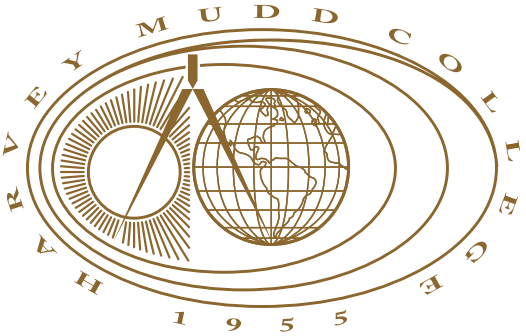
2009

Branching Diagrams for Group Inclusions Induced by Field Inclusions

Tedodore Spaide
Harvey Mudd College



Branching Diagrams for Group Inclusions Induced by Field Inclusions

Theodore Spaide

Michael Orrison, Advisor

Nicholas Pippenger, Reader

May, 2009

HARVEY MUDD COLLEGE

Department of Mathematics

Abstract

A Fourier transform for a finite group G is an isomorphism from the complex group algebra $\mathbb{C}G$ to a direct product of complex matrix algebras, which are determined beforehand by the structure of G. Given such an isomorphism, naive application of that isomorphism to an arbitrary element of CG takes time proportional to $|G|^2$. A fast Fourier transform for some (family of) groups is an algorithm which computes the Fourier transform of a group G of the family in less than $O(|G|^2)$ time, generally $O(|G| \log |G|)$ or $O(|G|(\log |G|)^2)$. I describe the construction of a fast Fourier transform for the special linear groups $SL_(q)$ with $q = 2^n$.

Contents

List of Figures

List of Tables

Acknowledgments

I would like to thank my advisor, Professor Michael Orrison, for providing me with advice and guidance throughout this project. I would also like to thank my second reader, Professor Nicholas Pippenger, for his helpful commentary. Finally, I would like to thank Claire Connelly for her corrections.

Chapter 1

Background

The primary purpose of this thesis is to study the properties of the representations of the group $SL_2(q^2)$ when restricted to act on the group $SL_2(q)$. In particular we wish to know how the irreducible representations of $SL_2(q^2)$ may be expressed in terms of the irreducible representations of $SL_2(q)$. We also handle the analogous question for the groups $\mathrm{Aff}(q^2)$ and $\mathrm{Aff}(q)$. Understanding the nature of the restrictions of the representations is useful in constructing fast Fourier transforms for the groups in question; we can use the subgroup structure of the groups to help us compute the discrete Fourier transforms.

1.1 Overview of Representation Theory

We recall some points of representation theory; for a general reference on representation theory see Baum and Clausen (1993) or Dummit and Foote (2004). Denote by $\mathbb{C}^{d\times d}$ the algebra of d by d matrices with complex entries. A *representation* of the group G is a homomorphism of algebras $\mathbb{C}G \to \mathbb{C}^{d\times d}$ for some d, the *degree* of ρ. Equivalently, we may view ρ as defining a linear action of $\mathbb{C}G$ on a vector space V of dimension d.

Two representations ρ and ρ' are said to be *equivalent* if they are equal up to a change of basis of V, that is, if there exists an invertible matrix T such that $T\rho(g) = \rho'(g)T$ for all $g \in G$. The representation ρ is called *irreducible* if it has no nontrivial proper invariant subspace; that is, if ρ acts on the vector space V, and if W is a subspace of V such that $\rho(g)W = W$ for all $g \in G$, then $W = 0$ or V. Maschke's theorem states that any representation which is not irreducible is the direct sum of two representations of lower degree, so that any representation may be written as the direct sum of irreducible

representations.

We also summarize some character theory. Given a representation ρ of G, the function $\chi(g) = Tr(\rho(g))$ is the *character* of ρ. Because the trace of matrices is unchanged by conjugation, $\chi(g)$ only depends on the conjugacy class of g and is often considered a function of conjugacy classes (a *class function*). If ρ is irreducible, then χ is called irreducible as well. If χ and χ' are irreducible, the first orthogonality relationship states that the inner product of χ and χ', defined by

$$(\chi, \chi') = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi'(g)},$$

is 1 if $\chi = \chi'$ and 0 otherwise.

If the characters of ρ and ρ' are χ and χ', respectively, then the character of the direct sum $\rho \oplus \rho'$ is the sum $\chi + \chi'$. Any two representations with the same character are equivalent; thus, given an arbitrary representation ρ that we wish to write as (being equivalent to) a direct sum of irreducible representations of G, we may determine these irreducible representations by writing the character of ρ as the sum of irreducible characters of G, which may be done using the orthogonality relation above.

The irreducible characters of of G are often summarized using a *character table*. A character table labels its rows with the irreducible representations of G and its columns with the conjugacy classes of G. The entries of the table are the values the characters of the corresponding representations take on the elements of the conjugacy classes. As in Dummit and Foote (2004) we use a representative of the conjugacy classes to stand for the entire classes, and also include the sizes of the classes below the representatives.

1.2 DFTs and FFTs

Wedderburn's theorem states that for a finite group G, $\mathbb{C}G$ is isomorphic to a direct sum $\bigoplus_i \mathbb{C}^{d_i \times d_i}$ of matrix algebras, where the isomorphism is given by the direct sum of each of the irreducible representations of G, of which there are finitely many up to equivalence (in fact, G has as many irreducible representations as it has conjugacy classes). This isomorphism is called a *discrete Fourier transform*, or *DFT*, for G.

Since a DFT D is an isomorphism, and $\mathbb{C}G$ is a $|G|$-dimensional vector space over $\mathbb{C}$, so is the matrix algebra $\bigoplus_i \mathbb{C}^{d_i \times d_i}$. Because each $\mathbb{C}^{d_i \times d_i}$ has dimension d_i^2, we must have $\sum_i d_i^2 = |G|$, so each $D(g)$ has up to $|G|$ nonzero

entries. In general, $D(g)$ will not have significantly fewer than $|G|$ entries. Thus if $a = \sum_{g \in G} \alpha_g g$ is an arbitrary element of $\mathbb{C}G$, then calculating $D(a)$ by naively evaluating $\sum_{g \in G} \alpha_g D(g)$ requires $O(|G|)$ vector operations, each of which takes $O(|G|)$ time, so the entire evaluation takes $O(|G|^2)$ time. An algorithm which takes less asymptotic time than $O(|G|^2)$ time is called a *Fast Fourier Transform*, or *FFT*.

We describe the general route we take to reduce the time to calculate the DFT from the $O(|G|^2)$ bound.

Given a subgroup $H < G$, we proceed as follows. If $g_1, \ldots, g_s$ are a complete set of left coset representatives for H, then we write

$$a = \sum_{g \in G} \alpha_g g = \sum_{i=1}^{s} \sum_{g \in g_i H} \alpha_g g = \sum_{i=1}^{s} g_i \sum_{h \in H} \alpha_{g_i h} h = \sum_{i=1}^{s} g_i a_i,$$

where $a_i = \sum_{h \in H} \alpha_{g_i h} h \in \mathbb{C}H$. Then we need only evaluate D on $s = |G : H|$ elements of $\mathbb{C}H$, perform the s multiplications $D(g_i)D(a_i)$, and then the $s - 1$ additions $\sum D(g_i)D(a_i)$.

