2014

A New Subgroup Chain for the Finite Affine Group

David Alan Lingenbrink Jr.
Harvey Mudd College

A New Subgroup Chain for the Finite Affine Group

David Lingenbrink

Michael E. Orrison, Advisor

Mohamed Omar, Reader

HARVEY MUDD COLLEGE

Department of Mathematics

May, 2014

Abstract

The finite affine group is a matrix group whose entries come from a finite field. A natural subgroup consists of those matrices whose entries all come from a subfield instead. In this paper, I will introduce intermediate subgroups with entries from both the field and a subfield. I will also examine the representations of these intermediate subgroups as well as the branching diagram for the resulting subgroup chain. This will allow us to create a fast Fourier transform for the group that uses asymptotically fewer operations than the brute force algorithm.

Contents

List of Figures

Acknowledgments

I would like to express my deepest appreciation to my advisor, Prof. Michael Orrison; without his support and kindness, I could never have completed this project. Thanks, too, to my second reader, Prof. Mohamed Omar. Thanks to Emily Fischer and Matt McDermott for reading drafts of my thesis and helping me understand what was unclear. Finally, thanks to my family and friends who have supported me through all my endeavors. I would not be here without them, and I feel incredibly blessed for their love and warmth.

Chapter 1

Background

We will first start with a motivating example. Consider some some finite group, G, and functions f, g that take G to $\mathbb{C}$. We then define the *convolution of f and g* to be the function

$$(f \star g)(x) := \sum_{y \in G} f(y) g(y^{-1}x)$$

for any $x \in G$.

We often define multiplication for spaces of functions via convolutions. Another example is in combinatorics: the product of the generating functions for sequences $\{a_n\}$ and $\{b_n\}$ is the generating function of $\{a_n \star b_n\}$.

A brute force calculation of the convolution is computationally difficult and would involve three steps: the evaluation of $f(y)$ and $g(y^{-1}x)$ for all $y \in G$, the multiplications of the form $f(y)g(y^{-1}x)$, and then the summation of all these summands. This would mean $2|G|$ total evaluations of f and g, $|G|$ multiplications and $|G| - 1$ summations of the terms in the sum. However, the discrete Fourier transform (or DFT) is an isomorphism that modifies the functions f and g to make convolutions (and the multiplication of very large integers (Emerencia, 2007)) much easier to compute. The DFT is an isomorphism between functions over G to the direct sum of rings of complex matrices. So, if f is a function from $G \to \mathbb{C}$, the DFT of f, or $D(f)$, is an element of $\bigoplus_{i=1}^{n} \mathbb{C}^{d_i \times d_i}$ where d_i is an integer for each i.

When we evaluate the DFT of a convolution, we get

$$D(f \star g)(x) = D(f)D(g).$$

The DFT turns a convolution into a matrix multiplication! Since the convolution is normally very inefficient to calculate, it seems like a more efficient approach to evaluating a convolution could utilize the DFT.

In systems engineering, it is common to compute the DFT of the finite cyclic group $\mathbb{Z}/n\mathbb{Z}$. Like the convolution in the example above, the discrete Fourier transform allows for computations that are difficult in the "untransformed" setting to become easy once they are "transformed." So, sometimes it is much faster to transform a computation using the DFT, compute the easier version in the transformed space, and then transform back using the inverse DFT. In the example above, it is often much more efficient to transform f and g using the DFT, compute their product, and then invert the transformation than simply evaluating $f \star g$ by brute force.

It remains unclear how long the DFT (and the inverse DFT) take to compute? The answer depends on the group, but a brute force algorithm exists for all finite groups that runs in $O(|G|^2)$ (Terras, 1999). Any algorithm that applies the discrete Fourier transform to a group G in asymptotically faster time than this is called a fast Fourier transform, or FFT for G. Let $q = p^{2^n}$ for some prime p. $\mathrm{Aff}(q)$ is a finite matrix group over a finite field. Finding a FFT for $\mathrm{Aff}(q)$ is the motivation for this thesis.

The Cooley-Tukey algorithm is a fast Fourier transform that relies on a subgroup chain (Terras, 1999). The goal of this thesis is to construct a subgroup chain for the finite affine group, $\mathrm{Aff}(q)$, that relies on field extensions and makes the Cooley-Tukey algorithm efficient. Since the group $\mathrm{Aff}(q)$ is a subgroup of $\mathrm{Aff}(q^2)$, one chain to consider is $\mathrm{Aff}(p) < \mathrm{Aff}(p^2) < \cdots < \mathrm{Aff}(q) < \mathrm{Aff}(q^2)$. In Chapter 2, we will examine this subgroup chain and its associated FFT. The discrete Fourier transform is the direct sum of a group's "irreducible" representations, so our first task is to understand the irreducible representations of $\mathrm{Aff}(q)$.

In Chapter 3, we will examine another subgroup chain. This chain involves a group, $\mathrm{Aff}(q, q^2)$, that is both a subgroup of $\mathrm{Aff}(q^2)$ and a supergroup of $\mathrm{Aff}(q)$. We will analyze this group, and examine its irreducible representations. The FFT for this subgroup chain is asymptotically better than the brute force algorithm. Finally, Chapter 4 touches on remaining questions from this research.

1.1 A Review of Representation Theory

We will start with a brief overview of representation theory before we dive into the discrete Fourier transform. For any group G, we define a *representation* of G to be a group homomorphism $\rho : G \to GL(V)$ for some vector space V. So, it is a map from G to $GL(V)$ such that $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for all $g_1, g_2 \in G$. We call the dimension of V the *dimension* of our representation, ρ. For the most part, we let $V = \mathbb{C}^n$, but it depends on the representation.

