , and the basis  $\{[s]\}_{s \in S}$ . Note that, if  $S$  is a group, then  $s = [s] \in \mathbb{C}S$  for all  $s \in S$ .

**3.3. Fourier bases for  $\mathbb{C}S$ .** Let  $S$  be a semigroup such that  $\mathbb{C}S$  is semisimple. This means that  $\mathbb{C}S$  decomposes into a direct sum of simple submodules (i.e., left ideals):

$$\mathbb{C}S = \bigoplus L_i.$$

Let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations of  $\mathbb{C}S$ . Then, according to Theorem 2.6,

$$(8) \quad \bigoplus_{\rho \in \mathcal{Y}} \rho : \mathbb{C}S \rightarrow \bigoplus_{\rho \in \mathcal{Y}} M_{d_\rho}(\mathbb{C})$$

is an isomorphism of algebras.

There is a natural basis for the algebra on the right: the set of matrices in the algebra with the property that exactly one entry is 1 (the rest being 0). The inverse image of this set is a basis for  $\mathbb{C}S$  called the *dual matrix coefficient basis* for  $\mathcal{Y}$ , or the *Fourier basis for  $\mathbb{C}S$  according to  $\mathcal{Y}$* . When we refer to a Fourier basis

for  $\mathbb{C}S$ , we mean any basis of  $\mathbb{C}S$  that can arise in this manner by choosing an appropriate  $\mathcal{Y}$ . Note that there is a unique Fourier basis for  $\mathbb{C}S$  (up to ordering) if and only if every irreducible representation of  $S$  has dimension 1 (as is the case for  $S = \mathbb{Z}/n\mathbb{Z}$ , for which the isomorphism (8) is the usual discrete Fourier transform and the associated Fourier basis is the usual basis of exponential functions).

Consider the natural basis for the algebra on the right. The preimage of a single column of these elements from the  $\rho^{th}$  block is a basis  $B$  for a submodule of  $\mathbb{C}S$ , and each element of  $\mathbb{C}S$  acts on  $B$  exactly as described by  $\rho$ . We therefore have that  $B$  is a basis for an irreducible submodule of  $\mathbb{C}S$  (isomorphic to the representation module for  $\rho$ ). Since the map above was an isomorphism, the preimages of distinct columns have intersection  $\{0\}$ , and we therefore have the well-known fact:

**Theorem 3.2.** *Each irreducible representation of  $\mathbb{C}S$  occurs in the decomposition of  $\mathbb{C}S$  into irreducibles exactly as many times as its dimension.*

#### 4. THE FOURIER TRANSFORM ON $\mathbb{C}S$

Let  $S$  be an inverse semigroup, and let  $\mathcal{Y}$  be any complete set of inequivalent, irreducible matrix representations of  $\mathbb{C}S$ .

**Definition.** The isomorphism (8) is called a *Fourier transform* on  $\mathbb{C}S$ .

**Definition.** Let  $f \in \mathbb{C}S$ . The *Fourier transform* of  $f$  is the image of  $f$  in the matrix algebra

$$\bigoplus_{\rho \in \mathcal{Y}} M_{d_\rho}(\mathbb{C})$$

via the isomorphism (8). Equivalently, the Fourier transform of  $f$  is the re-expression of  $f$  in  $\mathbb{C}S$  in terms of a Fourier basis for  $\mathbb{C}S$ .

Let  $f \in \mathbb{C}S$  be given with respect to one of the natural bases, i.e., either  $f = \sum_{s \in S} f(s)s$  or  $f = \sum_{s \in S} f(s) \lfloor s \rfloor$ . We shall sometimes say “calculating the Fourier transform on  $\mathbb{C}S$ ” to mean calculating the Fourier transform of an arbitrary element  $f \in \mathbb{C}S$  given with respect to one of the natural bases, where the choice of  $\mathcal{Y}$  is understood.

**Definition.** Let  $\rho$  be a representation of  $\mathbb{C}S$ . Define

$$\hat{f}(\rho) = \begin{cases} \sum_{s \in S} f(s)\rho(s) & \text{if } f = \sum_{s \in S} f(s)s, \\ \sum_{s \in S} f(s)\rho(\lfloor s \rfloor) & \text{if } f = \sum_{s \in S} f(s) \lfloor s \rfloor. \end{cases}$$

For  $\rho \in \mathcal{Y}$ ,  $\hat{f}(\rho)$  is therefore just the  $\rho^{th}$  block in the image of  $f$  in the isomorphism (8).

*Remark.* Since the map in (8) is an isomorphism, it respects multiplication, and hence the Fourier transform turns the convolution of elements of  $\mathbb{C}S$  (1) into multiplication of block-diagonal matrices. It turns convolution into pointwise multiplication if and only if all irreducible representations of  $S$  have degree one, which, for example, is the case for  $S = \mathbb{Z}/n\mathbb{Z}$ .

5. DECOMPOSITION OF  $\mathbb{C}R_n$  INTO A MATRIX ALGEBRA  
OVER GROUP ALGEBRAS

Let  $S$  be an inverse semigroup. The theorem in this section is a special case of Theorem 4.6 in Steinberg [34], which provides an explicit isomorphism between  $\mathbb{C}S$  and a direct sum of matrix algebras over group algebras. The groups appearing in the group algebras are the maximal subgroups of  $S$ . The purpose of this section is to explain this isomorphism in the case when  $S = R_n$ .

This turns out to be a very important isomorphism for the FFT theory for  $R_n$ . It allows us to easily describe a complete set of inequivalent, irreducible representations for  $R_n$  (Section 6.1), it allows us to describe explicit Fourier bases for  $\mathbb{C}R_n$  (Section 6.2), it allows us to easily state the Fourier inversion theorem for  $\mathbb{C}R_n$  (Section 6.3), and it forms the basis for one of our FFT algorithms (Section 9).

Let  $D_k \subseteq \mathbb{C}R_n$  be the  $\mathbb{C}$ -span of  $\{|s\rangle : s \in R_n, \text{rk}(s) = k\}$ . By (6), we have that  $\mathbb{C}R_n = \bigoplus_{i=0}^n D_k$ , so that the product of two elements in  $D_k$  is an element of  $D_k$ , and the product of an element in  $D_i$  with an element in  $D_j$  is 0 if  $i \neq j$ .

For  $k \in \{0, \dots, n\}$ , we identify  $S_k \subseteq R_n$  with the subgroup of elements of rank  $k$  with domain and range equal to  $\{1, \dots, k\}$ . We therefore take  $S_0$  to be the set consisting of the zero map, and  $S_0 \cong S_1$ . The following decomposition theorem was implicit in the work of Munn and made explicit in [34], Theorem 4.6.

**Theorem 5.1.**  $D_k \cong M_{\binom{n}{k}}(\mathbb{C}S_k)$ , and thus  $\mathbb{C}R_n \cong \bigoplus_{k=0}^n M_{\binom{n}{k}}(\mathbb{C}S_k)$ .

*Proof.* Use the  $k$ -subsets of  $\{1, \dots, n\}$  to index the rows and columns of  $M_{\binom{n}{k}}(\mathbb{C}S_k)$  in such a way that  $\{1, \dots, k\}$  is the first  $k$ -set. If  $A$  and  $B$  are two  $k$ -subsets of  $\{1, \dots, n\}$ , let  $p_{(A \rightarrow B)}$  denote the unique order-preserving bijection from  $A$  to  $B$ . Keeping in mind that our maps act on the left of sets, define a map

$$\phi : D_k \rightarrow M_{\binom{n}{k}}(\mathbb{C}S_k)$$

by defining it on a basis element  $|s\rangle$ :

$$\phi(|s\rangle) = p_{(\text{ran}(s) \rightarrow \{1, \dots, k\})} sp_{(\{1, \dots, k\} \rightarrow \text{dom}(s))} E_{\text{ran}(s), \text{dom}(s)},$$

where  $E_{\text{ran}(s), \text{dom}(s)}$  is the  $\binom{n}{k} \times \binom{n}{k}$  matrix with a 1 in the  $\text{ran}(s), \text{dom}(s)$  position and 0 elsewhere. Observe that  $p_{(\text{ran}(s) \rightarrow \{1, \dots, k\})} sp_{(\{1, \dots, k\} \rightarrow \text{dom}(s))} \in S_k$  by construction.

It is easy to show that  $\phi$  is an isomorphism and that  $\phi^{-1}$  is induced by

$$gE_{A,B} \mapsto \left| p_{(\{1, \dots, k\} \rightarrow A)} gp_{(B \rightarrow \{1, \dots, k\})} \right|.$$

Note that if  $g \in S_k \subseteq R_n$ , then

$$\phi(|g\rangle) = gE_{1,1}.$$

□

*Notational Remark.* For the rest of the paper, if  $A$  and  $B$  are  $k$ -subsets of  $\{1, \dots, n\}$ , then we will denote the unique order-preserving bijection from  $A$  to  $B$  by  $p_{(A \rightarrow B)}$ .

6. CONSEQUENCES OF THEOREM 5.1

**6.1. Explicit matrix representations of  $\mathbb{C}R_n$ .** Let  $G$  be a finite group. The representations of the matrix algebra  $M_n(\mathbb{C}G)$  were studied as early as 1942 by

A.H. Clifford in the context of Brandt groupoids [4]. In the notation of Section 5, we have

$$\mathbb{C}R_n \cong \bigoplus_{k=0}^n M_{\binom{n}{k}}(\mathbb{C}S_k).$$

Given an irreducible matrix representation  $\rho$  of  $S_k$  (or of  $\mathbb{C}S_k$ ), we can “tensor up” to an irreducible matrix representation  $\bar{\rho}$  of  $M_{\binom{n}{k}}(\mathbb{C}S_k)$  and then extend  $\bar{\rho}$  to an irreducible matrix representation of  $\mathbb{C}R_n$  by declaring it to be 0 on the other summands. Specifically, for  $g \in S_k$ ,

$$(9) \quad \bar{\rho}(gE_{A,B}) = E_{A,B} \otimes \rho(g).$$

Let  $\text{IRR}(S_k)$  be any complete set of inequivalent, irreducible matrix representations of  $S_k$ . For  $\rho_1, \rho_2 \in \text{IRR}(S_k)$ , [4] shows that  $\bar{\rho}_1$  and  $\bar{\rho}_2$  are equivalent if and only if  $\rho_1$  and  $\rho_2$  are equivalent, and that all irreducible matrix representations (up to equivalence) of  $M_{\binom{n}{k}}(\mathbb{C}S_k)$  are obtained in this manner.

Therefore, the distinct irreducible representations of  $\mathbb{C}R_n$  are in one-to-one correspondence with the elements of  $\bigcup_{k=0}^n \text{IRR}(S_k)$ . Many explicit descriptions of  $\text{IRR}(S_k)$  are known. Two well-known computationally advantageous ones are Young’s seminormal and Young’s orthogonal forms. A description of the former may be found in [3], and a description of the latter in [10].

To be completely explicit, suppose  $f \in \mathbb{C}R_n$ , with  $f = \sum_{s \in R_n} f(s) \lfloor s \rfloor$ , and let  $\rho \in \text{IRR}(S_k)$ . Then  $\bar{\rho}$  is an irreducible matrix representation of  $\mathbb{C}R_n$ , and

$$\begin{aligned} \bar{\rho}(f) &= \sum_{s \in R_n} f(s) \bar{\rho}(\lfloor s \rfloor) \\ &= \sum_{\substack{s \in R_n : \\ \text{rk}(s)=k}} f(s) \bar{\rho}(\lfloor s \rfloor) \\ &= \sum_{\substack{A \subseteq \{1, \dots, n\} \\ |A|=k}} \sum_{\substack{B \subseteq \{1, \dots, n\} \\ |B|=k}} \sum_{g \in S_k} f(p_{\{1, \dots, k\} \rightarrow A} g p_{(B \rightarrow \{1, \dots, k\})}) (E_{A,B} \otimes \rho(g)). \end{aligned}$$

We have thus effectively described the irreducible representations of  $\mathbb{C}R_n$  by describing their actions on the  $\{\lfloor s \rfloor\}$  basis. We remark that, if desired, one could obtain a description of the irreducible representations of  $R_n$  by looking at these representations on the  $\{s\}$  basis via (7). We also remark that there are other ways to describe a complete set of inequivalent, irreducible representations for  $R_n$  that do not involve decomposing it into a sum of matrix algebras over group algebras, or indeed referencing the  $\{\lfloor s \rfloor\}$  basis at all. For example, see Grood’s description in [13], Halverson’s description in [14], or Section 10.2.