Of these tasks, the additions and multiplications may be sped up if the DFT D has some nice structure with respect to the subgroup H and we are clever in choosing some g_i such that $D(g_i)$ are sparse (or the product of sparse matrices). As for calculating the $D(a_i)$, note that by Maschke's theorem, when D is considered as a representation of H, it is equivalent to the direct sum of irreducible representations of H. If we have chosen D such that the restriction of D to $\mathbb{C}H$ is in fact *equal* to such a direct sum, and all the equivalent direct summands are themselves equal, then this problem reduces to quickly evaluating the a_i at certain irreducible representations of H: namely, those that appear as direct summands of D. By a weakened form of Frobenius Reciprocity (see e.g. Dummit and Foote (2004)) we can say that any irreducible representation of H appears as a direct summand in at least one irreducible representation of G, and thus as a direct summand of D. Thus our problem has reduced to evaluating the a_i for all the irreducible representations of H.

The evaluation of all the representations of H is itself equivalent to evaluation of the DFT of H. We can calculate the DFT of H in a similar way to that of G by using a subgroup K of H. Repeating this procedure, we obtain a recursive procedure for computing D using some chain of subgroups $G = G_n > G_{n-1} > \cdots > G_1 > G_0 = \{1\}$. For the case where we merely had $G > H$, we required that D restrict to a direct sum of irreducible representations of H when restricted to elements of H, such that any two equivalent irreducible representations were in fact equal. For this

more general case, we want this property to extend to every containment $G_{i+1} > G_i$. Namely, when D is restricted to G_{n-1}, it is the direct sum $\oplus_j D_j$ of irreducible representations of G_{n-1}, such that if D_j and $D_{j'}$ are equivalent, then they are equal; when this is further restricted to G_{n-2}, each of the D_j will not just be equivalent to a direct sum of irreducible representations D'_k for G_{n-2}, but *equal* to such a direct sum, and any D'_k and $D'_{k'}$ that are equivalent will also be equal. Each of these D'_k will similarly split up when restricted to G_{n-3}, and so on. If this condition holds all the way down to G_0, then the representation D is called *adapted* to the chain $\{G = G_n > G_{n-1} > \cdots > G_1 > G_0 = \{1\}\}$. Because all DFTs are obtained from each other by equivalence—that is, through a change of basis on the space V—we can determine an adapted DFT by determining the basis for V. Such a basis is also called adapted.

1.2.1 Branching Diagrams

If e is an element of an adapted basis, then the restriction of D to G_k acts upon e according to some irreducible representation D_k of G_k. Because D_{k+1} and D_k both act on a space containing e, and both are irreducible (for their own groups), D_k must be a summand of the restriction $D_{k+1}|_{G_k}$. We express this structure graphically with the use of the *branching diagram* for $G = G_n > G_{n-1} > \cdots > G_1 > G_0 = \{0\}$, a multigraph whose vertices correspond to the irreducible representations of the G_i, and which has ℓ edges from the representation D_k of G_k to the representation D_{k+1} of G_{k+1} if $D_{k+1}|_{G_k}$ has D_k as a summand with multiplicity ℓ. An example of a branching diagram (for $\mathrm{Aff}(9) > \mathrm{Aff}(3) > 1$) is shown in Figure 2.1. Then we can index the basis elements e by paths in the branching diagram from the trivial representation on G_0 to some representation on G_n: following the path backward from G_n to G_0 tells us which representation D_n of G_n acts on e, which of the summands D_{n-1} of $D_n|_{G_{n-1}}$ acts on e, and so on.

For each irreducible representation D_n of $G = G_n$ we can construct a corresponding *centrally primitive idempotent* e_n. If χ is the character corresponding to D_n, then the group ring element

$$e_n = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

has the property that $D_n(e_n)$ is the identity, and, if D'_n is a nonisomorphic irreducible representation, then $D'_n(e_n)$ is zero. With the path-based indexing scheme in mind, $D(e_n)$ leaves fixed the basis element v if its path in the

branching diagram ends at D_n and sends it to zero otherwise. Similarly, if D_k is an irreducible representation of G_k with centrally primitive idempotent e_k, then $D(e_k)$ leaves fixed those basis elements whose paths in the branching diagrams pass through D_k and sends to zero the others.

Given a path in the branching diagram through $D_1, \ldots, D_n$, the product

$$D(e_1)D(e_2)\cdots D(e_n)$$

is then a projection onto the subspace generated by those basis elements whose paths in the branching diagram are precisely those paths which pass through $D_1, \ldots, D_n$. Assuming for now there are no edges of degree more than one, each such product is then a projection onto a subspace of dimension one, because there is one such path through all these representations. This is perhaps easier to understand in terms of the matrix entries; if we let $M_{i,j}$ be the matrix with a 1 in the (i, j) entry and zeroes everywhere else, the products $D(\rho_1)\cdots D(\rho_n)$ are just the matrices $M_{i,i}$. By multiplying other matrices on the left by $M_{i,i}$ and the right by $M_{j,j}$ we can obtain the matrices $M_{i,j}$. If we instead do the projections in $\mathbb{C}G$ by multiplying on the right and left by the ρ_k, we instead get the preimages $D^{-1}(M_{i,j}) \in \mathbb{C}G$, which is precisely the basis we want to use for computations with adapted DFTs.

In the general case, there will be edges of degree greater than one. In this case the projections will project onto subspaces of dimension greater than one, so we must then choose bases for these subspaces to find the $M_{i,j}$. If we are lucky, specific bases will suggest themselves to us, but otherwise we will need to use some process such as Gram-Schmidt to find one.

1.3 Previous Results

To narrow the focus of the thesis and give some context we review some previous results on FFTs.

- **Abelian Groups**: By the Fundamental Theorem of Finitely Generated Abelian Groups (see e.g. Dummit and Foote (2004)), any finite abelian group G is expressable as the product of cyclic groups. Thus the analysis reduces to calculating FFTs for $\mathbb{Z}/n\mathbb{Z}$ and to extending these to products of the groups. The first task has been studied even before the advent of the group-theoretical study of FFTs, and the second can be done without requiring too much effort. It has been shown that the DFT of any finite abelian G has linear complexity at most $8|G|\log|G|$ [(Baum et al., 1991)].

- **Solvable and Supersolvable Groups**: FFTs on solvable groups G can be performed in time $O(|G|^{3/2})$ [(Beth, 1987)]. If G is instead supersolvable, an FFT can be computed in time $O(|G| \log |G|)$ [(Baum, 1991)]. This is a generalization of the result for abelian groups.

- **The Symmetric Group**: FFTs have been shown to exist for the group S_n that take time $O(n^2 \cdot n!)$ (recall that $|S_n| = n!$ and $\log n! \sim n \log n$) [(Maslen, 1998)].

- $SL_2(q)$: FFTs for $SL_2(q)$, the special linear group over the finite field $\mathbb{F}_q$ with q odd have been found by considering the subgroup chain

$$\begin{aligned} SL_2(q) &= \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} | \alpha\delta - \beta\gamma = 0 \right\} \\ &\geq \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \right\} \\ &\geq \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \right\} \\ &\geq \{1\} \end{aligned}$$

  [(Lafferty and Rockmore, 1992; Maslen and Rockmore, 2000)]. These FFTs take $O(q^4 \log q)$ time; because $|SL_2(q)| = q^3 - q$, the time taken can alternately be expressed as $O(|SL_2(q)|^{4/3} \log |SL_2(q)|)$.