1.1.1 Equivalent definitions for representations

For a group G, we define the *group ring* of G over $\mathbb{C}$ to be the ring

$$\mathbb{C}G := \left\{ \sum_{g \in G} a_g g \,\middle|\, a_g \in \mathbb{C} \right\}$$

where if $a = \sum_{g \in G} a_g g \in \mathbb{C}G$ and $b = \sum_{g \in G} b_g g \in \mathbb{C}G$, we define

$$a + b := \sum_{g \in G} (a_g + b_g) g$$

and

$$ab := \sum_{g,h \in G} (a_g b_h) gh.$$

An equivalent definition of a group ring is

$$\mathbb{C}G := \{f : G \to \mathbb{C}\},$$

since each $x = \sum_{g \in G} a_g g \in \mathbb{C}G$ (from our original definition) can be seen as a function, f, from $G \to \mathbb{C}$ by setting $f(g) = a_g$.

For any representation, $\rho : G \to GL(\mathbb{C}^n)$, we can extend the representation to the homomorphism $\tilde{\rho} : \mathbb{C}G \to \mathbb{C}^{n \times n}$ (where $\mathbb{C}^{n \times n}$ is the ring of all complex $n \times n$ matrices) where

$$\tilde{\rho}\left(\sum_{g \in G} \alpha_g g \right) := \sum_{g \in G} \alpha_g \rho(g).$$

This allows us to discuss representations in two ways: as homomorphisms between G and $GL(\mathbb{C}^n)$ and as homomorphisms between the group ring $\mathbb{C}G$ and $\mathbb{C}^{n \times n}$. Depending on the context, both definitions are used.

1.1.2 Tools from Representation Theory

The theorems behind the material presented in this section can be found in Dummit and Foote (2004).

Consider representations ρ (with associated vector space V) and ρ' (with associated vector space V'). We say ρ and ρ' are *equivalent* if there exists a linear transformation $T : V \to V'$ such that $T\rho(g) = \rho'(g)T$ for all $g \in G$. Notice that if ρ is 1-dimensional, it will only be equivalent to itself, since $T\rho(g)T^{-1} = \rho(g)$ for all T, since T is a scalar and multiplication is commutative for scalars. The group $\mathbb{Z}/2\mathbb{Z}$ has representations ρ_1 and ρ_2 that both send $0 \in \mathbb{Z}/2\mathbb{Z}$ to $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and send $1 \in \mathbb{Z}/2\mathbb{Z}$ to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, respectively. We say that ρ_1 and ρ_2 are equivalent because, for all $g \in \mathbb{Z}/2\mathbb{Z}$,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rho_1(g) = \rho_2(g) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1}.$$

A representation is called *reducible* if it has a non-trivial invariant subspace: there exists a subspace $U \subset V$ where $U \neq \{0\}$ and $U \neq V$ such that $\rho(g)u \in U$ for all $u \in U$. In the above, ρ_1 and ρ_2 are reducible because $U_1 = \left\langle \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\rangle$ and $U_2 = \left\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle$ are invariant subspaces for both ρ_1 and ρ_2. If a representation is not reducible, we say it is *irreducible*. In general, there are a finite number of irreducible representations of a group, up to isomorphism.

One of the most important tools from representation theory is character theory. Given a representation ρ of G, we define its *character* to be a function from G to $\mathbb{C}$ defined by

$$\chi(g) := \mathrm{Tr}(\rho(g))$$

for each $g \in G$. Let χ_1 be the character of ρ_1 and χ_2 the character of ρ_2. We see that $\chi_1(0) = \chi_2(0) = 2$, and $\chi_1(1) = \chi_2(1) = 0$.

An important result of representation theory states that two representations ρ, ρ' have the same character if and only if they are equivalent.

In addition, we can define an inner product for characters: for some group G and characters $\chi : G \to \mathbb{C}$ and $\psi : G \to \mathbb{C}$, define the *inner product* of χ and ψ to be

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

The inner product allows for some very efficient calculation: χ is the character of an irreducible representation if and only if $\langle \chi, \chi \rangle = 1$. If χ and ψ are characters of irreducible representations ρ and γ, respectively, and $\chi \neq \psi$, then $\langle \chi, \psi \rangle = 0$ and χ and ψ are called *orthogonal*. However, if $\chi = \psi$, then ρ and γ are equivalent representations.

Any finite group G will have an equal number of irreducible representations and conjugacy classes. So, suppose G has irreducible representations $\rho_1, \ldots \rho_N$. Then, it must have N distinct conjugacy classes. If the representations' dimensions are $d_1, \ldots d_N$, respectively, we will have $|G| = \sum_{i=1}^{N} d_i^2$.

Maschke's theorem states that every representation of a group, G, is equivalent to a direct sum of irreducible representations of G. This allows us to decompose representations into their irreducible parts. By doing so, we can narrow our sights to the calculation of irreducible representations, since all other representations are just direct sums of the irreducible ones. So, if we know some representation σ of G is equal to $\bigoplus_i \rho_i$ for irreducible representations ρ_i, for any $g \in G$, we can calculate $\sigma(g)$ just by taking the direct sum of the $\rho_i(g)$'s.

1.1.3 Induced Representations

A common method for creating a representation of a group is to "induce" a representation from a subgroup. Assume we have groups H and G where $H \leq G$ and the index, $|G : H|$, is s. Let H have a representation, ρ.