**6.2. Explicit Fourier bases for  $\mathbb{C}R_n$ .** Let  $\text{IRR}(S_k)$  be a complete set of inequivalent, irreducible matrix representations for  $S_k$ , for  $k \in \{0, \dots, n\}$ . For each  $\rho \in \text{IRR}(S_k)$ , let  $\bar{\rho}$  denote its extension (via the method discussed in Section 6.1) to  $\mathbb{C}R_n$ . We take  $\mathcal{Y} = \bigcup_{k=0}^n \{\bar{\rho} : \rho \in \text{IRR}(S_k)\}$ .

It is now easy to explicitly describe the Fourier basis for  $\mathbb{C}R_n$  according to  $\mathcal{Y}$  in terms of the natural  $\{\lfloor s \rfloor\}$  basis. That is, if  $B \subseteq \mathbb{C}R_n$  is the set of inverse images

of the natural basis of  $\bigoplus_{\bar{\rho} \in \mathcal{Y}} M_{d_{\bar{\rho}}}(\mathbb{C})$  in the isomorphism

$$(10) \quad \bigoplus_{\bar{\rho} \in \mathcal{Y}} \bar{\rho} : \mathbb{C}R_n \rightarrow \bigoplus_{\bar{\rho} \in \mathcal{Y}} M_{d_{\bar{\rho}}}(\mathbb{C}),$$

then for each  $b \in B$ ,

$$b = \sum_{s \in R_n} b(s) \lfloor s \rfloor.$$

We will now describe the coefficients  $b(s)$ .

We begin by assuming we have an explicit description of a Fourier basis for  $\mathbb{C}S_k$  for each  $k \in \{0, \dots, n\}$ . That is, if  $C$  is the set of inverse images of the natural basis of the algebra on the right in the isomorphism

$$(11) \quad \bigoplus_{\rho \in \text{IRR}(S_k)} \rho : \mathbb{C}S_k \rightarrow \bigoplus_{\rho \in \text{IRR}(S_k)} M_{d_{\rho}}(\mathbb{C}),$$

then, for each  $c \in C$ ,

$$c = \sum_{x \in S_k} c(x)x,$$

and we assume that we know the coefficients  $c(x)$ . They may be found, for example, by using the standard Fourier inversion theorem for groups (Theorem 6.2).

Now, fix  $\rho \in \text{IRR}(S_k)$ . Fix  $c_{i,j} \in \mathbb{C}S_k$ ,

$$c_{i,j} = \sum_{x \in S_k} c_{i,j}(x)x,$$

to be the inverse image in the isomorphism (11) of the element of

$$\bigoplus_{\rho \in \text{IRR}(S_k)} M_{d_{\rho}}(\mathbb{C})$$

that is 1 in the  $i, j$  position in the  $\rho$  block and 0 elsewhere.  $\bar{\rho}$  is a block matrix whose rows and columns are indexed by the  $k$ -subsets of  $\{1, \dots, n\}$ , and whose entries are themselves  $d_{\rho} \times d_{\rho}$  matrices. Call the  $m^{\text{th}}$   $k$ -set  $M$  and the  $n^{\text{th}}$   $k$ -set  $N$ .

**Theorem 6.1.** *Let  $X$  be a  $d_{\rho} \times d_{\rho}$  matrix with a 1 in the  $i, j$  position and 0 elsewhere. The inverse image in the isomorphism (10) of the element of  $\bigoplus_{\bar{\rho} \in \mathcal{Y}} M_{d_{\bar{\rho}}}(\mathbb{C})$  that is  $E_{m,n} \otimes X$  in the  $\bar{\rho}$  block and 0 elsewhere is*

$$\lfloor p_{(\{1, \dots, k\} \rightarrow M)} \rfloor \left( \sum_{x \in S_k} c_{i,j}(x) \lfloor x \rfloor \right) \lfloor p_{(N \rightarrow \{1, \dots, k\})} \rfloor.$$

*Proof.* If  $\bar{\gamma} \in \mathcal{Y}$ ,  $\bar{\gamma} \neq \bar{\rho}$ , then

$$\bar{\gamma} \left( \lfloor p_{(\{1, \dots, k\} \rightarrow M)} \rfloor \left( \sum_{x \in S_k} c_{i,j}(x) \lfloor x \rfloor \right) \lfloor p_{(N \rightarrow \{1, \dots, k\})} \rfloor \right) = 0$$

because

$$\bar{\gamma} \left( \sum_{x \in S_k} c_{i,j}(x) \lfloor x \rfloor \right) = 0.$$

On the other hand,

$$\begin{aligned} \bar{\rho} & \left( \lfloor p_{\{\{1, \dots, k\} \rightarrow M\}} \rfloor \left( \sum_{x \in S_k} c_{i,j}(x) \lfloor x \rfloor \right) \lfloor p_{(N \rightarrow \{1, \dots, k\})} \rfloor \right) \\ & = (E_{m,1} \otimes I_{d_\rho}) (E_{1,1} \otimes X) (E_{1,n} \otimes I_{d_\rho}) = E_{m,n} \otimes X. \end{aligned}$$

□

**6.3. The Fourier inversion formula for  $\mathbb{C}R_n$ .** We begin by recalling the Fourier inversion theorem for groups.

**Theorem 6.2.** *Let  $G$  be a finite group, and let  $f = \sum_{s \in G} f(s)s \in \mathbb{C}G$ . Let  $\text{IRR}(G)$  be a complete set of inequivalent, irreducible matrix representations for  $G$ . Then*

$$f(s) = \frac{1}{|G|} \sum_{\rho \in \text{IRR}(G)} d_\rho \text{trace}(\hat{f}(\rho)\rho(s^{-1})).$$

*Proof.* See [30], Section 6.2. □

We now state a preliminary lemma, which is a direct consequence of Theorem 6.2 and Section 6.1.

**Lemma 6.3.** *Let  $f = \sum_{x \in R_n} f(x) \lfloor x \rfloor \in \mathbb{C}R_n$ , and let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations for  $R_n$ , induced by*

$$\bigoplus_{k \in \{0, \dots, n\}} \text{IRR}(S_k)$$

*in the manner described in Section 6.1. Let  $\text{rk}(x) = k$ . Write*

$$x = p_{\{\{1, \dots, k\} \rightarrow \text{ran}(x)\}} y p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}$$

*for a unique  $y \in S_k$ .*

*The  $\text{ran}(x), \text{dom}(x)$  entry of  $\hat{f}(\bar{\rho})$  is a  $d_\rho \times d_\rho$  matrix. If we denote it by  $\hat{f}(\bar{\rho})_{\text{ran}(x), \text{dom}(x)}$ , then we have*

$$f(x) = \frac{1}{|S_k|} \sum_{\rho \in \text{IRR}(S_k)} d_\rho \text{trace}(\hat{f}(\bar{\rho})_{\text{ran}(x), \text{dom}(x)} \rho(y^{-1})).$$

*Proof.* For  $\rho \in \text{IRR}(S_k)$  we have

$$\hat{f}(\bar{\rho}) = \sum_{s \in R_n} f(s) \bar{\rho}(\lfloor s \rfloor),$$

with  $\bar{\rho}(\lfloor s \rfloor) = 0$  if  $\text{rk}(s) \neq k$ . By definition of  $\bar{\rho}$ , the Fourier transform  $\hat{f}(\bar{\rho})$  may be computed block by block (and thus may be inverted block by block). The  $\text{ran}(x), \text{dom}(x)$  entry of  $\hat{f}(\bar{\rho})$  is determined by the values  $f(s)$  for which  $\text{ran}(s) = \text{ran}(x)$  and  $\text{dom}(s) = \text{dom}(x)$ , and these values do not affect any other entries of  $\hat{f}(\bar{\rho})$ . Explicitly, the  $\text{ran}(x), \text{dom}(x)$  entry of  $\hat{f}(\bar{\rho})$  is given by

$$\sum_{s \in S_k} f(p_{\{\{1, \dots, k\} \rightarrow \text{ran}(x)\}} s p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}) \rho(s).$$

Let us define a function  $f_{\text{ran}(x), \text{dom}(x)}$  on  $S_k$  by

$$f_{\text{ran}(x), \text{dom}(x)}(s) = f(p_{(\{1, \dots, k\} \rightarrow \text{ran}(x))} s p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}).$$

Then

$$\begin{aligned} \sum_{s \in S_k} f(p_{(\{1, \dots, k\} \rightarrow \text{ran}(x))} s p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}) \rho(s) &= \sum_{s \in S_k} f_{\text{ran}(x), \text{dom}(x)}(s) \rho(s) \\ &= \hat{f}_{\text{ran}(x), \text{dom}(x)}(\rho). \end{aligned}$$

The Fourier inversion theorem for groups then applies and yields:

$$\begin{aligned} f(x) &= f(p_{(\{1, \dots, k\} \rightarrow \text{ran}(x))} y p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}) \\ &= \frac{1}{|S_k|} \sum_{\rho \in \text{IRR}(S_k)} d_\rho \text{trace} \left( \hat{f}_{\text{ran}(x), \text{dom}(x)}(\rho) \rho(y^{-1}) \right), \end{aligned}$$

and since

$$\hat{f}_{\text{ran}(x), \text{dom}(x)}(\rho) = \hat{f}(\bar{\rho})_{\text{ran}(x), \text{dom}(x)},$$

we are done.  $\square$

Now, let  $\mathcal{S}$  be *any* set of inequivalent, irreducible matrix representations for  $R_n$ . We define some notation before stating the Fourier inversion theorem for  $\mathbb{C}R_n$ .

Let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations for  $R_n$  induced by  $\bigcup_{k \in \{0, \dots, n\}} \text{IRR}(S_k)$  in the manner described in Section 6.1. If  $\rho \in \text{IRR}(S_k)$ , we have the corresponding  $\bar{\rho} \in \mathcal{Y}$ , which is equivalent to some representation in  $\mathcal{S}$ , which we denote by  $\bar{\rho}$ .

**Theorem 6.4** (Fourier inversion theorem for  $\mathbb{C}R_n$ ). *Let*

$$f = \sum_{x \in R_n} f(x) \lfloor x \rfloor \in \mathbb{C}R_n.$$

*Let  $\text{rk}(x) = k$ , and let us denote the semigroup inverse of  $x$  by  $x^{-1}$ . Then*

$$f(x) = \frac{1}{|S_k|} \sum_{\rho \in \text{IRR}(S_k)} d_\rho \text{trace} \left( \hat{f}(\bar{\rho}) \bar{\rho}(\lfloor x^{-1} \rfloor) \right).$$

*Proof.* Since  $\bar{\rho}$  is equivalent to  $\rho$ , write

$$\bar{\rho} = A^{-1} \bar{\rho} A$$

for some invertible matrix  $A$ . We therefore have

$$\hat{f}(\bar{\rho}) = A^{-1} \hat{f}(\bar{\rho}) A.$$

As in Lemma 6.3, let  $y$  be the unique element of  $S_k$  such that

$$x = p_{(\{1, \dots, k\} \rightarrow \text{ran}(x))} y p_{(\text{dom}(x) \rightarrow \{1, \dots, k\})}.$$

Now, we have

$$\begin{aligned}
\text{trace} \left( \hat{f}(\bar{\rho})_{\text{ran}(x), \text{dom}(x)} \rho(y^{-1}) \right) &= \text{trace} \left( \left[ \hat{f}(\bar{\rho}) \right] [E_{\text{dom}(x), \text{ran}(x)} \otimes \rho(y^{-1})] \right) \\
&= \text{trace} \left( \hat{f}(\bar{\rho}) \bar{\rho}([x^{-1}]) \right) \\
&= \text{trace} \left( \left[ A^{-1} \hat{f}(\bar{\rho}) A \right] [A^{-1} \bar{\rho}([x^{-1}]) A] \right) \\
&= \text{trace} \left( A^{-1} \hat{f}(\bar{\rho}) \bar{\rho}([x^{-1}]) A \right) \\
&= \text{trace} \left( \hat{f}(\bar{\rho}) \bar{\rho}([x^{-1}]) \right),
\end{aligned}$$

the last equality arising from the similarity-invariance of the trace. The theorem now follows from Lemma 6.3.  $\square$

## 7. ASSOCIATING FUNCTIONS ON $S$ TO ELEMENTS OF $\mathbb{C}S$

We are now ready to address the issues that arise in choosing how to associate functions on  $S$  to elements of the semigroup algebra  $\mathbb{C}S$ . We also define the Fourier transform and the convolution of functions on  $S$ .