Now we consider the inclusion $SL_2(q^2) > SL_2(q)$. Applying the FFT as described in this thesis to the inclusion $SL_2(q^2) > SL_2(q)$ involves summing the terms $D(g_i)D(a_i)$, where the a_i are elements of $\mathbb{C}SL_2(q)$ and the g_i range over a complete set of coset representatives for $SL_2(q)$ in $SL_2(q^2)$. In Section 3.2 it is shown that $|SL_2(q)| = q^3 - q$. Thus there are $|SL_2(q^2) : SL_2(q)| = \frac{q^6 - q^2}{q^3 - q} = q^3 + q$ representatives, and each $D(g_i)D(a_i)$ has up to $|SL_2(q^2)| = q^6 - q^2$ entries, and the entire summation process could take up to $O(q^9) = O(|SL_2(q^2)|^{3/2})$ time. This bound is no better than the $O(|G|^{3/2})$ bound for solvable groups given in (Beth, 1987), and strictly worse than the existing $O(q^8 \log q)$ bounds for $SL_2(q^2)$ in particular [(Lafferty and Rockmore, 1992; Maslen and Rockmore, 2000)]. Thus, while the analysis of this thesis may lead to FFTs, they will require adjustments, such as those discussed in Section 4, to be competitive.

Similar analysis shows that applying similar techniques to the inclusion $SL_2(q^k) > SL_2(q)$ will take $O(|SL_2(q^k)|^{\frac{2k-1}{k}})$ time, which is even worse for

larger values of k. Thus the inclusion $SL_2(q^2) > SL_2(q)$ is, for the current discussion, the best case we can study.

Chapter 2

The Affine Group

The task of looking at the special linear group is not a particularly easy one, and it is helpful to look first at an "easier" finite matrix group, the affine group. While Fourier analysis of this group is in general non-analogous to that of the special linear group, there are certain areas—namely in the calculation of its representations and the determination of branching diagrams for certain inclusions—that may serve as a model for the "main" problem of $SL_2(q)$.

2.1 A Word on Finite Fields

In this section we recall some definitions and constructions involving finite fields. For a general overview of finite fields, see Dummit and Foote (2004); for the concepts that are more specific to the particular case of constructing representations of $SL_2(q)$, see, for example, (Tanaka, 1967; A. Zelevinskii, 1974).

Let p be a prime. For any $n \geq 1$ there is a unique field of order p^n, the *finite field of order* p^n, denoted $\mathbb{F}_p$. $\mathbb{F}_p$, is the field $\mathbb{Z}/p\mathbb{Z}$, under the standard arithmetic operations. For arbitrary $n \geq 1$, $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}_p$ of the polynomial $x^{p^n} - x$. That is, $\mathbb{F}_{p^n}$ is the smallest algebraic extension of $\mathbb{F}_p$ containing all the roots of $x^{p^n} - x$; in this case, all the elements of $\mathbb{F}_{p^n}$ are roots; that is, all $x \in \mathbb{F}_{p^n}$ satisfy $x^{p^n} - x$.

$\mathbb{F}_{p^d}$ is (isomorphic to) a subfield of $\mathbb{F}_{p^n}$ if and only if d divides n. If d does divide n, then $\mathbb{F}_{p^d}$ contains $x \in \mathbb{F}_{p^n}$ if and only if $x^{p^d} - x = 0$. In particular, if q is a prime power, then $\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^2}$. In fact, if $\mathbb{F}$ is a quadratic extension of $\mathbb{F}_q$, then $|\mathbb{F}| = q^2$. By the uniqueness of finite fields,

we have $\mathbb{F} = \mathbb{F}_{q^2}$. Thus $\mathbb{F}_{q^2}$ is a quadratic extension of $\mathbb{F}_q$.

The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$. Let α be a generator of $\mathbb{F}_{q^2}^\times$ and let $\gamma = \alpha^{q+1}$. The $q-1$ elements γ^j for $0 \le j < q-1$ are distinct and satisfy

$$\gamma^{jq} - \gamma^j = \alpha^{j\cdot q^2} - \alpha^j = \alpha^{j^{q^2}} - \alpha^j = 0.$$

Then the q roots of the polynomial $x^q - x$ are the γ^j and 0, so they form the finite field $\mathbb{F}_q$. Thus $\mathbb{F}_q$ is a subfield of $\mathbb{F}_q^2$, generated by $\gamma = \alpha^{q+1}$.

In general, arbitrary generators γ for $\mathbb{F}_q$ and α for $\mathbb{F}_{q^2}$ will not necessarily have this relationship. If $q = 2^n$, then $\mathbb{F}_q$ may be constructed by finding a polynomial $h_n(x)$ of degree n that is irreducible over $\mathbb{F}_2$, and adjoining a root γ to $\mathbb{F}_2$. Similarly, $\mathbb{F}_{q^2}$ may be constructed by adjoining a root α of $h_{2n}(x)$ to $\mathbb{F}_2$, where h_{2n} is irreducible of degree $2n$ over $\mathbb{F}_2$. If $h_n(\alpha^{q+1}) \neq 0$, then there is no way that $\alpha^{q+1} = \gamma$; conversely, if $h_n(\alpha^{q+1}) = 0$, then we may consider $\alpha^{q+1} = \gamma$. Thus we need to find polynomials h_n, h_{2n} such that if α is a root of h_{2n} then α^{q+1} is a root of h_n.

If $G = \langle z \rangle$ is cyclic of order n (written multiplicatively), then we define the one-dimensional representation $\chi_{k/n}$ on G by $\chi_{k/n}(z^j) = e^{2\pi ijk/n}$; here k need only be defined up to mod n. In particular, there are representations $\chi_{k/(q-1)}$ on $\mathbb{F}_q^\times$ and $\chi_{k/(q^2-1)}$ on $\mathbb{F}_{q^2}^\times$. That is, if α and γ are generators of $\mathbb{F}_q^\times$ and $\mathbb{F}_{q^2}^\times$, respectively, then $\chi_{k/(q-1)}(\alpha^j) = e^{2\pi ijk/(q-1)}$ and $\chi_{k/(q^2-1)}(\gamma^j) = e^{2\pi ijk/(q^2-1)}$. Because $\mathbb{F}_q^\times \le \mathbb{F}_{q^2}^\times$, we may consider $\chi_{k/(q^2-1)}$ as a character on $\mathbb{F}_q^\times$. In particular, we have

$$\begin{aligned}
\chi_{k/(q^2-1)}(\alpha^j) &= \chi_{k/(q^2-1)}(\gamma^{(q+1)j}) \\
&= e^{2\pi ijk(q+1)/(q^2-1)} \\
&= e^{2\pi ijk/(q-1)} \\
&= \chi_{k/(q-1)}(\alpha^j).
\end{aligned}$$

Thus,

$$\chi_{k/(q^2-1)}|_{\mathbb{F}_q^\times} = \chi_{k/(q-1)}; \tag{2.1}$$

that is, $\chi_{k/(q^2-1)}$ acts like $\chi_{k/(q-1)}$ when restricted to $\mathbb{F}_q^\times$.