Let $\{g_1, \ldots, g_s\}$ be a complete set of left coset representatives of H in G. Consider also any $g \in G$ and coset representative g_i. By the definition of our coset reps, $gg_i = g_j h$ for exactly one coset representative g_j and $h \in H$. Next, assume $g_j^{-1} g g_i \in H$. This implies there is an $h \in H$ such that $g_j^{-1} g g_i = h$, or equivalently, $gg_i = g_j h$. By the above, there is precisely one g_j and h such that the $gg_i = g_j h$. So, $g_j^{-1} g g_i \in H$ for precisely one j.

We will first expand the definition of ρ. Let $\rho'(h) = \rho(h)$ for all $h \in H$ and $\rho'(g) = 0$ for all $g \notin H$. Then, we define the *induced representation* $\rho \uparrow G$ to be

$$\rho \uparrow G(g) := \begin{pmatrix} \rho'(g_1^{-1} g g_1) & \rho'(g_1^{-1} g g_2) & \cdots & \rho'(g_1^{-1} g g_s) \\ \rho'(g_2^{-1} g g_1) & \rho'(g_2^{-1} g g_2) & \cdots & \rho'(g_2^{-1} g g_s) \\ \vdots & \vdots & \ddots & \vdots \\ \rho'(g_s^{-1} g g_1) & \rho'(g_s^{-1} g g_2) & \cdots & \rho'(g_s^{-1} g g_s) \end{pmatrix}.$$

Note that, clearly, any representation of G can be *restricted* to a representation of H. Let ρ be a representation of G with associated vector space V. We denote $\rho \downarrow H$ to be the *restriction of* ρ *into* H. We define $\rho \downarrow H(h) = \rho(h)$ for all $h \in H$, so $\rho \downarrow H : H \to GL(V)$. We know $\rho \downarrow H$ will satisfy $\rho \downarrow H(h_1 h_2) = \rho \downarrow H(h_1) \rho \downarrow H(h_2)$ for $h_1, h_2 \in H$, and thus $\rho \downarrow H$ is a valid representation of H.

1.2 Finite Fields

Our work will primarily deal with a specific matrix group over finite fields. Because of this, understanding the basics of finite field theory will help us understand this group.

For any prime p and $n \geq 1$, there is exactly one field (up to isomorphism) of order p^n (Garling, 1986). We denote this field $\mathbb{F}_{p^n}$. Although $\mathbb{F}_p$ is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{F}_{p^n}$ for $n > 1$ is generally more complicated. In fact, $\mathbb{F}_{p^n}$ is the splitting field over $\mathbb{F}$ 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 $x^{p^n} - x = 0$. Put another way, $\mathbb{F}_{p^n}$ can be viewed as $\mathbb{F}_p[x]/(f)$, where we take the polynomials with coefficients in $\mathbb{F}_p$ and mod out by an irreducible degree n polynomial, f.

Consider any $k \in \mathbb{Z}$. If G is a multiplicative cyclic group of order n with generator z, we can define the representation $\chi_{k/n}$ on G by

$$\chi_{k/n}(z^j) = e^{2\pi ijk/n}.$$

Notice this only needs to be defined up to mod n, since

$$\chi_{k/n}(z^j) = e^{2\pi ijk/n} = e^{2\pi ijk/n}e^{2\pi ij} = e^{2\pi ij(k+n)/n} = \chi_{(k+n)/n}(z^j).$$

So, this gives us n distinct irreducible one-dimensional representations of G.

The multiplicative group of a finite field (which we denote $\mathbb{F}_q^\times$) is cyclic. So, $\mathbb{F}_q^\times$ is cyclic and has $q-1$ elements. Once we find a generator of this cyclic group, we have $q-1$ one-dimensional representations of $\mathbb{F}_q^\times$ of the form $\chi_{k/q-1}$ as demonstrated above.

By Garling (1986), $\mathbb{F}_{p^a}$ is a subfield of the field F if and only if $F = \mathbb{F}_{p^{ab}}$ for some $b \in \mathbb{Z}$.

1.3 Discrete Fourier Transform

By Wedderburn's theorem (see page 36 of Clausen and Baum (1993)), for any finite group G, $\mathbb{C}G$ is isomorphic to the direct sum of matrix algebras, $\oplus_i \mathbb{C}^{d_i \times d_i}$, with the isomorphism given by the direct sum of a complete set of pairwise-inequivalent irreducible representations of G. This isomorphism is called the *discrete Fourier transform*, or *DFT*, of G.

Let D denote the DFT of G. Since D is an isomorphism and $\mathbb{C}G$ is a $|G|$-dimensional complex vector space, so is $\oplus_i \mathbb{C}^{d_i \times d_i}$. Since each $\mathbb{C}^{d_i \times d_i}$ has dimension d_i^2, we must have $\sum d_i^2 = |G|$. So, for any element $g \in G$, $D(g)$ has at most $|G|$ non-zero entries.

Consider any $a \in \mathbb{C}G$. We can write $a = \sum_{g \in G} a_g g$, for $a_g \in \mathbb{C}$. If we want to calculate $D(a)$, we could simply compute

$$D(a) = D\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} D(a_g g) = \sum_{g \in G} a_g D(g).$$

First, let us examine how long this calculation takes to evaluate through brute force. We see that evaluating each $D(g)$ would take $O(|G|)$ operations per g. Then, we would scale each $D(g)$ to get the summands $a_g D(g)$, which would take $O(|G|)$ operations per g. Since there are $|G|$ g's, we would have already preformed $O(|G|^2)$ operations. Then, we would have to sum each of the $a_g D(g)$'s which would take $O(|G|)$ operations per binary sum and since there are $|G|$ terms to sum, this brings our total run time to $O(|G|^2)$. Any algorithm that takes asymptotically fewer operations than $O(|G|^2)$ is called a *fast Fourier transform*, or *FFT*.