Let  $S$  be an inverse semigroup. Let  $f : S \rightarrow \mathbb{C}$ . Having defined two “natural” bases for  $\mathbb{C}S$ , we have two natural choices for how to associate  $f$  to an element of  $\mathbb{C}S$ , either

$$f \leftrightarrow \sum_{s \in S} f(s)s \quad \text{or} \quad f \leftrightarrow \sum_{s \in S} f(s)[s].$$

In the first case, which we shall call the *semigroup association model*, the elements  $s$  in  $\mathbb{C}S$  are associated to the characteristic functions of the elements  $s \in S$ . In the second case, which we shall call the *groupoid association model*, the elements  $[s]$  in  $\mathbb{C}S$  are associated to the characteristic functions of the elements  $s \in S$ .

**Definition** (Fourier transform of a function on  $S$ ). Let  $f : S \rightarrow \mathbb{C}$ . Given an association model, the Fourier transform of  $f$  is defined to be the Fourier transform of the associated element of  $\mathbb{C}S$ .

Thus, if the groupoid association model is used, then the Fourier transform of  $f$  is

$$\bigoplus_{\rho \in \mathcal{Y}} \sum_{s \in S} f(s)\rho([s]),$$

and if the semigroup association model is used, then the Fourier transform of  $f$  is

$$\bigoplus_{\rho \in \mathcal{Y}} \sum_{s \in S} f(s)\rho(s),$$

where  $\mathcal{Y}$  is a complete set of inequivalent, irreducible matrix representations of  $\mathbb{C}S$ . The convolution of functions on  $S$  is also defined by the association model.

**Definition** (convolution of functions on  $S$ ). Let  $f, g : S \rightarrow \mathbb{C}$ . Choosing an association model defines how the images of  $f$  and  $g$  in  $\mathbb{C}S$  multiply. Denote the images of  $f, g$  in  $\mathbb{C}S$  by  $\bar{f}, \bar{g}$  respectively. Then we define, for  $s \in S$ :

Under the semigroup association model,  $f * g(s) =$  the  $s^{th}$  coefficient of  $\bar{f} * \bar{g}$  expressed with respect to the  $\{s\}$  basis. Under the groupoid association model,  $f * g(s) =$  the  $[s]^{th}$  coefficient of  $\bar{f} * \bar{g}$  expressed with respect to the  $\{[s]\}$  basis.

For the case  $S = R_n$ , what follows is an overview of the considerations one should take into account when choosing which function association model to use.

**Consideration 1** (convolution). Convolution of functions on  $R_n$  is defined by the association model used. If the semigroup association model is used, then convolution of  $\mathbb{C}$ -valued functions  $f, g$  on  $R_n$  is defined by (1). Specifically,

$$(f * g)(s) = \sum_{r, t \in R_n : rt=s} f(r)g(t).$$

If the groupoid association model is used, then convolution of  $\mathbb{C}$ -valued functions  $f, g$  on  $R_n$  is defined by their multiplication in  $\mathbb{C}R_n$  with respect to the  $\{\lfloor s \rfloor\}$  basis. Specifically,

$$(f * g)(s) = \sum_{\substack{r \in R_n : \\ \text{ran}(s) = \text{ran}(r)}} f(r)g(r^{-1}s).$$

**Consideration 2** (inner products). There is a natural inner product for  $\mathbb{C}$ -valued functions  $f, g$  on  $R_n$ :

$$\langle f, g \rangle = \sum_{s \in R_n} f(s)\overline{g(s)}.$$

It would be nice to use this inner product. Choosing an inner product on functions and an association model induces an inner product on  $\mathbb{C}R_n$  (or equivalently, choosing an inner product on  $\mathbb{C}R_n$  and an association model induces an inner product on functions on  $R_n$ ). Specifically, if we choose the above inner product, then the semigroup association model induces the inner product  $\langle \cdot, \cdot \rangle_1$  on  $\mathbb{C}R_n$  defined by

$$\langle s, t \rangle_1 = \begin{cases} 1 & \text{if } s = t, \\ 0 & \text{otherwise,} \end{cases}$$

and the groupoid association model induces the inner product  $\langle \cdot, \cdot \rangle_2$  on  $\mathbb{C}R_n$  defined by

$$\langle \lfloor s \rfloor, \lfloor t \rfloor \rangle_2 = \begin{cases} 1 & \text{if } \lfloor s \rfloor = \lfloor t \rfloor, \\ 0 & \text{otherwise.} \end{cases}$$

However, choosing the inner product  $\langle \cdot, \cdot \rangle_1$  leads to undesirable consequences with regards to the Fourier basis for  $\mathbb{C}R_n$ , as described in Consideration 3. For this reason, if the semigroup association model is used, then it is recommended to take the inner product  $\langle \cdot, \cdot \rangle_2$  on  $\mathbb{C}R_n$  and use that to induce an inner product on  $\mathbb{C}$ -valued functions on  $R_n$ .

**Consideration 3** (orthogonality of isotypic subspaces of  $\mathbb{C}R_n$ ). Since  $\mathbb{C}R_n$  is semisimple, we have

$$\mathbb{C}R_n = \bigoplus L_i,$$

where each  $L_i$  is simple. Let us group them according to their isomorphism classes:

$$\mathbb{C}R_n = \bigoplus_{\bar{\rho} \in \mathcal{Y}} V_{\bar{\rho}},$$

where  $\mathcal{Y}$  is a complete set of inequivalent, irreducible matrix representations for  $R_n$ , and  $V_{\bar{\rho}}$  is the sum of all simple submodules of  $\mathbb{C}R_n$  isomorphic to the representation module for  $\bar{\rho} \in \mathcal{Y}$ . The  $V_{\bar{\rho}}$  are called the *isotypic subspaces* or *isotypic submodules* of  $\mathbb{C}R_n$ . Note that this decomposition does not depend on the choice of  $\mathcal{Y}$ . Let

$v \in V_{\bar{\rho}}, v' \in V_{\bar{\rho}'}.$  We would like to have an inner product  $(\cdot, \cdot)$  on  $\mathbb{C}R_n$  such that, if  $V_{\bar{\rho}} \neq V_{\bar{\rho}'},$  then

$$(v, v') = 0,$$

i.e., an inner product under which the isotypic subspaces of  $\mathbb{C}R_n$  are orthogonal. The claim is that  $\langle \cdot, \cdot \rangle_2$  accomplishes this and that  $\langle \cdot, \cdot \rangle_1$  in general does not.

**Theorem 7.1.** *Let  $V_{\bar{\rho}} \neq V_{\bar{\rho}'}. Then, using the notation above,  $\langle v, v' \rangle_2 = 0.$$*

*Proof.* By linearity, it suffices to show this in the case that  $v$  and  $v'$  are Fourier basis elements of  $\mathbb{C}R_n.$  We take  $\mathcal{Y}$  to be the set induced by  $\bigcup_{k \in \{0, \dots, n\}} \text{IRR}(S_k)$  in the manner described in Section 6.1, and we assume that  $v$  and  $v'$  are part of a Fourier basis for  $\mathbb{C}R_n$  according to  $\mathcal{Y}.$

We know that

$$\mathbb{C}S_k = \bigoplus_{\rho \in \text{IRR}(S_k)} W_\rho,$$

where  $W_\rho$  is the sum of all the irreducible submodules of  $\mathbb{C}S_k$  isomorphic to the representation module for  $\rho.$  If  $w \in W_\rho, w' \in W_{\rho'}, W_\rho \neq W_{\rho'},$  then under the inner product  $[\cdot, \cdot]$  on  $\mathbb{C}S_k$  defined by

$$[\sum_{s \in S_k} a(s)s, \sum_{s \in S_k} b(s)s] = \sum_{s \in S_k} a(s)\overline{b(s)},$$

it follows from the discussion in Chapter 2 of [30] that we have  $[w, w'] = 0.$

Now, suppose that  $\bar{\rho}$  was induced by  $\rho \in \text{IRR}(S_k)$  and that  $\bar{\rho}'$  was induced by  $\rho' \in \text{IRR}(S_j).$  By Theorem 6.1, when written in terms of the natural  $\{|s|\}$  basis,  $v$  contains nonzero coefficients only for the elements  $|s|$  where  $s$  is of rank  $k,$  and  $v'$  contains nonzero coefficients only for the elements  $|s|$  where  $s$  is of rank  $j.$  Thus, if  $k \neq j,$  we have  $\langle v, v' \rangle_2 = 0.$  Suppose then that  $k = j.$  By Theorem 6.1, we have

$$\begin{aligned} v &= [p_{(\{1, \dots, k\} \rightarrow B)}] \sum_{s \in S_k} v(s) |s| [p_{(A \rightarrow \{1, \dots, k\})}], \\ v' &= [p_{(\{1, \dots, k\} \rightarrow B')}] \sum_{s \in S_k} v'(s) |s| [p_{(A' \rightarrow \{1, \dots, k\})}], \end{aligned}$$

for  $A, A', B, B'$  some  $k$ -subsets of  $\{1, \dots, n\},$  and

$$\sum_{s \in S_k} v(s)s \in W_\rho, \quad \sum_{s \in S_k} v'(s)s \in W_{\rho'}$$

some Fourier basis elements for  $\mathbb{C}S_k.$

If  $A \neq A'$  or  $B \neq B',$  it is apparent that  $\langle v, v' \rangle_2 = 0,$  so suppose further that  $A = A'$  and  $B = B'.$

Now, since  $V_{\bar{\rho}} \neq V_{\bar{\rho}'},$  we have  $\rho \neq \rho',$  and we therefore note that

$$[\sum_{s \in S_k} v(s)s, \sum_{s \in S_k} v'(s)s] = 0.$$

For convenience, we temporarily denote  $p_{(\{1, \dots, k\} \rightarrow B)}$  by  $p_B$  and  $p_{(A \rightarrow \{1, \dots, k\})}$  by  $p_A.$  We have

$$\langle v, v' \rangle_2 = \sum_{s \in S_k} \sum_{t \in S_k} v(s)\overline{v'(t)} \langle [p_B s p_A], [p_B t p_A] \rangle_2,$$

and  $\lfloor p_B s p_A \rfloor = \lfloor p_B t p_A \rfloor$  if and only if  $s = t$ , so

$$\langle v, v' \rangle_2 = \sum_{s \in S_k} v(s) \overline{v'(s)} = [\sum_{s \in S_k} v(s), \sum_{s \in S_k} v'(s)] = 0.$$

□

*Remark 7.2.* The isotypic subspaces  $V_{\bar{\rho}}$  need not be orthogonal under the inner product  $\langle \cdot, \cdot \rangle_1$ . For example, consider  $\mathbb{C}R_1$ , which has two nonisomorphic irreducible representations, each of degree 1, and hence a unique Fourier basis. It decomposes as

$$\mathbb{C}R_1 = (\mathbb{C}\text{-span}(\lfloor \text{Id} \rfloor)) \oplus (\mathbb{C}\text{-span}(\lfloor 0 \rfloor)).$$

We have

$$\langle \lfloor \text{Id} \rfloor, \lfloor 0 \rfloor \rangle_1 = \langle \text{Id} - (0), (0) \rangle_1 = -1.$$

## 8. FFT ALGORITHM CONSIDERATIONS

**8.1. Computational complexity.** If  $G$  is a finite group, then  $\{g\}_{g \in G}$  indexes the natural basis of  $\mathbb{C}G$ . If  $S$  is an inverse semigroup, then  $\mathbb{C}S$  has two natural bases, the  $\{s\}_{s \in S}$  basis and the  $\{\lfloor s \rfloor\}_{s \in S}$  basis. We therefore define the following two corresponding notions of computational complexity for the Fourier transform on  $\mathbb{C}S$ .