2.2 Representations of the Affine Group

Let $\mathrm{Aff}(q)$, the *affine group* over $\mathbb{F}_q$, be the multiplicative group of matrices of the form

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix},$$

where $x \in \mathbb{F}_q^\times$ and $y \in \mathbb{F}_q$. Because x may be any of the $q-1$ elements of $\mathbb{F}_q^\times$, and y may be any of the q elements of $\mathbb{F}_q$, we have $|\mathrm{Aff}(q)| = q(q-1)$.

To describe the irreducible representations on $\mathrm{Aff}(q)$ we define a non-trivial character on the additive group of $\mathbb{F}_q$. Let $q = p^n$. For $x \in \mathbb{F}_q$, define

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}.$$

Because $\mathbb{F}_q$ has characteristic p, we have $(x+y)^p = x^p + y^p$ for $x, y \in \mathbb{F}_q$; using this we can easily show that $\mathrm{Tr}(x)^p = \mathrm{Tr}(x)$ and that $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$. The equation $\mathrm{Tr}(x)^p = \mathrm{Tr}(x)$ is exactly the criterion for $\mathrm{Tr}(x)$ to be an element of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Thus $\mathrm{Tr}(x)$ is an integer modulo p, so the function $\psi(x) = e^{2\pi i \,\mathrm{Tr}(x)/p}$ is well-defined. Since Tr is additive it follows that $\psi(x+y) = \psi(x)\psi(y)$, so ψ is a one-dimensional representation on the additive group of $\mathbb{F}_q$, and thus an irreducible representation.

We construct the irreducible representations on $\mathrm{Aff}(q)$; for a more detailed account, see Terras (1999). There are two classes of such representations:

1. Those inherited from $\mathbb{F}_q^\times$. For each representation $\chi_{k/(q-1)}$ of $\mathbb{F}_q^\times$, we define
$$\chi_{k/(q-1)} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \chi_{k/(q-1)}(x).$$

2. One induced from $\mathbb{F}_q$. The subgroup H of matrices of the form $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$ is isomorphic to the additive group of $\mathbb{F}_q$ under the identification $y \to \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$. Thus $\psi \left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) = \psi(y)$ is a representation of H. We let $\xi = Ind_H^G \psi$, the representation induced from ψ.

The $\chi_{k/(q-1)}$ and ξ are the irreducible representations on $\mathrm{Aff}(q)$

Recall that, by definition of an induced representation, any $\xi(g)$ acts on the vector space W of functions $f : \mathrm{Aff}(q) \to \mathbb{C}$ satisfying $f(hg) = \psi(h)f(g)$ whenever $h \in H$, and this action is given by $[\xi(g)f](x) = f(xg)$. If $g_1, \ldots, g_n$ form a complete set of right coset representatives of H, then any

$f \in W$ is uniquely determined by the values $f(g_1), \ldots, f(g_n)$. The matrices $\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for $x \in \mathbb{F}_q^\times$ are such a set; if we let e_x be the function in W satisfying

$$e_x \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = \begin{cases} 1, & x = y \\ 0, & \text{otherwise,} \end{cases}$$

then $\{e_x | x \in \mathbb{F}_q^\times\}$ forms a basis for W; thus W is $(q-1)$-dimensional and ξ has order $q-1$. We compute the matrix elements of $\xi \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with respect to the e_x; for any $y \in \mathbb{F}_q^\times$, we have

$$\begin{aligned} \left[\xi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} e_x\right] \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} &= e_x \left(\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \right) \\ &= e_x \left(\begin{pmatrix} 1 & by \\ 0 & 1 \end{pmatrix} \begin{pmatrix} ay & 0 \\ 0 & 1 \end{pmatrix} \right) \\ &= \psi \begin{pmatrix} 1 & by \\ 0 & 1 \end{pmatrix} e_x \begin{pmatrix} ay & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{cases} \psi(by), & x = ay \\ 0, & \text{otherwise} \end{cases} \\ &= \begin{cases} cl\psi(a^{-1}bx), & a^{-1}x = y \\ 0, & \text{otherwise} \end{cases} \\ &= \psi(a^{-1}bx) e_{a^{-1}x} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Thus

$$\xi \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} e_x = \psi(a^{-1}bx) e_{a^{-1}x}. \tag{2.2}$$

We may intuitively interpret this result as follows. We determine ξ by letting the matrix $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ act on $\left(\begin{smallmatrix} y & 0 \\ 0 & 1 \end{smallmatrix}\right)$ by right multiplication, sending it to a multiple of the matrix $\left(\begin{smallmatrix} ay & 0 \\ 0 & 1 \end{smallmatrix}\right)$. As is often the case, we may consider transformations of group elements to be the "opposite" transformations of functions *on* those group elements. Thus we send e_{ay} to some multiple of e_y; renaming variables gives us the result that e_x will be sent to some multiple of $e_{a^{-1}x}$.

2.3 Characters of the Affine Group

We calculate the irreducible characters of the affine group directly from the irreducible representations. The $\chi_{k/(q-1)}$ are already one-dimensional

Representative	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}\gamma^j&0\\0&1\end{smallmatrix}\right)$
Size	1	$q-1$	q
$\chi_{k/(q-1)}$	1	1	$e^{2\pi ijk/(q-1)}$
ξ	$q-1$	-1	0

Table 2.1: Character table for Aff(q).

representations, so they are also characters. For ξ, we use Equation 2.2 to calculate the trace. The analysis splits into three cases:

1. $a = 1, b = 0$. Since ξ has degree $(q-1)$, we have
$$Tr\left(\tau\begin{pmatrix}1&0\\0&1\end{pmatrix}\right) = q-1.$$

2. $a = 1, b \neq 0$. $Tr\left(\tau\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\right) = \sum_{x\in\mathbb{F}_q^\times}\psi(bx) = \sum_{x\in\mathbb{F}_q^\times}\psi(x)$, since multiplication by b simply permutes the elements of $\mathbb{F}_q^\times$. Since ψ and the trivial additive character on $\mathbb{F}_q$ are distinct irreducible characters, they are orthogonal, so $\sum_{x\in\mathbb{F}_q}\psi(x) = 0$. Thus $Tr\left(\tau\left(\begin{smallmatrix}1&b\\0&1\end{smallmatrix}\right)\right) = \sum_{x\in\mathbb{F}_q^\times}\psi(x) = -\psi(0) = -1$.

3. $a \neq 1$. In this case $e_x \neq e_{a^{-1}x}$ for any x, so $\tau\left(\begin{smallmatrix}a&b\\0&1\end{smallmatrix}\right)$ has no nonzero diagonal matrix elements. Thus $\mathrm{Tr}\left(\tau\left(\begin{smallmatrix}a&b\\0&1\end{smallmatrix}\right)\right) = 0$.

Combining the traces of ξ with the traces of the $\chi_{k/(q-1)}$, which are already one-dimensional, we get the character table for Aff(q). Here γ is a generator for $\mathbb{F}_q^\times$, and there is one $\left(\begin{smallmatrix}\gamma^j&0\\0&1\end{smallmatrix}\right)$ conjugacy class for each $1 \leq j < q-1$.

2.4 Branching Diagram for Subgroup Inclusion

We consider the restriction of the irreducible representations of Aff(q^2) to Aff(q). Denote by Tr_q, ψ_q, and ξ_q the trace operator on $\mathbb{F}_q$, the associated character on $\mathbb{F}_q$, and the induced representation on Aff(q). Let Tr_{q^2}, ψ_{q^2}, and ξ_{q^2} be analogously defined for $\mathbb{F}_{q^2}$ and Aff(q^2). We define α to be a generator of $\mathbb{F}_{q^2}^\times$ which satisfies $\gamma = \alpha^{q+1}$.