One common approach to creating an FFT is to utilize a subgroup. Imagine we have a group G where we want to calculate the DFT. Also suppose we have a subgroup $H < G$. Let $g_1, \dots g_s$ be a complete set of the left coset representatives of H. In other words, G is the disjoint union $G = \bigcup_{i=1}^{s} g_i H$. We can write

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

where $a_i = \sum_{h \in H} a_{g_i h} h \in \mathbb{C}H$. This could allow us to speed up the calculation of the discrete Fourier transform of a, $D(a)$. Since D is a ring isomorphism,

$$D(a) = D\left(\sum_{i=1}^{s} g_i a_i\right) = \sum_{i=1}^{s} D(g_i a_i) = \sum_{i=1}^{s} D(g_i) D(a_i).$$

We could precompute $D(g_i)$, since this part of the calculation will be identical no matter what the a is. So, unless we are calculating the DFT for very few a's, we don't need to include the computation of $D(g_i)$ in our calculation. Also, it only adds $s\ O(|G|)$ operations.

In addition, we will need to evaluate D on $s = |G : H|$ elements of $\mathbb{C}H$ (the $D(a_i)$'s). Then, once we have computed these, we perform the s multiplications $D(g_i)D(a_i)$ and the $s - 1$ additions in $\sum D(g_i)D(a_i)$.

Immediately, this does not seem to necessarily be an improvement in running time. However, if our DFT has a nice structure, it can be very beneficial. For example, if we could choose the g_i so that $D(g_i)$ were sparse, our s multiplications of the form $D(g_i)D(a_i)$ would be very quick. Similarly, if $D(g_i)$ was a product of sparse matrices, we might see a decrease in running time.

By Maschke's theorem, $D \downarrow H$ is equivalent to a direct sum of irreducible representations of H. Imagine we select D so that $D \downarrow H$ is in fact equal to this direct sum, and all equivalent direct summands are themselves equal. If we do this, then $D(a_i)$ reduces to evaluating $\rho(a_i)$ for several different irreducible representations ρ of H. By Frobenius Reciprocity (Dummit and Foote, 2004), we know that any irreducible representation of H occurs in at least one irreducible representation of G, and thus a direct summand of D. Thus, evaluating the DFT of G is equivalent to calculating $\rho(a_i)$ for all irreducible representations ρ of H.

1.3.1 Branching Diagrams

My project is not to construct branching diagrams (Spaide, 2009), but they are very useful at communicating subgroup and representation structure.

Let G be a group and $H < G$ a subgroup of G. Let $\rho_1, \ldots, \rho_p$ and $\sigma_1, \ldots, \sigma_s$ be a complete set of inequivalent irreducible representations of G and H, respectively. Let s_i be the dimension of representation σ_i and p_i be the dimension of representation ρ_i. By Maschke's theorem, $\rho_i \downarrow H = \oplus_{j=1}^{s} a_j \sigma_j$, where each a_j is a nonnegative integer, and $p_i = \sum_{j=1}^{s} a_j s_i$. This holds for each ρ_i, and a *branching diagram* is a common way of presenting this information. A branching diagram is a multigraph whose vertices correspond to the irreducible representations of G and H. If $\rho_i \downarrow H = \oplus_{j=1}^{s} a_j \sigma_j$, there is an edge of multiplicity a_j between the vertex ρ_i and σ_j for each j.

We can extend branching diagrams to handling subgroup chains $G_1 > G_2 > \ldots > G_n$ where we draw edges between adjacent groups as we did above. See Figure 1.1 for an example of a branching diagram; below is the derivation.

For an example, consider the subgroup chain $\mathbb{Z}/4\mathbb{Z} > 2\mathbb{Z}/4\mathbb{Z} > 4\mathbb{Z}/4\mathbb{Z}$. The elements of $\mathbb{Z}/4\mathbb{Z}$ are $\{0, 1, 2, 3\}$, with addition modulo 4 as the group operation. The elements of $2\mathbb{Z}/4\mathbb{Z}$ are $\{0, 2\}$ with addition modulo 4. Then, finally, we will let $4\mathbb{Z}/4\mathbb{Z}$ has elements $\{0\}$. In this way, the subgroup structure $4\mathbb{Z}/4\mathbb{Z} < 2\mathbb{Z}/4\mathbb{Z} < \mathbb{Z}/4\mathbb{Z}$ is clear.

Each of those groups is cyclic, so we already know some of their one-dimensional irreducible representations. $\mathbb{Z}/4\mathbb{Z}$ has four irreducible inequivalent one-dimensional representations of the form (for $0 \leq k < 4$)

$$\chi_{k/4}(x) = e^{2\pi ixk/4}.$$

By the same logic as above, $2\mathbb{Z}/4\mathbb{Z}$ has two irreducible inequivalent one-dimensional representations of the form (for $0 \leq k < 2$)

$$\chi_{k/2}(x) = e^{2\pi ixk/4}$$

and $4\mathbb{Z}/4\mathbb{Z}$ has one irreducible inequivalent one-dimensional representations of the form

$$\chi_{0/1}(x) = e^{2\pi ix0/1} = 1.$$

We can see that these are *a complete set of inequivalent irreducible representations* for $\mathbb{Z}/4\mathbb{Z}$ since we found four inequivalent irreducible one-dimensional representations, and the sum of the squared dimensions for these representations is 4, which is the order of the group. Thus, there are no more irreducible representations to find. The same argument holds for $2\mathbb{Z}/4\mathbb{Z}$ and $4\mathbb{Z}/4\mathbb{Z}$.