**Definition** (computational complexity). Let  $\mathcal{Y}$  be a complete set of inequivalent, irreducible matrix representations for  $\mathbb{C}S$ . For an arbitrary element  $f \in \mathbb{C}S$  expressed with respect to the  $\{s\}$  basis,

$$f = \sum_{s \in S} f(s)s,$$

the number of operations needed to compute the Fourier transform of  $f$ , i.e., to compute

$$(12) \quad \hat{f}(\rho) = \sum_{s \in S} f(s)\rho(s)$$

for all  $\rho \in \mathcal{Y}$ , is denoted by  $\mathcal{T}_{\mathcal{Y}}^s(S)$ .

For an arbitrary element  $f \in \mathbb{C}S$  expressed with respect to the  $\{\lfloor s \rfloor\}$  basis,

$$f = \sum_{s \in S} f(s) \lfloor s \rfloor,$$

the number of operations needed to compute the Fourier transform of  $f$ , i.e., to compute

$$(13) \quad \hat{f}(\rho) = \sum_{s \in S} f(s)\rho(\lfloor s \rfloor)$$

for all  $\rho \in \mathcal{Y}$ , is denoted by  $\mathcal{T}_{\mathcal{Y}}^{\lfloor s \rfloor}(S)$ .

Now, let  $\mathcal{Y}$  vary over all complete sets of inequivalent, irreducible representations for  $\mathbb{C}S$ . We define

$$\begin{aligned} \mathcal{C}^s(S) &= \min_{\mathcal{Y}}(\mathcal{T}_{\mathcal{Y}}^s(S)), \\ \mathcal{C}^{\lfloor s \rfloor}(S) &= \min_{\mathcal{Y}}(\mathcal{T}_{\mathcal{Y}}^{\lfloor s \rfloor}(S)), \text{ and} \\ \mathcal{C}(S) &= \max(\mathcal{C}^s(S), \mathcal{C}^{\lfloor s \rfloor}(S)). \end{aligned}$$

An *operation* is defined to be a single complex multiplication together with a complex addition. For the purposes of our analysis, we assume that all representations in  $\mathcal{Y}$  are precomputed (i.e., evaluated at every basis element  $s$  of  $\mathbb{C}S$  or at every basis element  $[s]$  of  $\mathbb{C}S$ ) and stored in memory.

If  $G$  is a group, the  $\{s\}$  and the  $\{[s]\}$  bases of  $\mathbb{C}G$  are identical, so we may drop the superscripts on the complexity notation. For example,

$$\mathcal{T}_{\mathcal{Y}}^s(G) = \mathcal{T}_{\mathcal{Y}}^{[s]}(G) = \mathcal{T}_{\mathcal{Y}}(G).$$

Now, let  $\mathcal{Y}$  be any complete set of inequivalent, irreducible matrix representations for  $\mathbb{C}R_n$ . A naive implementation of the Fourier transform on  $R_n$ , i.e., computing (12) and (13) directly, gives

$$\mathcal{C}(R_n) \leq \sum_{\rho \in \mathcal{Y}} |R_n| d_{\rho}^2,$$

which, by (4), gives

**Theorem.**  $\mathcal{C}(R_n) \leq |R_n|^2$ .

As  $n$  grows, this cost quickly becomes prohibitive.

For the same reason, we also have  $\mathcal{C}(G) \leq |G|^2$  for any group  $G$ , but many families of groups enjoy results along the lines of  $\mathcal{C}(G) = O(|G| \log^c |G|)$ . Indeed, such upper bounds remain the goal in group FFT theory. There are also groups  $G$  for which there currently exist greatly improved (but not  $O(|G| \log^c |G|)$ ) algorithms, such as matrix groups over finite fields or, more generally, finite groups of Lie type [21]. It is conjectured that there are universal constants  $c_1, c_2$  such that for any group  $G$ ,  $\mathcal{C}(G) \leq c_1 |G| \log^{c_2} |G|$  [24]. It is currently known that, for example,

$$\mathcal{C}(\mathbb{Z}/n\mathbb{Z}) = O(n \log n),$$

$$\mathcal{C}(G) \leq 8.5 |G| \log |G| \text{ for any supersolvable group } G, \text{ and}$$

$$\mathcal{C}(S_n) = O(|S_n| \log^2 |S_n|) \text{ (where } S_n \text{ is the symmetric group on } n \text{ letters).}$$

See [2], [1], and [20], respectively, for these results, or see Section 8.3 for a description of an  $O(|S_n| \log^3 |S_n|)$  FFT on  $S_n$ .

We now state the main results of this paper.

**Theorem 8.1.**  $\mathcal{C}^{[s]}(R_n) = O(|R_n| \log^2 |R_n|)$ .

**Theorem 8.2.** For any  $\epsilon > 0$ ,  $\mathcal{C}^s(R_n) = O(|R_n|^{1+\epsilon})$ , and hence

$$\mathcal{C}(R_n) = O(|R_n|^{1+\epsilon}).$$

We prove these results in Sections 9.1 and 9.2, respectively.

**8.2. FFTs on groups.** In this section, we describe a general method used to construct FFTs on groups. This section is basically an elaboration of the main idea in [21] and is included in the interest of keeping this document self-contained. This method is used in the FFT on  $S_n$  given in Section 8.3 (which itself is used in the FFT for  $R_n$  given in Section 9). We also will generalize this method directly to create an FFT for  $R_n$  in Section 10.

Let  $G$  be a group and let  $H$  be a subgroup of  $G$ .  $H$  partitions  $G$  into cosets  $yH$ . Let  $C \subseteq G$  be a full set of coset representatives for distinct cosets (i.e.,

$G = \bigcup_{y \in C} yH$ , and  $y_1 \neq y_2 \in C \Rightarrow y_1 H \cap y_2 H = \emptyset$ ). Let  $\rho$  be a representation of  $G$ . Then, since  $\rho$  is a homomorphism, we have the factorization

$$(14) \quad \hat{f}(\rho) = \sum_{g \in G} f(g)\rho(g) = \sum_{y \in C} \rho(y) \sum_{h \in H} f_y(h)\rho(h),$$

where  $f_y(h) = f(yh)$ .

Let  $\mathcal{Y}_G$  and  $\mathcal{Y}_H$  be complete sets of irreducible, inequivalent matrix representations for  $G$  and  $H$ , respectively, adapted to the chain  $G > H$ . We would like to compute  $\hat{f}(\rho)$  for all  $\rho \in \mathcal{Y}_G$ . The idea is that if we already knew all the  $\hat{f}_y(\gamma)$  for all  $\gamma$  in  $\mathcal{Y}_H$  and  $y \in C$ , then we could construct the inner sums in (14) based on how  $\rho$  splits when restricted to  $H$ . (To do this in practice for a particular group  $G$ , we would need a theorem that says how  $\rho$  splits when restricted to  $H$ . Such theorems are known as *branching theorems*.) Since  $\mathcal{Y}_H$ ,  $\mathcal{Y}_G$  are adapted, this construction can be done for free, since (say  $\rho|_H = \rho_1 \oplus \cdots \oplus \rho_k$ )

$$\sum_{h \in H} f_y(h)\rho(h) = \sum_{h \in H} f_y(h) [\rho_1(h) \oplus \cdots \oplus \rho_k(h)] = \hat{f}_y(\rho_1) \oplus \cdots \oplus \hat{f}_y(\rho_k).$$

Then, to finish computing  $\hat{f}(\rho)$ , we need to multiply  $\frac{|G|}{|H|}$  matrices together and add the results. Denote  $\sum_{h \in H} f_y(h)\rho(h)$  by  $A_y(\rho)$ . Then by choosing our representations  $\mathcal{Y}_G$ ,  $\mathcal{Y}_H$  for  $G$  and  $H$  to be adapted to the chain  $G > H$ , we have

**Theorem 8.3.**

$$\mathcal{T}_{\mathcal{Y}_G}(G) \leq \frac{|G|}{|H|} \mathcal{T}_{\mathcal{Y}_H}(H) + M_G(C),$$

where  $M_G(C)$  is the number of operations needed to compute the sums

$$\sum_{y \in C} \rho(y) A_y(\rho)$$

for all  $\rho \in \mathcal{Y}_G$ , given the matrices  $A_y(\rho)$ .

$M_G(C)$  can be made small by choosing the coset representatives  $y \in C$  in such a way that  $\rho(y)$  is a sparse matrix (or, more generally, can be factored into a small number of sparse matrices).

Of course, this method can be used recursively with a subgroup chain and a corresponding collection of chain-adapted representations, as in [21], [24].

**8.3. An FFT on the symmetric group.** In this section, we describe an algorithm to compute the FFT on  $S_n$ . The FFT algorithm for  $R_n$  presented in Section 9 explicitly uses FFTs on  $S_n$ , and ideas from this algorithm are used in the FFT on  $R_n$  presented in Section 10.

Consider  $S_n$  and the subgroup chain  $S_n > S_{n-1} > \cdots > S_1 = \{1\}$ , where  $S_k$  is identified with the subgroup of  $S_n$  that fixes the points  $k+1, \dots, n$ . Choose a complete, inequivalent, irreducible set of matrix representations for  $\mathbb{C}S_n$  adapted to this chain and call it  $\mathcal{Y}_n$ . Two well-known choices are Young's orthogonal and Young's seminormal forms (see, for example, [10]). Let  $t_j$  be the transposition  $(j-1, j)$ . Let  $e$  denote the identity element of  $S_n$ . We use the following set of coset representatives:

$$\{T_i : 1 \leq i \leq n, T_i = \underbrace{e \cdots e}_i t_{i+1} t_{i+2} \cdots t_n\}.$$

Thus, for example,  $T_1 = t_2 t_3 \cdots t_n$ ,  $T_{n-1} = t_n$ , and  $T_n = e$ . We therefore obtain

$$(15) \quad \sum_{s \in S_n} f(s)\rho(s) = \sum_{i=1}^n \rho(T_i) \sum_{s \in S_{n-1}} f_{T_i}(s)\rho(s),$$

which then implies

$$(16) \quad \mathcal{T}_{\mathcal{Y}_n}(S_n) \leq \frac{|S_n|}{|S_{n-1}|} \mathcal{T}_{\mathcal{Y}_{n-1}}(S_{n-1}) + M_{S_n}(\{T_i\}).$$

Once we have calculated all the  $f_{T_i}$  on  $S_{n-1}$ , then for any  $\rho \in \mathcal{Y}_n$ , we can reconstruct (for free, since we are using chain-adapted matrix representations) the inner sums in (15) based on how  $\rho$  splits when restricted to  $S_{n-1}$ . This splitting is described by the branching theorem for  $S_n$  (see, for example, [10], p. 304).

We now turn to analyzing the  $M_{S_n}(\{T_i\})$  term in (16). Notice that, for  $j > 2$ ,  $t_j \in S_j$  and  $t_j$  commutes with  $S_{j-2}$  (and  $t_2 \in S_2$  and  $t_2$  commutes with  $S_1$ ). It is easy to derive from the combinatorics of Young tableaux (see, for example, [16]) that the maximum multiplicity occurring in the restriction of any irreducible representation of  $S_j$  to  $S_{j-2}$  is 2. By Schur's Lemma, then, for any  $j$  ( $2 \leq j \leq n$ ) and any  $\rho \in \mathcal{Y}_n$ ,  $\rho(t_j)$  contains at most 2 nonzero entries per row and column.