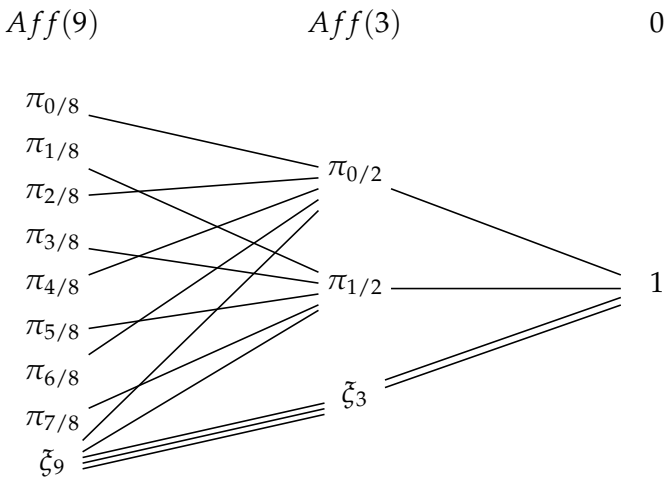


Figure 2.1: Branching diagram for $SL_2(4) > SL_2(2) > 0$.

The character table for $\mathrm{Aff}(q^2)$ is derived from that for $\mathrm{Aff}(q)$, with q replaced by q^2, and with γ replaced by α. Then, when restricted to $\mathrm{Aff}(q)$, $\chi_{k/(q^2-1)}$ simply becomes $\chi_{k/(q-1)}$, as per Equation 2.1. ξ_{q^2} takes the value q^2-1 on the identity, -1 on the conjugacy class generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, and 0 on all other elements. Thus,

$$\begin{aligned}(\xi_{q^2}|_{\mathrm{Aff}(q)}, \xi_q) &= \frac{1}{|\mathrm{Aff}(q)|}\left((q-1)(q^2-1)+(q-1)(-1)(-1)\right)\\ &= \frac{q^2(q-1)}{q(q-1)}\\ &= q,\end{aligned}$$

and

$$\begin{aligned}(\xi_{q^2}|_{\mathrm{Aff}(q)}, \chi_{k/(q-1)}) &= \frac{1}{|\mathrm{Aff}(q)|}\left((q^2-1)+(q-1)(-1)\right)\\ &= \frac{q(q-1)}{q(q-1)}\\ &= 1,\end{aligned}$$

so that ξ_{q^2} restricts to a sum of ξ_q with multiplicity q, and, for each $0 \le k < q-1$, the character $\chi_{k/(q-1)}$. The branching diagram for $\mathrm{Aff}(9) > \mathrm{Aff}(3) > 1$, for example, is given in Figure 2.1.

Chapter 3

The Special Linear Group

Define $SL_2(q)$, the *special linear group* of degree 2 over $\mathbb{F}_q$, to be the multiplicative group of 2×2 matrices with unit determinant whose entries belong to $\mathbb{F}_q$. That is, $SL_2(q)$ contains matrices

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ and $\alpha\delta - \beta\gamma = 1$. $SL_2(q)$ will have different properties depending on whether q is even or odd. We restrict our attention to the case where q is even.

3.1 Characters of the Special Linear Group

A description of the representations and characters is given in A. Zelevinskii (1974). We describe the characters here to determine the branching diagram and examine the representations in greater detail later.

Consider first the set $N = \{x^2 + x | x \in \mathbb{F}_q\}$. N is an additive subgroup of $\mathbb{F}_q$, because $\mathbb{F}_q$ has characteristic 2. N has index 2 in $\mathbb{F}_q$, because for $x \in \mathbb{F}_q$, there are exactly two $x' \in \mathbb{F}_q$ such that $x'^2 + x' = x^2 + x$, namely $x' = x, x+1$; thus $|N| = \frac{q}{2}$.

Any nonzero $y \in N$ can also be expressed in the form $\frac{1}{\tau+\tau^{-1}}$ for $\tau \in \mathbb{F}_q$. In particular, if $y = x^2 + x$, we can set $\tau = 1 + \frac{1}{x}$. Up to reciprocation, τ is unique; that is, if $\frac{1}{\tau_1+\tau_1^{-1}} = \frac{1}{\tau_2+\tau_2^{-1}}$, then $\tau_1 = \tau_2$ or $\tau_1 = \tau_2^{-1}$.

If $y \notin N$, then the polynomial $x^2 + x = y$ has no solution for $x \in \mathbb{F}_q$. However, it has a solution in $\mathbb{F}_{q^2}$. Recall that any quadratic extension of $\mathbb{F}_q$ is $\mathbb{F}_{q^2}$. We explicitly describe the construction of such an extension. Fix $a \notin$

N. Then the polynomial $h(x) = x^2 + x + a$ is irreducible in $\mathbb{F}_q$; otherwise, we have $h(x) = (x - x_1)(x - x_2)$ for some x_1, x_2. Then $h(x_1) = 0$, so $x_1^2 + x_1 = -a = a$, and $a \in N$, contrary to assumption. We thus construct $\mathbb{F}_{q^2}$ by adjoining a root ν of $h(x)$ to $\mathbb{F}_q$.

We will need some more facts about this extension. Define conjugation on $\mathbb{F}_{q^2}$ to be the automorphism $\bar{z} = z^q$. This map fixes $\mathbb{F}_q$ and sends ν to the other root of $h(x)$, namely $\nu + 1$. Thus for $x, y \in \mathbb{F}_q$ we have $\overline{x + y\nu} = x + y(\nu + 1)$. The norm of an element $z \in \mathbb{F}_q$ is $N(z) = z\bar{z} = z^{q+1}$. Define the *unit circle* C in $\mathbb{F}_{q^2}$ to be the set of elements z such that $N(z) = z^{q+1} = 1$. If α is a generator of $\mathbb{F}_{q^2}^\times$ then C contains precisely the elements $\alpha^{j(q-1)}$ for $j = 0, \ldots, q$, so C is a multiplicative subgroup of $\mathbb{F}_{q^2}^\times$ of order $q + 1$ generated by α^{q-1}. In the same way we defined $\chi_{k/(q-1)}$ and $\chi_{k/(q^2-1)}$ on $\mathbb{F}_q^\times$ and $\mathbb{F}_{q^2}^\times$, we define $\chi_{k/(q+1)}$ on C: $\chi_{k/(q+1)}(\alpha^{j(q-1)}) = e^{2\pi ijk/(q+1)}$.

Now let $y \notin N$. Since N has index 2 in $\mathbb{F}_q$, it follows that $y \in N + a$, so $y = x^2 + x + a = (x + \nu)^2 + (x + \nu)$ for some $x \in \mathbb{F}_q$. Then the associated $\tau = 1 + \frac{1}{x+\nu}$. Note that

$$\begin{aligned}
\tau\bar{\tau} &= \left(1 + \frac{1}{x+\nu}\right)\left(1 + \frac{1}{x+\nu+1}\right) \\
&= 1 + \frac{1}{x+\nu} + \frac{1}{x+\nu+1} + \frac{1}{y} \\
&= 1 + \frac{x+\nu+1+x+\nu+1}{y} \\
&= 1,
\end{aligned}$$

so τ is an element of the unit circle C. Conversely, if $1 \neq \tau \in C$, then $\frac{1}{\tau+\tau^{-1}} \in \mathbb{F}_q$.