We see that $\chi_{k/4}(2) = -1$ if $k = 1$ or $k = 3$, and $\chi_{k/4}(2) = 1$ otherwise. Thus,

$$\chi_{1/4} \downarrow 2\mathbb{Z}/4\mathbb{Z} = \chi_{3/4} \downarrow 2\mathbb{Z}/4\mathbb{Z} = \chi_{1/2}$$

and

$$\chi_{0/4} \downarrow 2\mathbb{Z}/4\mathbb{Z} = \chi_{2/4} \downarrow 2\mathbb{Z}/4\mathbb{Z} = \chi_{0/2}.$$

Then, both $\chi_{0/2}$ and $\chi_{1/2}$ is equal to $\chi_{0/1}$ when restricted to $\mathbb{Z}/1\mathbb{Z}$ since $4\mathbb{Z}/4\mathbb{Z}$ only contains the identity which is always sent to the identity by representations. This gives us the edges of our branching diagram. The branching diagram is presented in Figure 1.

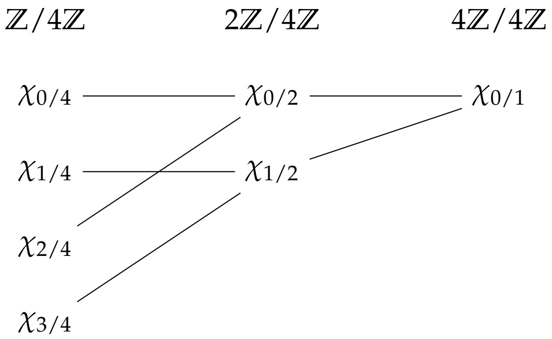

Figure 1.1 Branching Diagram for $\mathbb{Z}/4\mathbb{Z} > 2\mathbb{Z}/4\mathbb{Z} > 4\mathbb{Z}/4\mathbb{Z}$

Chapter 2

The Affine Group

We define $\text{Aff}(q)$ to be the *finite affine group* over $\mathbb{F}_q$ as follows:

$$\text{Aff}(q) := \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \middle| \, x, y \in \mathbb{F}_q, x \neq 0 \right\}$$

with matrix multiplication as the group operation.

For convenience, in the element $A = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \text{Aff}(q)$, we call x the *diagonal entry* of A and y the *non-diagonal entry* of A.

We can see that $\text{Aff}(q)$ is, in fact, a group by the following. First, since it is a subset of the general linear group, $GL_2(\mathbb{F}_q)$, all we need to show is that it is closed under multiplication and that inverses exist in $\text{Aff}(q)$. So, if $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in \text{Aff}(q)$, then

$$AB = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}.$$

Since a and c are non-zero, ac is nonzero. So, $AB \in \text{Aff}(q)$, and $\text{Aff}(q)$ is closed under the group operation.

Next, we must show that inverses exist in $\text{Aff}(q)$. Let $A' = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}$. Since $a \neq 0$, $a^{-1} \neq 0$, so $A' \in \text{Aff}(q)$. Next, notice

$$AA' = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b - b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

where I is the identity of $\text{Aff}(q)$. Thus, $A' = A^{-1}$, the inverse of A, and inverses exist in $\text{Aff}(q)$. $\text{Aff}(q)$ is a subgroup of $GL_2(\mathbb{F}_q)$.

2.1 A natural subgroup chain for Aff(q)

The order of $|\mathrm{Aff}(q)|$ is fairly easy to calculate. There are $(q-1)$ possible diagonal entries (since it is in $\mathbb{F}_q$, and is non-zero) and q possible non-diagonal entries (since it can be any element of $\mathbb{F}_q$, including zero). So, $|\mathrm{Aff}(q)| = (q-1)q$.

Consider any $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ and nonnegative integer m (we denote this $m \in \mathbb{Z}_{\geq 0}$). By Garling (1986), $\mathbb{F}_q \leq \mathbb{F}_{q^m}$. So, since $a, b \in \mathbb{F}_q \leq \mathbb{F}_{q^m}$, $a, b \in \mathbb{F}_{q^m}$ and $A \in \mathrm{Aff}(q^m)$. Thus, $\mathrm{Aff}(q) \leq \mathrm{Aff}(q^m)$. Thus, since $q = p^n$, $\mathrm{Aff}(p^n) \leq \mathrm{Aff}(p^{nm})$.

This gives us a very natural subgroup chain. For any non-zero integers $a, b, c, \ldots$,

$$\mathrm{Aff}(p^a) \leq \mathrm{Aff}(p^{ab}) \leq \mathrm{Aff}(p^{abc}) \leq \cdots .$$

So, in particular, for the group $\mathrm{Aff}(p^{2^n})$, we have the subgroup chain

$$\mathrm{Aff}(p) \leq \mathrm{Aff}(p^2) \leq \cdots \leq \mathrm{Aff}(p^{2^{n-1}}) \leq \mathrm{Aff}(p^{2^n}).$$

2.2 The conjugacy classes of Aff(q)

Recall that the number of representations of Aff(q) is equal to the number of conjugacy classes of Aff(q). We will first find the conjugacy classes of this group, so we will know how many irreducible representations to look for. Consider any $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q)$. We recall that A is precisely conjugate to the elements of Aff(q) of the form BAB^{-1}, where $B \in \mathrm{Aff}(q)$. So, for $B = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$,

$$BAB^{-1} = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c^{-1} & -c^{-1}d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & cb + d(1-a) \\ 0 & 1 \end{pmatrix}.$$

From the definition of conjugacy, we see that the identity is in its own conjugacy class (it is only conjugate to itself). Next, if we let $a = 1$ and $b \neq 0$, the matrix is conjugate to matrices of the form

$$\begin{pmatrix} 1 & cb \\ 0 & 1 \end{pmatrix}$$

where $c \neq 0$. Since $b \neq 0$, we can choose $c = b^{-1}e$ for any nonzero $e \in \mathbb{F}_q$ so that $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ is conjugate to $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$. Thus, this conjugacy class contains $q-1$ elements: all the elements of $\mathrm{Aff}(q)$ with diagonal entry 1 and nonzero non-diagonal entry.