Fix  $\rho \in \mathcal{Y}_n$ . Since  $\rho(T_i) = \rho(t_{i+1})\rho(t_{i+2}) \cdots \rho(t_n)$ , computing  $\rho(T_i)A_{T_i}(\rho)$  for an arbitrary matrix  $A_{T_i}(\rho)$  may be accomplished by multiplying  $A_{T_i}(\rho)$  on the left by  $\rho(t_n)$ , multiplying the result on the left by  $\rho(t_{n-1})$ , multiplying the result of that on the left by  $\rho(t_{n-2})$ , etc. It therefore takes a maximum of  $2(n-i)d_\rho^2$  operations to perform the multiplication  $\rho(T_i)A_{T_i}(\rho)$  (keeping in mind that multiplying by the identity matrix may be done for free), and once  $\rho(T_i)A_{T_i}(\rho)$  has been computed for all  $T_i$ , it takes a maximum of  $(n-1)d_\rho^2$  operations to add the results to give  $\sum_{i=1}^n \rho(T_i)A_{T_i}(\rho)$ . Letting  $\rho$  vary over  $\mathcal{Y}_n$ , then, implies

$$\begin{aligned} M_{S_n}(\{T_i\}) &\leq \sum_{\rho \in \mathcal{Y}_n} \sum_{i=1}^n 2(n-i)d_\rho^2 + \sum_{\rho \in \mathcal{Y}_n} (n-1)d_\rho^2 \\ &= (n-1)(n)|S_n| + (n-1)|S_n| \\ &= (n^2 - 1)|S_n|. \end{aligned}$$

Putting this together with (16), we obtain:

$$\mathcal{T}_{\mathcal{Y}_n}(S_n) \leq n\mathcal{T}_{\mathcal{Y}_{n-1}}(S_{n-1}) + (n^2 - 1)|S_n|.$$

Induction on  $n$  then yields

**Theorem 8.4.**  $\mathcal{T}_{\mathcal{Y}_n}(S_n) \leq \frac{2}{3}n(n+1)^2n!$

This is of order  $n!(\log n!)^3 = |S_n| \log^3 |S_n|$ . The algorithm described here is the heart of Clausen's FFT on  $S_n$  [3].

By a more careful analysis of the matrix multiplications involved, Maslen has obtained an algorithm for the FFT on  $S_n$  of complexity  $O(|S_n| \log^2 |S_n|)$  ([20], Theorem 1.1):

**Theorem 8.5.** *Let  $\mathcal{Y}_n$  denote a complete set of inequivalent, irreducible representations for  $S_n$  in Young's orthogonal or seminormal form. Then*

$$\mathcal{T}_{\mathcal{Y}_n}(S_n) \leq \frac{3}{4}n(n-1)|S_n|.$$

### 9. AN ALGORITHM FOR THE FFT ON $R_n$

In this section, we present the faster of our two algorithms for the FFT on  $R_n$ . In the process, we prove Theorems 8.1 and 8.2.

**9.1. An FFT for changing from the  $\{\lfloor s \rfloor\}$  basis to a Fourier basis.** Let  $f \in CR_n$  be an arbitrary element, given with respect to the  $\{\lfloor s \rfloor\}$  basis:

$$f = \sum_{s \in R_n} f(s) \lfloor s \rfloor.$$

Let  $\mathcal{Y}_k$  denote Young's seminormal (or orthogonal) matrix representations for  $S_k$ . For our complete set of inequivalent, irreducible representations for  $R_n$ , we take the set  $\mathcal{Y}$  induced by  $\bigcup_{k \in \{0, \dots, n\}} \mathcal{Y}_k$  in the manner described in Section 6.1. If  $\bar{\rho} \in \mathcal{Y}$  was induced by  $\rho \in \mathcal{Y}_k$ , then we have that  $\hat{f}(\bar{\rho})$  is an  $\binom{n}{k} \times \binom{n}{k}$  matrix whose rows and columns are indexed by the  $k$ -subsets of  $\{1, \dots, n\}$ , with entries themselves  $d_\rho \times d_\rho$  matrices. By Theorem 5.1 and (9), we know that for  $s \in R_n$ ,

$$\bar{\rho}(\lfloor s \rfloor) = \begin{cases} 0 & \text{if } \text{rk}(s) \neq k, \\ E_{\text{ran}(s), \text{dom}(s)} \otimes \rho(p_{(\text{ran}(s) \rightarrow \{1, \dots, k\})} sp_{(\{1, \dots, k\} \rightarrow \text{dom}(s))}) & \text{otherwise.} \end{cases}$$

Let  $A$  and  $B$  be  $k$ -subsets of  $\{1, \dots, n\}$ . Then the  $A, B$  entry of  $\hat{f}(\bar{\rho})$  is

$$(17) \quad \hat{f}(\bar{\rho})_{A,B} = \sum_{s \in S_k} f(p_{(\{1, \dots, k\} \rightarrow A)} sp_{B \rightarrow \{1, \dots, k\}}) \rho(s).$$

If we define a function  $f_{A,B}$  on  $S_k$  by

$$f_{A,B}(s) = f(p_{(\{1, \dots, k\} \rightarrow A)} sp_{B \rightarrow \{1, \dots, k\}}),$$

then (17) is just  $\hat{f}_{A,B}(\rho)$ , a Fourier transform on  $S_k$ . An obvious algorithm presents itself: for each  $k$ , run  $\binom{n}{k}^2$  FFTs on  $S_k$ . By Theorem 8.5,

$$\mathcal{T}_{\mathcal{Y}_k}(S_k) \leq \frac{3}{4}k(k-1)|S_k|.$$

**Theorem** (Theorem 8.1).  $\mathcal{C}^{\lfloor s \rfloor}(R_n) = O(|R_n| \log^2 |R_n|)$ .

*Proof.* By the above algorithm,

$$\begin{aligned} \mathcal{T}_{\mathcal{Y}}^{\lfloor s \rfloor}(R_n) &\leq \sum_{k=0}^n \binom{n}{k}^2 \mathcal{T}_{\mathcal{Y}_k}(S_k) \\ &\leq \sum_{k=0}^n \binom{n}{k}^2 \frac{3}{4}k(k-1)k! \\ &\leq \frac{3}{4}n(n-1) \sum_{k=0}^n \binom{n}{k}^2 k! \\ &\leq \frac{3}{4}n(n-1)|R_n|. \end{aligned}$$

Since  $\mathcal{C}^{\lfloor s \rfloor}(R_n) \leq \mathcal{T}_{\mathcal{Y}}^{\lfloor s \rfloor}(R_n)$ ,  $|R_n| \geq n!$ , and  $n = O(\log(n!))$ , we are done.  $\square$

**9.2. An FFT for changing from the  $\{s\}$  basis to a Fourier basis.** Let  $f \in \mathbb{C}R_n$  be an arbitrary element, given with respect to the  $\{s\}$  basis:

$$f = \sum_{s \in R_n} f(s)s.$$

Thanks to the algorithm in Section 9.1, a simple algorithm for calculating the Fourier transform of  $f$  is evident: use the set  $\mathcal{Y}$  of inequivalent, irreducible matrix representations for  $R_n$  used in Section 9.1, re-express  $f$  in terms of the  $\{\lfloor s \rfloor\}$  basis, and then run the algorithm in Section 9.1. Under this approach, the only algorithmic complexity left to consider is the complexity of changing from the  $\{s\}$  basis to the  $\{\lfloor s \rfloor\}$  basis. Suppose

$$f = \sum_{s \in R_n} g(s) \lfloor s \rfloor.$$

Since

$$s = \sum_{t \in R_n : t \leq s} \lfloor t \rfloor,$$

basic linear algebra gives

$$g(s) = \sum_{x \in R_n : x \geq s} f(x).$$

Given  $s \in R_n$  with  $\text{rk}(s) = k$ , there are  $|R_{n-k}|$  elements  $x \in R_n$  satisfying  $x \geq s$ . A naive implementation of the  $\{s\} \rightarrow \{\lfloor s \rfloor\}$  change of basis therefore takes at most

$$(18) \quad \sum_{k=0}^n \binom{n}{k}^2 k! |R_{n-k}|$$

operations.

If we consider the matrix that encodes this change of basis (which consists only of zeroes and ones), then (18) is the number of ones in this matrix, counted row by row, since a row corresponding to an element  $s \in R_n$  of rank  $k$  has  $|R_{n-k}|$  ones in it. On the other hand, a column corresponding to an element  $s \in R_n$  of rank  $k$  has  $2^k$  ones in it, so counting column by column, we obtain:

$$\sum_{k=0}^n \binom{n}{k}^2 k! |R_{n-k}| = \sum_{k=0}^n \binom{n}{k}^2 k! 2^k,$$

and thus the  $\{s\} \rightarrow \{\lfloor s \rfloor\}$  change of basis takes at most

$$\sum_{k=0}^n \binom{n}{k}^2 k! 2^k \leq 2^n \sum_{k=0}^n \binom{n}{k}^2 k! = 2^n |R_n|$$

operations.

Putting this together with Theorem 8.1, we obtain

**Theorem** (Theorem 8.2). *Let  $\epsilon > 0$ . Then*

$$\mathcal{C}^s(R_n) = O(|R_n|^{1+\epsilon}).$$

*Proof.* The algorithm in this section consists of two steps: change from the  $\{s\}$  basis to the  $\{\lfloor s \rfloor\}$  basis, and then run the algorithm in Section 9.1. Thus

$$\begin{aligned} \mathcal{C}^s(R_n) &\leq \mathcal{T}_{\mathcal{Y}}^s(R_n) \\ &\leq 2^n |R_n| + \mathcal{T}_{\mathcal{Y}}^{\lfloor s \rfloor}(R_n) \\ &\leq 2^n |R_n| + \frac{3}{4}n(n-1)|R_n|. \end{aligned}$$

For large enough  $n$ , we have  $2^n \geq \frac{3}{4}n(n-1)$  and  $|R_n|^c \geq n!^c \geq 2^n$ , so

$$\mathcal{T}_{\mathcal{Y}}^s(R_n) = O(|R_n|^{1+\epsilon}).$$

□

*Remark.* In his doctoral thesis [19], the first author has developed an  $O(|R_n| \log^3 |R_n|)$  algorithm for the  $\{s\} \rightarrow \{\lfloor s \rfloor\}$  change of basis, which in turn yields the improved result  $\mathcal{C}(R_n) = O(|R_n| \log^3 |R_n|)$ .

## 10. ANOTHER ALGORITHM FOR THE FFT ON $R_n$

In this section, we present an algorithm for the FFT on  $R_n$  that is quite different from the algorithm presented in Section 9. The algorithm in Section 9 involved examining the poset structure of  $R_n$ , decomposing  $\mathbb{C}R_n$  into matrix algebras over group algebras, using matrix representations for  $R_n$  induced by computationally advantageous matrix representations of  $S_k$ , and running FFTs on  $S_k$ .

In contrast, the algorithm in this section directly generalizes the ideas in Sections 8.2 and 8.3. It involves finding a semigroup factorization of  $R_n$  into “cosets” and using a chain-adapted set of matrix representations to run recursive calculations on the sub-semigroup chain  $R_n > R_{n-1} > \dots > R_1$ . The algorithm in this section computes the Fourier transform of an element in  $\mathbb{C}R_n$  expressed with respect to the  $\{s\}$  basis directly, without referencing the  $\{\lfloor s \rfloor\}$  basis. It is not an  $O(|R_n| \log^c |R_n|)$  algorithm, so we do not consider the  $\{\lfloor s \rfloor\} \rightarrow \{s\}$  change of basis necessary to run it on the  $\{\lfloor s \rfloor\}$  basis. Even for an element expressed with respect to the  $\{s\}$  basis, the algorithm in Section 9 is slightly better. Nevertheless, we present this algorithm because the ideas involved may be helpful for designing FFTs on other inverse semigroups.