There are two classes of representations of $SL_2(q)$. Those of the first type are indexed by multiplicative characters χ of $\mathbb{F}_q^\times$, and are denoted by T_χ. Recalling that the characters of $\mathbb{F}_q^\times$ are themselves indexed as $\chi_{k/(q-1)}$, we alternatively denote the corresponding representation by $T_{k/(q-1)}$. Two representations $T_{k/(q-1)}$ and $T_{k'/(q-1)}$ are equivalent if and only if $k = k'$ or $k = -k'$ (here the equalities are properly equivalences modulo $(q-1)$). The representation $T_{0/(q-1)}$ corresponding to the trivial character $\chi_{0/(q-1)}$ on $\mathbb{F}_q^\times$ is the direct sum of two irreducible representations T^0 and 1, where 1 is the trivial character on $SL_2(q)$. If $k \neq 0$, then $T_{k/(q-1)}$ is irreducible.

Representations of the second type are indexed by nontrivial multiplicative characters χ of C, and are denoted by R_χ, or by $R_{k/(q+1)}$ in the case

Representative	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$	$g_\tau, \tau \in \mathbb{F}_q$	$g_\tau, \tau \in C$
Size	1	q^2-1	q^2+q	q^2-q
T_χ	$q+1$	1	$\chi(\tau)+\chi(\tau^{-1})$	0
R_χ	$q-1$	-1	0	$-(\chi(\tau)^2+\chi(\tau^{-1})^2)$
T^0	q	0	q	-1
1	1	1	1	1

Table 3.1: Character table for $SL(q)$.

that $\chi = \chi_{k/(q+1)}$. As with the $T_{k/(q-1)}$, we have that $R_{\chi_{k/(q+1)}}$ and $R_{\chi_{k'/(q+1)}}$ are equivalent iff $k = k'$ or $k = -k'$, and that $R_{k/(q+1)}$ is irreducible. For notational purposes, we define a "representation" $R_{0/(q+1)} = T^0 - 1$; that is, $R_{0/(q+1)} + 1 = T^0$, where again 1 is the trivial representation. This makes sense as long as any representation defined with $R_{0/(q+1)}$ as a direct summand also has 1 as a direct summand, as is the case here.

There are q conjugacy classes of $SL_2(q)$: the identity element, the class of nonidentity g which have trace 0, and, for each nonzero $x \in \mathbb{F}_q$, the class of g with trace x. In the latter case, what we care about is representing x as $\tau + \tau^{-1}$, where $\tau \in \mathbb{F}_q$ or $\tau \in C$, depending on whether $x^{-1} \in N$ or $\notin N$. To this end we set $g_\tau = \left(\begin{smallmatrix}\tau+\tau^{-1}&1\\1&0\end{smallmatrix}\right)$, the representative for the conjugacy class of matrices with trace $\tau + \tau^{-1}$. The character table of $SL_2(q)$ is seen in Table 3.1.

3.2 Branching Diagram for Subgroup Inclusion

The Table 3.1 gives us the character table for $SL_2(q^2)$ if we replace q by q^2, so we can use this to calculate the restrictions of the characters of $SL_2(q^2)$ to $SL_2(q)$. Here, replacing q by q^2 also means that we must now differentiate between those g_τ for which $\tau \in \mathbb{F}_{q^2}$, and those for which $\tau \in C'$, the unit circle in $\mathbb{F}_{q^4}$. However, for $x \in \mathbb{F}_q$ we have $x = \tau + \tau^{-1}$ where $\tau \in \mathbb{F}_q$ or $\tau \in C$. In either case, $\tau \in \mathbb{F}_{q^2}$. Thus if $g_\tau \in SL_2(q)$, we can necessarily say that $\tau \in \mathbb{F}_{q^2}$. Thus the fourth column does not enter into our consideration.

We still need the order of $SL_2(q)$. Define the *general linear group* of degree 2 over $\mathbb{F}_q$, $GL_2(q)$, to be the group of matrices with entries in $\mathbb{F}_q$ and any nonzero determinant. Elements of $GL_2(q)$ are in one-to-one correspondence with ordered bases of $\mathbb{F}_q^2$, since the columns of any nonsingular matrix form an ordered basis, and the elements of any ordered basis form the columns of a nonsingular matrix. We thus need to enumerate these bases.

The first element may be any of the q^2-1 nonzero elements of $\mathbb{F}_q^2$, and the second element any of the q^2-q nonmultiples of the first element. Thus there are $(q^2-q)(q^2-1)$ ordered bases, and so $|GL_2(q)| = (q^2-q)(q^2-1)$. Then the determinant map $GL_2(q) \to \mathbb{F}_q^\times$ has kernel $SL_2(q)$ and image $\mathbb{F}_q^\times$, so $|SL_2(q)| = |GL_2(q)|/|\mathbb{F}_q^\times| = (q^2-q)(q^2-1)/(q-1) = q^3-q$.

We can then compute the restrictions of the $R_{j/(q^2+1)}$ by calculating their inner products with all the characters of $SL_2(q)$. For example, we have

$$\begin{aligned}(R_{j/(q^2+1)}|_{SL_2(q)}, T_{k/(q-1)}) &= \frac{1}{|SL_2(q)|}\left((q+1)(q^2-1)+(-1)(q^2-1)\right)\\ &= \frac{q^3-q}{q^3-q}\\ &= 1,\end{aligned}$$

and so on. Computing all these yields

$$R_{j/(q^2+1)}|_{SL_2(q)} = \sum_{k=1}^{q-2} T_{k/(q-1)} + \sum_{k=1}^{q} R_{k/(q+1)} + T^0.$$

The computation of the restrictions of the T_χ is not as simple, since we must add up factors of the form $\chi(\tau)+\chi(\tau^{-1})$. We will need the following to compute the inner products. Note that as $x = \frac{1}{\tau+\tau^{-1}}$ ranges over all elements of $N\backslash\{0\}$, τ and τ^{-1} range over all elements of $\mathbb{F}_q^\times\backslash\{1\}$. Thus for $k \neq 0$,

$$\begin{aligned}\sum_{\frac{1}{\tau+\tau^{-1}}\in N}\left(\chi_{k/(q-1)}(\tau)+\chi_{k/(q-1)}(\tau^{-1})\right) &= \sum_{1\neq\tau\in\mathbb{F}_q^\times}\chi_{k/(q-1)}(\tau)\\ &= \sum_{j=1}^{q-2} e^{ijk2\pi/(q-1)}\\ &= -1.\end{aligned}$$

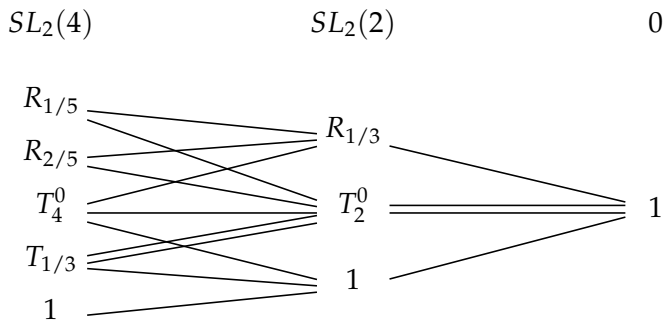


Figure 3.1: Branching diagram for $SL_2(4) > SL_2(2) > 0$.