Next, the matrix $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $a \neq 1$ is conjugate to matrices of the form

$$\begin{pmatrix} a & d(1-a) \\ 0 & 1 \end{pmatrix}$$

where $d \in \mathbb{F}_q$. Since $(1-a) \neq 0$, we can choose $d = (1-a)^{-1}e$ where $e \in \mathbb{F}_q$. So, $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is conjugate to all elements of the form $\begin{pmatrix} a & e \\ 0 & 1 \end{pmatrix}$. This gives us $q-2$ more conjugacy classes, since there are $q-2$ nonzero and non-one choices for a. This has exhausted all the conjugacy classes of $\mathrm{Aff}(q)$.

In total, there are $1 + 1 + (q-2) = q$ conjugacy classes for $\mathrm{Aff}(q)$.

2.3 The representations of Aff(q)

As we noted in 1.2, the group $\mathbb{F}_q^\times$ comes with a few convenient multiplicative representations. Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$, there exist $q-1$ one-dimensional representations

$$\chi_{k/(q-1)}(\gamma^j) := e^{2\pi i k j/(q-1)}.$$

This allows us to define several of the irreducible representations of $\mathrm{Aff}(q)$ easily. Let $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q)$. Since $a \neq 0$, we can write $a = \gamma^j$ for some $j \in \mathbb{Z}_{\geq 0}$. So, $A = \begin{pmatrix} \gamma^j & b \\ 0 & 1 \end{pmatrix}$. We can define

$$\chi_{k/(q-1)}\left(\begin{pmatrix} \gamma^j & b \\ 0 & 1 \end{pmatrix}\right) := \chi_{k/(q-1)}(\gamma^j).$$

This defines $q-1$ distinct irreducible one-dimensional representations of $\mathrm{Aff}(q)$. Since there are q irreducible representations in total, this means there is one more representation to find.

If a group G has n irreducible representations and d_i is the dimension of the ith representation, then $\sum_{i=1}^n d_i^2 = |G|$. Thus, in our case,

$$q(q-1) = \sum_{i=1}^{q} d_i^2.$$

The first $q-1$ representations are all one-dimensional, so

$$q(q-1) = \sum_{i=1}^{q} d_i^2 = (q-1)1 + d_q^2.$$

This implies $d_q^2 = (q-1)^2$, and the last representation has dimension $q-1$. The representations we just found only used the diagonal entry of the elements of $\mathrm{Aff}(q)$. Our next representation will also use the non-diagonal entry.

Define

$$\mathrm{Tr}(x) := x + x^{p^1} + \ldots + x^{p^{n-1}}$$

for $x \in \mathbb{F}_q$. Since $\mathbb{F}_q$ can be seen as elements of $\mathbb{F}_p[x]$ modulo some irreducible polynomial of degree n, $\mathbb{F}_q$ has characteristic p ($p1 = 1+1+\ldots+1 = 0$) (Garling, 1986). Since $\mathbb{F}_q$ has characteristic p, we have, by the binomial theorem,

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}.$$

The only i such that p does not divide $\binom{p}{i}$ are $i=0$ and $i=p$. Thus,

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

since all the other terms are divisible by p, and $p=0$ in $\mathbb{F}_q$.

Because of this, we see that

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

We can recursively apply this to get

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

If $x=0$, $\mathrm{Tr}(x) = 0 = \mathrm{Tr}(x)^p$. Otherwise, $x \in \mathbb{F}_q^\times$, which is a multiplicative group of order $p^n - 1$. So, $x^{p^n-1} = 1$, and $x^{p^n} = x$. So,

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

Similarly,

$$\begin{aligned}\mathrm{Tr}(x+y) &= (x+y) + \cdots + (x+y)^{p^{n-1}} = y + \cdots + y^{p^{n-1}} + x + \cdots + x^{p^{n-1}} \\ &= \mathrm{Tr}(x) + \mathrm{Tr}(y).\end{aligned}$$

A theorem from Galois theory (see Garling (1986)) says that the Frobenius monomorphism $\psi(a) = a^p$, where p is the characteristic, only fixes the elements that are in the *prime field*, or the elements that are equal to integer multiples of the identity. In fact, ψ generates the automorphism group of $\mathbb{F}_q$. In our case, the prime field is simply $\mathbb{F}_p$. So, $\mathrm{Tr}(x)^p = \mathrm{Tr}(x)$ implies that $\mathrm{Tr}(x) \in \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Thus, $\mathrm{Tr}(x)$ can be viewed as an integer modulo p, and $\phi(x) := e^{2\pi i \mathrm{Tr}(x)/p}$ is well-defined. Since $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$, we see that $\phi(x+y) = \phi(x)\phi(y)$. So, ϕ is a one-dimensional representation of the additive group of $\mathbb{F}_q$.