**10.1. Another FFT for changing from the  $\{s\}$  basis to a Fourier basis.**  
Let  $f \in \mathbb{C}R_n$  be an arbitrary element, given with respect to the  $\{s\}$  basis:

$$f = \sum_{s \in R_n} f(s)s.$$

As with the symmetric group (Section 8.3), let  $t_j$  be the transposition  $(j-1, j)$ . We use the following sets of “coset representatives” (we call them “coset representatives” because they play the same role in this FFT as coset representatives do in group FFTs):

$$\{T_i : 1 \leq i \leq n, T_i = t_{i+1}t_{i+2} \cdots t_n\} \text{ (where } T_n = \text{Id}) \text{ and}$$

$$\{T^i : 1 \leq i \leq n-1, T^i = t_n t_{n-1} \cdots t_{i+1}\}.$$

We use the semigroup chain  $R_n > R_{n-1} > \dots > R_1$ , where

$$R_k = \{\sigma \in R_n : \sigma(j) = j \text{ if } j > k\}.$$

Halverson [14] has found a complete set of inequivalent, irreducible matrix representations for  $R_n$  adapted to this chain. The description may be found in Section 10.2. Call this set  $\mathcal{Y}_n$ . For each  $\rho \in \mathcal{Y}_n$ , we must compute

$$\hat{f}(\rho) = \sum_{s \in R_n} f(s)\rho(s).$$

A subsemigroup does not necessarily partition its parent semigroup into equally sized cosets, so we cannot directly factor through a subsemigroup as in (14). Instead, we use an approach for  $R_n$  that is based on the recursive formula (2). With this, we have the following factorization theorem.

**Theorem 10.1** (factorization theorem for  $R_n$ ). *For any representation  $\rho$  of  $R_n$ , if  $n \geq 3$ , we have the following factorization:*

$$(19) \quad \begin{aligned} \hat{f}(\rho) &= \sum_{i=1}^n \rho(T_i) \sum_{s \in R_{n-1}} f_{T_i}(s)\rho(s) + \rho([n]) \sum_{s \in R_{n-1}} f_{[n]}(s)\rho(s) \\ &\quad + \sum_{i=1}^{n-1} \left[ \sum_{s \in R_{n-1}} f^{T^i}(s)\rho(s) \right] \rho(T^i), \end{aligned}$$

where  $[n]$  is the link  $(1)(2) \cdots (n-1)[n]$ ,  $f_A(s) = f(As)$ , and

$$f^{T^i}(s) = \begin{cases} 0 & \text{if } n-1 \in \text{dom}(s), \\ f(sT^i) & \text{otherwise.} \end{cases}$$

*Proof.* See Section 10.3. □

As in the group case, we will use the above breakdown to compute  $\hat{f}(\rho)$  recursively. If we knew  $\widehat{f_{[n]}}(\gamma)$  for all  $\gamma \in \mathcal{Y}_{n-1}$ ,  $\widehat{f_{T_i}}(\gamma)$  for all  $\gamma \in \mathcal{Y}_{n-1}$  and  $1 \leq i \leq n$ , and  $\widehat{f^{T^i}}(\gamma)$  for all  $\gamma \in \mathcal{Y}_{n-1}$  and  $1 \leq i \leq n-1$ , using (19) we could reassemble them for free, since we are using chain-adapted representations, based on how  $\rho$  splits when restricted to  $R_{n-1}$  (see Theorem 10.6) to calculate the inner sums in (19). To finish computing  $\hat{f}(\rho)$  for any  $\rho \in \mathcal{Y}_n$ , then, we multiply these inner sums by the  $\rho(T_i)$ ,  $\rho(T^i)$ , and  $\rho([n])$  and add them up. Therefore, we have

**Lemma.** For  $n \geq 3$ ,

$$\mathcal{T}_{\mathcal{Y}_n}^s(R_n) \leq 2n\mathcal{T}_{\mathcal{Y}_{n-1}}^s(R_{n-1}) + M_{R_n},$$

where  $M_{R_n}$  is the total number of operations required to compute the sum (19) for all  $\rho \in \mathcal{Y}_n$ , given knowledge of the  $\widehat{f_{[n]}}$ , all the  $\widehat{f_{T_i}}$ , and all the  $\widehat{f^{T^i}}$  on  $R_{n-1}$ .

We now analyze  $M_{R_n}$  to obtain:

**Theorem 10.2.** For  $n \geq 3$ ,

$$(20) \quad \mathcal{T}_{\mathcal{Y}_n}^s(R_n) \leq 2n\mathcal{T}_{\mathcal{Y}_{n-1}}^s(R_{n-1}) + 2n^2|R_n|.$$

*Proof.* To analyze  $M_{R_n}$ , let:

- $M_1$  = The maximum number of operations necessary to calculate the matrix product  $\rho(T_i)A_{T_i}(\rho)$  for arbitrary matrices  $A_{T_i}(\rho)$ , for all  $\rho \in \mathcal{Y}_n$  and for all  $T_i$  ( $1 \leq i \leq n$ ).

- $M_2$  = The maximum number of operations necessary to calculate the matrix product  $A^{T^i}(\rho)\rho(T^i)$  for arbitrary matrices  $A^{T^i}(\rho)$ , for all  $\rho \in \mathcal{Y}_n$  and for all  $T^i$  ( $1 \leq i \leq n-1$ ).
- $M_3$  = The maximum number of operations necessary to calculate the matrix product  $\rho([n])A_{[n]}(\rho)$  for arbitrary matrices  $A_{[n]}(\rho)$ , for all  $\rho \in \mathcal{Y}_n$ .
- $M_4$  = The maximum number of operations necessary to add together  $2n$   $d_\rho \times d_\rho$  arbitrary matrices, for all  $\rho \in \mathcal{Y}_n$ .

Then  $M_{R_n} \leq \sum_{i=1}^4 M_i$ .

Analysis of  $M_1$ : For each  $\rho \in \mathcal{Y}_n$  and each  $T_i$ , we must perform the multiplication  $\rho(T_i)A_{T_i}(\rho) = \rho(t_{i+1})\rho(t_{i+2}) \cdots \rho(t_n)A_{T_i}(\rho)$  for an arbitrary matrix  $A_{T_i}(\rho)$ . As was the case with  $S_n$ , for  $j > 2$ ,  $t_j \in R_j$ ,  $t_j$  commutes with  $R_{j-2}$ , and  $\mathcal{M}(R_j, R_{j-2}) = 2$ . By Schur's Lemma,  $\rho(t_j)$  ( $j > 2$ ) contains at most 2 nonzero entries per row and column. For  $j = 2$ ,  $t_2 \in R_2$ , and the maximum dimension of an irreducible representation of  $R_2$  is 2. Therefore,  $\rho(t_2)$  contains at most 2 nonzero entries per row and column. Alternatively, it is obvious from the description of  $\mathcal{Y}_n$  (see Section 10.2) that  $\rho(t_j)$  ( $j \geq 2$ ) contains at most 2 nonzero entries per row and column. Therefore, multiplying an arbitrary matrix by  $\rho(t_j)$  on the left requires at most  $2d_\rho^2$  operations, and so performing the multiplication  $\rho(T_i)A_{T_i}(\rho)$  requires at most  $2(n-i)d_\rho^2$  operations. Therefore, we have

$$M_1 \leq \sum_{\rho \in \mathcal{Y}_n} \sum_{i=1}^n 2(n-i)d_\rho^2 = (n)(n-1)|R_n|,$$

where the final equality comes from (4).

Analysis of  $M_2$ : The only difference between  $M_1$  and  $M_2$  is that  $M_2$  involves multiplying arbitrary matrices by  $\rho(T^i)$  on the right rather than by  $\rho(T_i)$  on the left, so  $M_2$  is the same as  $M_1$  in the complexity analysis. Thus

$$M_2 \leq (n)(n-1)|R_n|.$$

Analysis of  $M_3$ : Since  $[n] \in R_n$ ,  $[n]$  commutes with  $R_{n-1}$ , and  $\mathcal{M}(R_n, R_{n-1}) = 1$ , we have that  $\rho([n])$  contains at most 1 nonzero entry per row. Thus

$$M_3 \leq \sum_{\rho \in \mathcal{Y}_n} d_\rho^2 = |R_n|.$$

Analysis of  $M_4$ : For a particular  $\rho$ , the matrix additions can be accomplished with  $(2n-1)d_\rho^2$  operations. Thus

$$M_4 \leq \sum_{\rho \in \mathcal{Y}_n} (2n-1)d_\rho^2 = (2n-1)|R_n|.$$

Putting this all together, we obtain

$$M_{R_n} \leq (2(n)(n-1) + 1 + 2n-1)|R_n| = 2n^2|R_n|.$$

□

We now prove that this algorithm gives the following complexity result.

**Theorem 10.3.** *For  $n \geq 5$ ,  $\mathcal{T}_{\mathcal{Y}_n}^s(R_n) \leq 2^n n|R_n|$ .*

*Proof.* Base case:  $|R_2| = 7$ , so a naive implementation of the FFT on  $R_2$  gives  $\mathcal{T}_{\mathcal{Y}_2}^s(R_2) \leq 49$ . Applying (20) repeatedly, we have

$$\begin{aligned}\mathcal{T}_{\mathcal{Y}_3}^s(R_3) &\leq 2(3)\mathcal{T}_{\mathcal{Y}_2}^s(R_2) + 2(3)^2|R_3| \leq 6(49) + 18(34) = 906, \text{ so} \\ \mathcal{T}_{\mathcal{Y}_4}^s(R_4) &\leq 2(4)\mathcal{T}_{\mathcal{Y}_3}^s(R_3) + 2(4)^2|R_4| \leq 8(906) + 32(209) = 13936, \text{ so} \\ \mathcal{T}_{\mathcal{Y}_5}^s(R_5) &\leq 2(5)\mathcal{T}_{\mathcal{Y}_4}^s(R_4) + 2(5)^2|R_5| \leq 10(13936) + 50(1546) = 216660, \text{ and} \\ 216660 &< 2^5(5)|R_5| = 247360.\end{aligned}$$

This proves the base case.

Similarly, for  $n = 6$ , we have

$$\begin{aligned}\mathcal{T}_{\mathcal{Y}_6}^s(R_6) &\leq 2(6)\mathcal{T}_{\mathcal{Y}_5}^s(R_5) + 2(6)^2|R_6| \leq 12(216660) + 72(13327) \\ &= 3559464, \text{ and } 3559464 < 2^6(6)|R_6| = 5117568.\end{aligned}$$

Now, let  $n \geq 7$ . Observe that, for  $\alpha = 1$  to  $n$ , the sets  $\{\sigma \in R_n : \sigma(\alpha) = n\}$  are disjoint, and each are of size  $|R_{n-1}|$ ; thus  $n|R_{n-1}| \leq |R_n|$ . Therefore, we have

$$\begin{aligned}
\mathcal{T}_{\mathcal{Y}_n}^s(R_n) &\leq 2n\mathcal{T}_{\mathcal{Y}_{n-1}}^s(R_{n-1}) + 2n^2|R_n| \\
&\leq 2n(2^{n-1}(n-1)|R_{n-1}|) + 2n^2|R_n| \\
&\leq 2^n(n-1)|R_n| + 2n^2|R_n| \\
&= 2^n n|R_n| + (2n^2 - 2^n)|R_n| \\
&\leq 2^n n|R_n| \text{ (since } 2n^2 \leq 2^n \text{ for } n \geq 7\text{).}
\end{aligned}$$

**10.2. Chain-adapted matrix representations for  $R_n$ .** In this section, we give a description of a complete set of irreducible, inequivalent, chain-adapted matrix representations for  $R_n$  relative to the chain  $R_n > R_{n-1} > \dots > R_1$ . The results herein are a special case of the results in [14].