We can then compute, for example,

$$\begin{aligned}
|SL_2(q)|(T_{j/(q^2-1)}, T_{k/(q-1)}) &= (q+1)(q^2+1) + (q^2-1) \\
&\quad + (q^2+q) \sum_{\frac{1}{\tau+\tau^{-1}} \in N} \left(\chi_{(j+k)/(q-1)}(\tau) + \chi_{(j+k)/(q-1)}(\tau^{-1}) \right) \\
&\quad + (q^2+q) \sum_{\frac{1}{\tau+\tau^{-1}} \in N} \left(\chi_{(j-k)/(q-1)}(\tau) + \chi_{(j-k)/(q-1)}(\tau^{-1}) \right) \\
&= (q+1)(q^2+1) + (q^2-1) - 2(q^2+q) \\
&= q^3 - q \\
&= |SL_2(q)|,
\end{aligned}$$

for $j \neq \pm k$. Calculating all such inner products, we find that

$$T_{j/(q^2-1)}|_{SL_2(q)} = \sum_{k=1}^{q-2} T_{k/(q-1)} + T_{j/(q-1)} + \sum_{\substack{k=0 \\ 2k \neq j}}^{q} R_{k/(q+1)} + 1,$$

and that

$$T^0|_{SL_2(q)} = \sum_{k=1}^{q-2} T_{k/(q-1)} + \sum_{k=1}^{q} R_{k/(q+1)} + T^0 + 1.$$

The branching diagram for $SL_2(4) > SL_2(2) > 0$—that is, the case for $q = 2$—is shown in Figure 3.1. To distunguish them the representation T^0 on $SL_2(4)$ has been called T_4^0, and the representation T^0 on $SL_2(2)$ has been called T_2^0.

3.3 Representations of the Special Linear Group

While the characters are useful in determining the branching diagram for the inclusion $1 \leq SL_2(q) \leq SL_2(q^2)$, we will still need to calculate the actual representations.

Let χ be a character of $\mathbb{F}_q^\times$. Define a function $f : \mathbb{F}_q^\times \backslash \{(0,0)\} \to \mathbb{C}$ to be *χ-homogeneous* if $f(tx_1, tx_2) = \chi(t)f(x_1, x_2)$ for any $t \in \mathbb{F}_q^\times$. Let V_χ be the vector space of χ–homogeneous functions. Then T_χ acts on V_χ in the following way: for any χ–homogeneous function f, $T_\chi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} (f)$ is the function defined by

$$\left[T_\chi \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) (f)\right] (x_1, x_2) = f(\alpha x_1 + \gamma x_2, \beta x_1 + \delta x_2).$$

We define a basis on V_χ so that we may express this action in matrix form. For any χ-homogeneous function f, we have $f(x, 0) = \chi(x)f(1, 0)$, and, for nonzero x_2, $f(x_1, x_2) = \chi(x_2)f(x_1/x_2, 1)$. Thus f is uniquely determined by its action on $(1, 0)$ and $(x, 1)$, for $x \in \mathbb{F}_q$. Define $e_x^{(\chi)}$ to be the χ–homogeneous function such that $e_x^{(\chi)}(x, 1) = 1$, $e_x^{(\chi)}(x', 1) = 0$ for $x \neq x'$, and $e_x^{(\chi)}(1, 0) = 0$. Define $e_\infty^{(\chi)}$ to be the χ-homogeneous function such that $e_\infty^{(\chi)}(x, 1) = 0$ for all $x \in \mathbb{F}_q$ and $e_\infty^{(\chi)}(1, 0) = 1$. We somewhat incorrectly write these as e_x and e_∞ because there is generally no danger of confusion over which χ is involved. Then, because f is uniquely determined by its action on $(1, 0)$ and $(x, 1)$, we have that f is uniquely expressible as a linear combination of the e_x and e_∞, so $\{e_x | x \in \mathbb{F}_q\} \cup \{e_\infty\}$ is a basis for V_χ.

We then compute the action of T_χ on each of these basis elements. For example, we calculate here $T_\chi \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) e_y$ in the case that $\alpha + \beta y \neq 0$ by considering its action separately on each of the $(x, 1)$ for $x \neq \frac{\delta}{\beta}$, on $(\frac{\delta}{\beta}, 1)$, and on $(1, 0)$.

On $(x,1)$ where $x \neq \frac{\delta}{\beta}$,

$$\begin{aligned}\left[T_\chi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} e_y\right](x,1) &= e_y(\alpha x+\gamma, \beta x+\delta) \\ &= \chi(\beta x+\delta) e_y(\frac{\alpha x+\gamma}{\beta x+\delta}, 1) \\ &= \begin{cases} \chi(\beta x+\delta), & \frac{\alpha x+\gamma}{\beta x+\delta} = y \\ 0, & \text{otherwise} \end{cases} \\ &= \begin{cases} \chi\left(\beta \frac{\gamma+\delta y}{\alpha+\beta y}+\delta\right), & x = \frac{\gamma+\delta y}{\alpha+\beta y} \\ 0, & \text{otherwise} \end{cases} \\ &= \chi\left(\frac{(\alpha\delta+\beta\gamma)+(\beta\delta+\beta\delta)y}{\alpha+\beta y}\right) e_{\frac{\gamma+\delta y}{\alpha+\beta y}}(x,1) \\ &= \chi^{-1}(\alpha+\beta y) e_{\frac{\gamma+\delta y}{\alpha+\beta y}}(x,1).\end{aligned}$$

Here χ^{-1} is the character $\chi^{-1}(g) = 1/\chi(g)$.

On $(\frac{\delta}{\beta}, 1)$,

$$\left[T_\chi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} e_y\right]\left(\frac{\delta}{\beta}, 1\right) = e_y\left(\frac{\alpha\delta}{\beta}+\gamma, 0\right) = 0.$$

We show that $\frac{\delta}{\beta} \neq \frac{\gamma+\delta y}{\alpha+\beta y}$; supposing otherwise, we have that

$$\begin{aligned}\frac{\delta}{\beta} &= \frac{\gamma+\delta y}{\alpha+\beta y} \\ \alpha\delta+\beta\delta y &= \beta\gamma+\beta\delta y \\ 0 = \alpha\delta-\beta\gamma &= 1,\end{aligned}$$

a contradiction, so that $\frac{\delta}{\beta} \neq \frac{\gamma+\delta y}{\alpha+\beta y}$, and therefore

$$\begin{aligned}\chi^{-1}(\alpha+\beta y) e_{\frac{\gamma+\delta y}{\alpha+\beta y}}(\frac{\delta}{\beta}, 1) &= 0 \\ &= \left[T_\chi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} e_y\right]\left(\frac{\delta}{\beta}, 1\right)\end{aligned}$$

On $(1,0)$,

$$\begin{aligned}\left[T_\chi \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} e_y\right](1,0) &= e_y(\alpha,\beta) \\ &= \begin{cases} \chi(\beta) e_y(\frac{\alpha}{\beta},1), & \beta \neq 0 \\ \chi(\alpha) e_y(1,0), & \beta = 0 \end{cases} \\ &= 0 \\ &= \chi^{-1}(\alpha+\beta y) e_{\frac{\gamma+\delta y}{\alpha+\beta y}}(1,0).\end{aligned}$$