Let

$$H := \left\{ \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} | y \in \mathbb{F}_q \right\}.$$

We see that H is a group and that $H \leq \mathrm{Aff}(q)$. We can define a representation, ϕ, of H by

$$\phi\left(\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}\right) := \phi(y).$$

We can then induce this representation to our group $\mathrm{Aff}(q)$. We see that

$$\left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \right\}_{x \in \mathbb{F}_q^\times}$$

is a complete set of left coset representatives of H in $\mathrm{Aff}(q)$. Call these representatives $g_1, \ldots, g_{q-1}$. So, we let our representation ρ to be

$$\rho(g) := \phi \uparrow \mathrm{Aff}(q)(g) = \begin{pmatrix} \rho(g_1^{-1}gg_1) & \rho(g_1^{-1}gg_2) & \cdots & \rho(g_1^{-1}gg_{q-1}) \\ \rho(g_2^{-1}gg_1) & \rho(g_2^{-1}gg_2) & \cdots & \rho(g_2^{-1}gg_{q-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \rho(g_{q-1}^{-1}gg_1) & \rho(g_{q-1}^{-1}gg_2) & \cdots & \rho(g_{q-1}^{-1}gg_{q-1}) \end{pmatrix}.$$

By Spaide (2009), this representation is irreducible. Figure 2.1 shows the branching diagram for $\mathrm{Aff}(3^2) > \mathrm{Aff}(3) > \{1\}$.

2.4 Cooley-Tukey Algorithm

To calculate the DFT of some $a \in \mathbb{C}\mathrm{Aff}(q^2)$, we will use the Cooley-Tukey algorithm described in the introduction. Recall we will use a subgroup chain for this algorithm; in this case we will use $\mathrm{Aff}(q^2) \geq \mathrm{Aff}(q) \geq \ldots$. If $a = \sum_{g \in \mathrm{Aff}(q^2)} a_g g$ (where each $a_g \in \mathbb{C}$), then

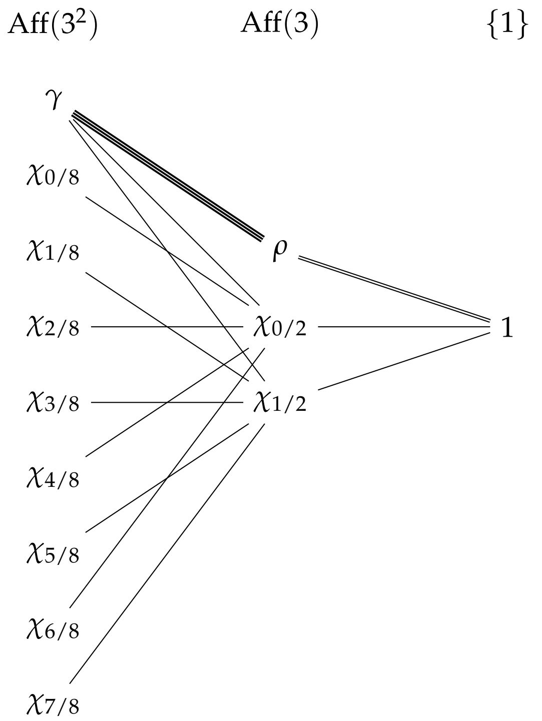

Figure 2.1 Branching Diagram for $\mathrm{Aff}(3^2) > \mathrm{Aff}(3) > \{1\}$

$$D(a) = D\left(\sum_{g \in \mathrm{Aff}(q^2)} a_g g\right) = \sum_{g \in \mathrm{Aff}(q^2)} a_g D(g).$$

If $\{g_1, \ldots g_s\}$ is a complete set of left coset representatives of $\mathrm{Aff}(q)$ in $\mathrm{Aff}(q^2)$, then

$$\begin{aligned} D(a) &= \sum_{g \in \mathrm{Aff}(q^2)} a_g D(g) \\ &= \sum_{i=1}^{s} \sum_{g \in g_i \mathrm{Aff}(q)} a_g D(g) \\ &= \sum_{i=1}^{s} D(g_i) \sum_{h \in \mathrm{Aff}(q)} a_{g_i h} D(h) \\ &= \sum_{i=1}^{s} D(g_i) D(a_i) \end{aligned}$$

for $a_i = \sum_{h \in \mathrm{Aff}(q)} a_{g_i h} h$. So, to evaluate $D(a)$, we need to evaluate $D(a_i)$ for $s = |\mathrm{Aff}(q^2) : \mathrm{Aff}(q)| = q(q+1)$ i's, as well as take the s products $D(g_i)D(a_i)$, and then do the $s-1$ sums between the terms.

The question remains: how long this will take? We will calculate the operations required for each step. We let $L(\mathrm{Aff}(q^2))$ denote the number of operations it takes to calculate $D(a)$ for $a \in \mathbb{C}\mathrm{Aff}(q^2)$. It will be useful to calculate $L(\mathrm{Aff}(q^2))$ in terms of $L(\mathrm{Aff}(q))$. We will split the calculation into three steps. So,

$$L(\mathrm{Aff}(q^2)) \in \mathcal{O}\left(A + P + S\right)$$

where A is the time to calculate the $D(a_i)$'s, P is the time to calculate the products $D(g_i) \times D(a_i)$, and S is the time to calculate the sums of the terms $D(g_i)D(a_i)$.

Evaluating $D(a_i)$ Time time to calculate $D(a_i)$ is $L(\mathrm{Aff}(q))$ by our definition. We need to calculate this for each of the s a_i's. So,

$$A = sL(\mathrm{Aff}(q)) = q(q+1)L(\mathrm{Aff}(q)) \in \mathcal{O}\left(q^2 L(\mathrm{Aff}(q))\right).$$

Evaluating the product $D(g_i) \times D(a_i)$ Let $\delta_1 = \sum_i d_i$ be the sum of the dimensions of the irreducible representations of $\mathrm{Aff}(q^2)$.