**Definition** (partition). A *partition*  $\lambda$  of a nonnegative integer  $k$  (written  $\lambda \vdash k$ ) is a weakly decreasing sequence of nonnegative integers whose sum is  $k$ . We consider two partitions to be equal if and only if they only differ by the number of 0's they contain, and we identify a partition  $\lambda$  with its Young diagram.

For example,  $\lambda = (5, 5, 3, 1)$  is a partition of 14, and

It is well known that a complete set of inequivalent, irreducible representations for  $R_n$  is indexed by the set of all partitions of the integers  $\{0, 1, \dots, n\}$  (see, for example, [13] or [31]). Therefore, for integers  $n \geq 0$ , let

$$\Lambda_n = \{\lambda \vdash k : 0 \leq k \leq n\}.$$

**Definition** ( $n$ -tableau,  $n$ -standard tableau). For  $\lambda \in \Lambda_n$ , define  $L$  to be an  $n$ -tableau of shape  $\lambda$  if it is a filling of the diagram for  $\lambda$  with numbers from  $\{1, 2, \dots, n\}$  such that each number in  $L$  appears at most once.  $L$  is an  $n$ -standard tableau if,

furthermore, the entries in each column of  $L$  increase from top to bottom and the entries in each row of  $L$  increase from left to right.

Fix  $\lambda$ . Let  $T_n^\lambda$  denote the set of  $n$ -standard tableaux of shape  $\lambda$ . The symmetric group acts on tableaux by permuting their entries. If  $L$  is an  $n$ -tableau, then  $(i-1, i)L$  is the tableau that is obtained from  $L$  by replacing  $i-1$  (if  $i-1 \in L$ ) with  $i$ , and by replacing  $i$  (if  $i \in L$ ) with  $i-1$ . Note that  $L \in T_n^\lambda$  need not imply  $(i-1, i)L \in T_n^\lambda$ .

Let  $\{v_L : L \in T_n^\lambda\}$  be a set of independent vectors. We form

$$V^\lambda = \mathbb{C}\text{-span}\{v_L : L \in T_n^\lambda\}.$$

As such, the symbols  $v_L$ , for  $L \in T_n^\lambda$ , are a basis for the vector space  $V^\lambda$ . Halverson defines an action of  $R_n$  on  $V^\lambda$  in such a way that (extending by linearity)  $V^\lambda$  is an irreducible  $\mathbb{C}R_n$ -module and such that, as  $\lambda$  ranges over  $\Lambda_n$ , the  $V^\lambda$  constitute a complete set of inequivalent, irreducible representation modules for  $R_n$ . We first describe this action, and we then describe an ordering of the bases for the  $V^\lambda$  so that the resulting matrix representations are chain-adapted to  $R_n > R_{n-1} > \dots > R_1$ .

**Definition** (content). If  $b$  is a box of  $\lambda$  in position  $(i, j)$ , then the *content* of  $b$  is defined to be

$$ct(b) = j - i.$$

Let  $L \in T_n^\lambda$ . If  $i-1, i \in L$ , then let  $L(i-1)$  and  $L(i)$  denote the box in  $L$  containing  $i-1$  and  $i$ , respectively.

To define the action of  $R_n$  on  $V^\lambda$ , it is sufficient to define the action of a set of generators of  $R_n$  on  $V^\lambda$ .

**Definition** (action of  $R_n$  on  $V^\lambda$ ). Define the action of the transpositions  $t_i = (i-1, i)$ , for  $2 \leq i \leq n$ , as follows:

$$t_i v_L = \begin{cases} \frac{1}{ct(L(i)) - ct(L(i-1))} v_L + \left(1 + \frac{1}{ct(L(i)) - ct(L(i-1))}\right) v_{L'} & \text{if } i-1, i \in L, \\ v_{t_i L} & \text{if exactly one of } i-1, i \in L, \\ v_L & \text{if } i-1, i \notin L, \end{cases}$$

where

$$v_{L'} = \begin{cases} v_{t_i L} & \text{if } t_i L \text{ is } n\text{-standard,} \\ 0 & \text{otherwise.} \end{cases}$$

Define the action of the link  $(1)(2)\cdots(n-1)[n] = [n]$  on  $V^\lambda$  by

$$[n]v_L = \begin{cases} v_L & \text{if } n \notin L, \\ 0 & \text{if } n \in L. \end{cases}$$

*Remark.* If  $\lambda = (0)$ , then  $V^\lambda$  is 1-dimensional, and the action of  $R_n$  on  $V^\lambda$  is the trivial action given by  $xv = v$  for all  $x \in R_n$  and all  $v \in V^\lambda$ .

**Theorem 10.4.** As  $\lambda$  varies over all partitions of all nonnegative integers less than or equal to  $n$ , the  $V^\lambda$  constitute a complete set of irreducible, pairwise non-isomorphic representation modules for  $R_n$  [14].

**Definition** (corner of a partition). A corner is a box  $c$  of  $\lambda$  for which  $\lambda$  contains no box to the right or below  $c$ . In other words, the corners are the possible positions of  $n$  in an  $n$ -standard tableau of shape  $\lambda$ .

We now record the branching theorem for  $R_n$ .

**Theorem 10.5** (branching theorem). *As a  $\mathbb{C}R_{n-1}$  module,*

$$V^\lambda \cong \bigoplus_{\mu \in \lambda^{-,=}} V^\mu,$$

where  $\lambda^{-,=}$  is the set of all partitions  $\mu \in \Lambda_{n-1}$  such that either  $\mu = \lambda$  (if  $\lambda \not\vdash n$ ) or  $\mu$  is obtained by removing a corner from  $\lambda$  [14].

Now, for purposes of chain-adaptation, we order the basis  $\{v_L\}$  for  $V^\lambda$  using the following generalized last-letter ordering.

We begin by partitioning the  $v_L$  into subsets based on the corners  $c_1, \dots, c_l$  of  $\lambda$ . Number the corners from top to bottom. Now, form the sets

$$V^\lambda(0) = \{v_L : L \in T_n^\lambda \text{ and } n \notin L\},$$

$$V^\lambda(i) = \{v_L : L \in T_n^\lambda \text{ and } n \in c_i \text{ of } L\}, \quad 1 \leq i \leq l,$$

and declare elements of  $V^\lambda(j)$  to be earlier in the ordering than elements of  $V^\lambda(k)$  whenever  $j < k$ . To order the subset  $V^\lambda(k)$ , delete the corner  $c_k$  (do nothing if  $k = 0$ ) and repeat the same ordering process (starting by identifying the corners of the resulting partition and partitioning the  $v_L$  into subsets based on those corners) with  $n - 1$  in place of  $n$ , etc.

As an example, consider  $\lambda = (2, 1, 1)$ , which has two corners, and  $R_5$ . Our ordered basis for the 15-dimensional  $V^\lambda$  is

$$\begin{aligned} v \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & \\ \hline 3 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline 4 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 5 \\ \hline 2 & \\ \hline 3 & \\ \hline 4 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 5 \\ \hline 2 & \\ \hline 3 & \\ \hline 4 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 5 \\ \hline 3 & \\ \hline 4 & \\ \hline 2 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 2 & 5 \\ \hline 1 & \\ \hline \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 2 & \\ \hline \\ \hline \end{array} \\ &< v \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 3 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 2 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 4 \\ \hline 3 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 2 & 4 \\ \hline 3 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 2 \\ \hline 4 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 1 & 3 \\ \hline 4 & \\ \hline 5 & \\ \hline \end{array} &< v \begin{array}{|c|c|} \hline 2 & 3 \\ \hline 4 & \\ \hline 5 & \\ \hline \end{array} \end{aligned}$$

*Remark.* If  $\lambda \vdash n$ , then the generalized last-letter ordering scheme given above reduces to the usual last-letter ordering scheme used for Young's orthogonal and seminormal representations of the symmetric group.

It is now easy to see, under this ordering of the bases for the  $V^\lambda$ , that the matrix representations described in this section are chain-adapted to the chain  $R_n > R_{n-1} > \dots > R_1$ . We know, by the branching theorem for  $R_n$ , how  $V^\lambda$  decomposes as a  $R_{n-1}$  module (it decomposes into the  $\mathbb{C}$ -span of the  $V^\lambda(k)$  for  $0 \leq k \leq l$ ), and it is obvious by the action of  $R_{n-1}$  on  $V^\lambda$  that

$$R_{n-1} \mathbb{C}\text{-span}(V^\lambda(k)) \subseteq \mathbb{C}\text{-span}(V^\lambda(k))$$

for all  $k$ . The same argument is used to induct down the chain  $R_n > \dots > R_1$ , now, and is trivial because we ordered our basis for  $V^\lambda$  inductively according to the same rule. We now restate the branching theorem for  $R_n$  under our ordering of the bases for the  $V^\lambda$ .

**Theorem 10.6** (branching theorem). *Let  $\rho^\lambda$  be the matrix representation associated to  $V^\lambda$  with respect to the basis  $\{v_L\}$ , with the basis ordered according to the generalized last-letter ordering. Then*

$$\rho^\lambda|_{R_{n-1}} = \bigoplus_{\mu \in \lambda^{-,=}} \rho^\mu,$$

where  $\lambda^{-,=}$  is the set of all partitions  $\mu \in \Lambda_{n-1}$  such that either  $\mu = \lambda$  or  $\mu$  is obtained by removing a corner from  $\lambda$ . The first  $\mu \in \lambda^{-,=}$  is the one that removes no corners (if  $\lambda \not\vdash n$ ), the next  $\mu$  is the one that removes the highest corner, the next  $\mu$  is the one that removes the second highest corner, etc.

**10.3. Proof of Theorem 10.1.** To provide motivation for the proof of Theorem 10.1, we begin by proving the recursive formula

**Theorem** (Theorem 2.3). *For  $n \geq 3$ ,  $|R_n| = 2n|R_{n-1}| - (n-1)^2|R_{n-2}|$ .*

*Proof.* Viewing the elements of  $R_n$  as rook matrices,  $R_n$  consists of those elements having all 0's in column  $n$  and row  $n$  (of which there are  $|R_{n-1}|$ ), together with, for each  $\alpha \in \{1, \dots, n\}$ , those having a 1 in position  $(\alpha, n)$  (of which there are  $n|R_{n-1}|$  total), together with, for each  $\alpha \in \{1, \dots, n-1\}$ , those having a 1 in position  $(n, \alpha)$  (of which there are  $(n-1)|R_{n-1}|$  total). Counting the number of elements of  $R_n$  in this way overcounts. For each  $(\alpha, \beta)$  with  $1 \leq \alpha, \beta \leq n-1$ , every element with 1's in positions  $(\alpha, n)$  and  $(n, \beta)$  (of which there are  $(n-1)^2|R_{n-2}|$  total) gets counted twice.  $\square$

Now, let  $f \in \mathbb{C}R_n$  be given with respect to the  $\{s\}$  basis. We prove Theorem 10.1.

**Theorem** (Theorem 10.1). *For any representation  $\rho$  on  $R_n$ , if  $n \geq 3$ , we have the following factorization:*

$$\begin{aligned} \hat{f}(\rho) &= \sum_{i=1}^n \rho(T_i) \sum_{s \in R_{n-1}} f_{T_i}(s) \rho(s) + \rho([n]) \sum_{s \in R_{n-1}} f_{[n]}(s) \rho(s) \\ &\quad + \sum_{i=1}^{n-1} \left[ \sum_{s \in R_{n-1}} f^{T^i}(s) \rho(s) \right] \rho(T^i), \end{aligned}$$

where  $[n]$  is the link  $(1)(2) \cdots (n-1)[n]$ ,  $f_A(s) = f(As)$ , and

$$f^{T^i}(s) = \begin{cases} 0 & \text{if } n-1 \in \text{dom}(s), \\ f(sT^i) & \text{otherwise.} \end{cases}$$

*Proof.* Let  $n \geq 3$ . We have 3 types of elements  $s$  of  $R_n$ .