Thus, $T_\chi \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) e_y = \chi^{-1}(\alpha+\beta y) e_{\frac{\gamma+\delta y}{\alpha+\beta y}}$. These calculations are the rough equivalent of the derivations of Equation 2.2 for the affine group; the intuitive explanation following that equation also roughly applies here. Calculating the action of $T_\chi \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in all cases gives us:

$$\begin{aligned} e_y \mapsto & \chi^{-1}(\alpha+\beta y) e_{\frac{\gamma+\delta y}{\alpha+\beta y}} && \alpha+\beta y \neq 0 \\ & \chi(\beta) e_\infty && \alpha+\beta y = 0 \\ e_\infty \mapsto & \chi^{-1}(\beta) e_{\frac{\delta}{\beta}} && \beta \neq 0 \\ & \chi(\alpha) e_\infty && \beta = 0. \end{aligned} \tag{3.1}$$

The representation T_{χ_0} associated to the trivial representation χ_0 is not irreducible. Let V_{const} be the subspace of V_{χ_0} consisting of constant functions and let V^0 be the subspace generated by the elements $f_y = e_y - e_\infty$ for $y \in \mathbb{F}_q$. These are the invariant subspaces of T_{χ_0}'s action on V_{χ_0}. T_{χ_0} acts as the trivial representation on V_{const} and T^0 on V^0. We can use Equation 3.1 to calculate the action of T^0 on the f_x. For example, if neither $\alpha+\beta x$ nor β are zero, we have

$$T_{\chi_0}(f_y) = T_{\chi_0}(e_y - e_\infty) = e_{\frac{\gamma+\delta y}{\alpha+\beta y}} - e_{\frac{\delta}{\beta}} = f_{\frac{\gamma+\delta y}{\alpha+\beta y}} - f_{\frac{\delta}{\beta}}.$$

Considering all the cases, we have

$$e_y \mapsto \begin{cases} f_{\frac{\gamma+\delta y}{\alpha+\beta y}} - f_{\frac{\delta}{\beta}}, & \alpha+\beta y, \beta \neq 0 \\ -f_{\frac{\delta}{\beta}}, & \alpha+\beta y = 0 \\ f_{\frac{\gamma+\delta y}{\alpha+\beta y}}, & \beta = 0. \end{cases} \tag{3.2}$$

The R_χ action of a generating set of $SL_2(q)$ with respect to a certain basis is given in (A. Zelevinskii, 1974). Namely, for each character χ of C, we let

R_χ act with respect to the basis $\{g_a^{(\chi)} | a \in \mathbb{F}_q^\times\}$; as before we (incorrectly) write only g_a because there is no confusion. In the following, we define the function ψ on $\mathbb{F}_q$ as $\psi(x) = 1$ if $x \in N$ and $\psi(x) = -1$ if $x \notin N$. Then we have

$$R_\chi \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} g_a = \psi(a\gamma) g_a \tag{3.3}$$

$$R_\chi \begin{pmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{pmatrix} g_a = g_{\delta^{-2}a} \tag{3.4}$$

$$R_\chi \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} g_a = \sum_{b \in \mathbb{F}_q^\times} K_\chi(a,b) g_b, \tag{3.5}$$

where $K_\chi(a,b) = -\frac{1}{q} \sum_{\tau \in C} \chi(\tau) \psi(ab(\tau + \tau^{-1}))$. The elements $\left(\begin{smallmatrix} 1 & 0 \\ \gamma & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ generate $SL_2(q)$, by the relations

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{cases} \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \delta\beta & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha/\beta & 1 \end{pmatrix}, & \beta \neq 0 \\ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha\gamma & 1 \end{pmatrix}, & \beta = 0, \end{cases}$$

so Equations 3.3–3.5 suffice to define R_χ on all of $SL_2(q)$.

Chapter 4

Future Work

We have studied the characters and representations of the groups $\mathrm{Aff}(q)$ and $SL_2(2^d)$, and determined the branching diagrams for the inclusions $\mathrm{Aff}(q^2) > \mathrm{Aff}(q)$ and $SL_2(2^{2d}) > SL_2(2^d)$. However, there are a number of directions for future research in this area.

1. While some tools for the study of the characters and representations of $SL_2(2^n)$ have been developed, it still remains to implement and study the efficiency of an FFT as described in this thesis.

2. The matrix groups studied in this thesis are a very specific class of groups. A similar analysis could be performed on others, most immediately the general linear group $GL_2(q)$ and the group $SL_2(q)$ where q is no longer a power of 2 but of an odd prime.

3. As shown in Section 1.3, FFTs resulting from the work of this thesis require further improvement to be competitive. There are several techniques which could be used to speed these FFTs up.

   (a) The structure of the matrices $D(g_i)D(a_i)$ may be relatively sparse, so that each has significantly fewer than $|SL_2(q)|$ nonzero entries. If this could be shown, then adding all the $D(g_i)D(a_i)$ could be sped up.

   (b) The high time it takes to add all the terms $D(g_i)D(a_i)$ arises because there are so many of them, which in turn occurs because $|SL_2(q^2) : SL_2(q)|$ is large. If intermediate subgroups H such that $SL_2(q^2) > H > SL_2(q)$ were studied, the resulting summations would involve fewer terms.

(c) The previous point operates on the idea that we want to cluster the elements of $SL_2(q^2)$ into a partition coarser than the partition into the left cosets of $SL_2(q)$. If we instead look at the double cosets of $SL_2(q)$, these might prove to have some nice structure we can also use to speed up the FFT.

Bibliography

G. Narkunskaya A. Zelevinskii. Representations of the group $SL(2, F_q)$ where $q = 2^n$. *Funktsional'nyi Analiz i Ego Prilozheniya*, 8(3):75–76, 1974. 2.1, 3.1, 3.3

Ulrich Baum. Existence and efficient construction of fast Fourier transforms for supersolvable groups. *Computational Complexity*, 1:235–256, 1991. 1.3

Ulrich Baum and Michael Clausen. *Fast Fourier Transforms*. Wissenschaftsverlag, 1993. 1.1

Ulrich Baum, Michael Clausen, and Benno Tietz. Improved upper complexity bounds for the discrete Fourier transform. *AAECC*, 2:35–43, 1991. 1.3

Thomas Beth. On the computation complexity of the generalized Fourier transform. *Theor. Comp. Sci.*, 51:331–339, 1987. 1.3

David Dummit and Richard Foote. *Abstract Algebra*. John Wiley and Sons, Inc., 2004. 1.1, 1.2, 1.3, 2.1

John Lafferty and Daniel Rockmore. Fast Fourier analysis for SL_2 over a finite field and related numerical experiments. *Experimental Mathematics*, 1:115–139, 1992. 1.3

David Maslen. The efficient computation of Fourier transforms on the symmetric group. *Mathematics of Computation*, 67:1121–1147, 1998. 1.3

David Maslen and Daniel Rockmore. Double coset decompositions and computational harmonic analysis on groups. *Journal of Fourier Analysis and Applications*, 6(4):349–388, 2000. 1.3

Shun'ichi Tanaka. Construction and classification of irreducible representations of special linear group of the second order over a finite field. *Osaka J. Math*, 4:65–84, 1967. 2.1

Audrey Terras. *Fourier Analysis on Finite Groups and Applications*. Cambridge University Press, 1999. 2.2