- Type 1: Those for which  $s(n) = i$  for some  $1 \leq i \leq n$ .
- Type 2: Those for which both  $s(i) = n$  for some  $1 \leq i \leq n-1$  and  $n \notin \text{dom}(s)$ .
- Type 3: Those for which both  $s(i) \neq n$  for all  $1 \leq i \leq n$  and  $n \notin \text{dom}(s)$ .

By the argument given in the proof of Theorem 2.3, this counts all elements of  $R_n$  precisely once.

Now, let  $1 \leq i \leq n$ . View the “coset representative”  $T_i$  as a permutation matrix, and view the elements  $s \in R_n$  as rook matrices. Multiplying any matrix  $X$  on the left by  $T_i$  simply moves row  $j$  of  $X$  to row  $j+1$  (for all  $j$  such that  $i \leq j \leq n-1$ ) and moves row  $n$  of  $X$  to row  $i$ . Thus, as  $s$  varies over  $R_{n-1}$ ,  $T_i s$  varies bijectively over  $\{s \in R_n : s(n) = i\}$ . Therefore, we have

$$\begin{aligned} \sum_{s \in R_n \text{ of Type 1}} f(s)\rho(s) &= \sum_{i=1}^n \sum_{s \in R_{n-1}} f(T_i s)\rho(T_i s) \\ &= \sum_{i=1}^n \sum_{s \in R_{n-1}} f_{T_i}(s)\rho(T_i)\rho(s) \\ &= \sum_{i=1}^n \rho(T_i) \sum_{s \in R_{n-1}} f_{T_i}(s)\rho(s), \end{aligned}$$

where  $f_{T_i}(s) = f(T_i s)$ .

Similarly, multiplying any matrix  $X$  on the right by  $T^i$  moves column  $j$  of  $X$  to column  $j+1$  ( $i \leq j \leq n-1$ ) and moves column  $n$  of  $X$  to column  $i$ . Thus, as  $s$  varies over  $R_{n-1}$ ,  $sT^i$  varies bijectively over  $\{s \in R_n : s(i) = n\}$ . So

$$\begin{aligned} \sum_{s \in R_n : s(i)=n} f(s)\rho(s) &= \sum_{s \in R_{n-1}} f(sT^i)\rho(sT^i) \\ &= \sum_{s \in R_{n-1}} f(sT^i)\rho(s)\rho(T^i). \end{aligned}$$

To ensure that we only count the elements of Type 2, we restrict our attention to  $1 \leq i \leq n-1$ , and we set the function values of the elements of Type 1 appearing in the above sum to 0:

$$\begin{aligned} \sum_{s \in R_n \text{ of Type 2}} f(s)\rho(s) &= \sum_{i=1}^{n-1} \sum_{s \in R_{n-1}} f^{T^i}(s)\rho(sT^i) \\ &= \sum_{i=1}^{n-1} \left[ \sum_{s \in R_{n-1}} f^{T^i}(s)\rho(s) \right] \rho(T^i), \end{aligned}$$

where

$$f^{T^i}(s) = \begin{cases} 0 & \text{if } n-1 \in \text{dom}(s) \text{ (i.e., } n \in \text{dom}(sT^i)), \\ f(sT^i) & \text{otherwise.} \end{cases}$$

Finally,

$$\begin{aligned} \sum_{s \in R_n \text{ of Type 3}} f(s)\rho(s) &= \sum_{s \in R_{n-1}} f([n]s)\rho([n]s) \\ &= \rho([n]) \sum_{s \in R_{n-1}} f_{[n]}(s)\rho(s). \end{aligned}$$

Putting this all together, then, we find that for any representation  $\rho$  of  $R_n$  and any  $n \geq 3$ ,

$$\begin{aligned} \hat{f}(\rho) &= \sum_{s \in R_n \text{ of Type 1}} f(s)\rho(s) + \sum_{s \in R_n \text{ of Type 2}} f(s)\rho(s) + \sum_{s \in R_n \text{ of Type 3}} f(s)\rho(s) \\ &= \sum_{i=1}^n \rho(T_i) \sum_{s \in R_{n-1}} f_{T_i}(s)\rho(s) + \rho([n]) \sum_{s \in R_{n-1}} f_{[n]}(s)\rho(s) \\ &\quad + \sum_{i=1}^{n-1} \left[ \sum_{s \in R_{n-1}} f^{T^i}(s)\rho(s) \right] \rho(T^i). \end{aligned}$$

□

## 11. CONCLUDING REMARKS

The extension of FFTs to semigroups creates a new collection of interesting challenges. We remark that many of the ideas in this paper (such as those from [34] and several of the results in this paper that follow from them) can be extended to general inverse semigroups. As with groups, FFT algorithms for inverse semigroups will vary from semigroup to semigroup, but a number of the underlying ideas are the same for any inverse semigroup FFT. These ideas can be cast in a general framework, which we intend to help guide the development of future FFTs, and this general framework is the subject of a paper currently in preparation.

Also, as mentioned previously, spectral analysis for the rook monoid involves projecting a function onto the isotypic subspaces of  $\mathbb{C}R_n$ , which can be accomplished by means of an FFT, and examining the resulting projections. A variety of interesting issues arises in this analysis, and we have worked out a detailed example, consisting of partially ranked voting data on  $R_5$ , to explain them. These results are the subject of a paper currently in preparation.

## REFERENCES

- [1] U. Baum, *Existence and efficient construction of fast Fourier transforms for supersolvable groups*, Comput. Complex. **1/3** (1992), 235–256. MR1165193 (93d:20031)
- [2] L. I. Bluestein, *A linear filtering approach to the computation of the discrete Fourier transform*, IEEE Trans. Electroacoustics **18** (1970), no. 4, 451–455.
- [3] M. Clausen and U. Baum, *Fast Fourier transforms for symmetric groups: Theory and implementation*, Math. Comput. **61** (1993), no. 204, 833–847. MR1192969 (94a:20028)
- [4] A. H. Clifford, *Matrix representations of completely simple semigroups*, Amer. J. Math. **64** (1942), no. 1, 327–342. MR0006551 (4:4a)
- [5] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, vol. 1, Mathematical Surveys No. 7, AMS, Providence, RI, 1961. MR0132791 (24:A2627)
- [6] \_\_\_\_\_, *The Algebraic Theory of Semigroups*, vol. 2, Mathematical Surveys No. 7, AMS, Providence, RI, 1967. MR0218472 (36:1558)

- [7] J. W. Cooley and J. W. Tukey, *An algorithm for machine calculation of complex Fourier series*, Math. Comput. **19** (1965), 297–301. MR0178586 (31:2843)
- [8] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley and Sons, New York, 1962. MR0144979 (26:2519)
- [9] P. Diaconis, *A generalization of spectral analysis with application to ranked data*, Ann. Statist. **17** (1989), no. 3, 949–979. MR1015133 (91a:60025)
- [10] P. Diaconis and D. Rockmore, *Efficient computation of the Fourier transform on finite groups*, J. Amer. Math. Soc. **3** (1990), no. 2, 297–332. MR1030655 (92g:20024)
- [11] ———, *Efficient computation of isotypic projections for the symmetric group*, DIMACS Series in Disc. Math. and Theor. Comp. Sci. **11** (1993), 87–104. MR1235796 (94g:20022)
- [12] B. Farb and R. K. Dennis, *Noncommutative Algebra*, Graduate Texts in Mathematics, vol. 144, Springer-Verlag, New York-Heidelberg, 1993. MR1233388 (94j:16001)
- [13] C. Grood, *A Specht module analog for the rook monoid*, Electron. J. Combin. **9** (2002). MR1887083 (2003a:05150)
- [14] T. Halverson, *Representations of the  $q$ -rook monoid*, J. Algebra **273** (2004), 227–251. MR2032458 (2005f:20011)
- [15] R. B. Holmes, *Mathematical foundation of signal processing II. The role of group theory*, Massachusetts Institute of Technology Technical Report 781 (October 13, 1987).
- [16] G. D. James, *The representation theory of the symmetric groups*, Lect. Notes Math., Springer-Verlag, Berlin **682** (1978). MR513828 (80g:20019)
- [17] S. Janson and V. Mazorchuk, *Some remarks on the combinatorics of  $IS_n$* , Semigroup Forum **70** (2005), no. 3, 391–405. MR2148152 (2006c:20123)
- [18] M. V. Lawson, *Inverse Semigroups: The Theory of Partial Symmetries*, World Scientific, Singapore, 1998. MR1694900 (2000g:20123)
- [19] M. Malandro, *Fast Fourier Transforms for Inverse Semigroups*, Thesis, Dartmouth College (2008).
- [20] D. K. Maslen, *The efficient computation of Fourier transforms on the symmetric group*, Math. Comput. **67** (1998), no. 223, 1121–1147. MR1468943 (99a:20009)
- [21] D. K. Maslen and D. N. Rockmore, *Adapted diameters and FFTs on groups*, Proc. 6th ACM-SIAM SODA, 253–262. MR1321855 (95k:65131)
- [22] ———, *Generalized FFTs—A survey of some recent results*, Proc. 1995 DIMACS Workshop on Groups and Computation **28** (1997), 183–238. MR1444138 (98k:20020)
- [23] ———, *Separation of variables and the computation of Fourier transforms on finite groups, I*, J. Amer. Math. Soc. **10** (1997), no. 1, 169–214. MR1396896 (97i:20019)
- [24] ———, *The Cooley-Tukey FFT and group theory*, Notices of the AMS **48** (2001), no. 10, 1151–1161. MR1861656 (2002k:20022)
- [25] W. D. Munn, *On semigroup algebras*, Proc. Cambridge Philos. Soc. **51** (1955), 1–15. MR0066355 (16:561c)
- [26] ———, *The characters of the symmetric inverse semigroup*, Proc. Cambridge Philos. Soc. **53** (1957), 13–18. MR0081910 (18:465d)
- [27] ———, *Matrix representations of semigroups*, Proc. Cambridge Philos. Soc. **53** (1957), 5–12. MR0082050 (18:489g)
- [28] J. Rhodes and Y. Zalcstein, *Elementary representation and character theory of finite semigroups and its application*, Monoids and Semigroups with Applications, pp. 334–367, World Sci. Publishing, River Edge, NJ, 1991. MR1142387 (92k:20129)
- [29] D. N. Rockmore, *Recent progress and applications in group FFTs*, NATO Science Series, Computational Noncommutative Algebra and Applications, vol. 136, pp. 227–254, Kluwer Acad. Publ., Dordrecht, 2004. MR2159215 (2007j:43012)
- [30] J. P. Serre, *Linear Representations of Finite Groups*, Graduate Texts in Mathematics, vol. 42, Springer-Verlag, New York-Heidelberg, 1977. MR0450380 (56:8675)
- [31] L. Solomon, *Representations of the rook monoid*, J. Algebra **256** (2002), 309–342. MR1939108 (2003m:20091)
- [32] R. Stanley, *Enumerative Combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, 1997. MR1442260 (98a:05001)
- [33] B. Steinberg, *Möbius functions and semigroup representation theory*, J. Comb. Theor. Ser. A. **113** (2006), 866–881. MR2231092 (2007c:20144)
- [34] ———, *Möbius functions and semigroup representation theory II: Character formulas and multiplicities*, Adv. in Math. **217** (2008), 1521–1557. MR2382734

- [35] F. Yates, *The design and analysis of factorial experiments*, Imp. Bur. Soil Sci. Tech. Comm. **35** (1937).

DEPARTMENT OF MATHEMATICS, 6188 KEMENY HALL, DARTMOUTH COLLEGE, HANOVER, NEW HAMPSHIRE 03755

*Current address:* Department of Mathematics and Statistics, Sam Houston State University, Box 2206, Huntsville, Texas 77341-2206

*E-mail address:* malandro@shsu.edu

DEPARTMENT OF MATHEMATICS, 6188 KEMENY HALL, DARTMOUTH COLLEGE, HANOVER, NEW HAMPSHIRE 03755

*E-mail address:* rockmore@cs.dartmouth.edu