Both $D(g_i)$ and $D(a_i)$ will have up to $|\mathrm{Aff}(q^2)|$ non-zero entries (in the same locations) arranged in a block diagonal $\delta_1 \times \delta_1$ matrix. Each block of size d_i will take d_i^3 operations to multiply. So, the entire multiplication $D(g_i) \times D(a_i)$ takes $\delta_3 = \sum_i d_i^3$. Recall that $\mathrm{Aff}(q^2)$ has $q^2 - 1$ one-dimensional representations and one (q^2-1)-dimensional representation. Thus, $\delta_3 = (q^2-1)1^3 + 1(q^2-1)^3 = q^2(q^2-1)^2 \in \mathcal{O}(q^6)$. We need to perform s of these multiplications, so the multiplication requires

$$P = sq^2(q^2-1)^2 = q(q+1)q^2(q^2-1)^2 \in \mathcal{O}\left(q^8\right)$$

operations.

Evaluating the sums $D(g_i)D(a_i) + D(g_{i+1})D(a_{i+1})$ In general, it should be hard to make the $D(g_i)D(a_i)$'s sum nicely, since $D(b)$ (for $b \in \mathbb{C}\mathrm{Aff}(q^2)$) does not in general have significantly fewer than $|\mathrm{Aff}(q^2)| = q^2(q^2 - 1)$ non-zero entries.

In the worst case, $\sum_{i=1}^{m} D(g_i)D(a_i)$ and $D(g_{i+1})D(a_{i+1})$ both have $|\mathrm{Aff}(q^2)| = q^2(q^2-1)$ non-zero entries (in the same positions), so the sum will take $|\mathrm{Aff}(q^2)| = q^2(q^2-1)$ operations. We need to perform this sum $s - 1 = q(q+1) - 1$ times, no matter how we split it up. Our total number of operations is

$$S = (s-1)|\mathrm{Aff}(q^2)| = (q(q+1)-1)q^2(q^2-1) \in \mathcal{O}\left(q^6\right).$$

So, in total, we have

$$\begin{aligned} L(\mathrm{Aff}(q^2)) &\in \mathcal{O}\left(A + P + S\right) \\ &\in \mathcal{O}\left(q^2 L(\mathrm{Aff}(q)) + q^8 + q^6\right) \\ &\in \mathcal{O}\left(q^2 L(\mathrm{Aff}(q)) + q^8\right) \\ &\in \mathcal{O}\left(|\mathrm{Aff}(q)| L(\mathrm{Aff}(q)) + |\mathrm{Aff}(q^2)|^2\right). \end{aligned}$$

This recurrence relation is not reassuring. We know we can calculate $L(\mathrm{Aff}(p)) \in \mathcal{O}(|\mathrm{Aff}(p)|^2) = \mathcal{O}(p^4)$. Then, since $|\mathrm{Aff}(p)| = (p-1)p$ and $|\mathrm{Aff}(p^2)| = (p^2-1)p^2$,

$$\begin{aligned} L(\mathrm{Aff}(p^2)) &\in \mathcal{O}\left(p^2 L(\mathrm{Aff}(p)) + p^8\right) \\ &\in \mathcal{O}\left(p^6 + p^8\right) \\ &\in \mathcal{O}\left(p^8\right). \end{aligned}$$

I claim that $L(\mathrm{Aff}(p^{2^i})) \in \mathcal{O}(p^{4\cdot 2^i}) = \mathcal{O}\left(|\mathrm{Aff}(p^{2^i})|^2\right)$ for $i \geq 1$. We see it holds for the base case above. Assume it holds for $L(\mathrm{Aff}(p^{2^n}))$. Then,

$$\begin{aligned} L(\mathrm{Aff}(p^{2^{n+1}})) &\in \mathcal{O}\left(p^{2^{n+1}} L(\mathrm{Aff}(p^{2^n})) + p^{4\cdot 2^{n+1}}\right) \\ &\in \mathcal{O}\left(p^{2^{n+1}} p^{4\cdot 2^n} + p^{4\cdot 2^{n+1}}\right) \\ &\in \mathcal{O}\left(p^{3\cdot 2^{n+1}} + p^{4\cdot 2^{n+1}}\right) \\ &\in \mathcal{O}\left(p^{4\cdot 2^{n+1}}\right) \\ &\in \mathcal{O}\left(|\mathrm{Aff}(p^{2^{n+1}})|^2\right), \end{aligned}$$

as desired. This running time is the same as could be obtained through a brute force algorithm! It seems like our index is really causing us trouble here, since the dominating terms is found by multiplying the index by the size of the larger group. This will not allow our algorithm to have the speed-up we desire. It seems like the best way to reduce the running time is to decrease the index of the subgroup chain, since that contributed so heavily to the running time. The next section will evaluate a new subgroup chain for $\mathrm{Aff}(q)$ that has a smaller index.

Chapter 3

The Intermediate Affine Group

We define $\mathrm{Aff}(q, q^2)$ to be the *intermediate affine group* over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ as follows:

$$\mathrm{Aff}(q, q^2) := \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \middle| \, x \in \mathbb{F}_q, y \in \mathbb{F}_{q^2}, x \neq 0 \right\}.$$

Once again, in the element $A = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q, q^2)$, we call x the *diagonal entry* of A and y the *non-diagonal entry* of A.

We can see that $\mathrm{Aff}(q, q^2)$ is, in fact, a group by the following. First, since it is a subset of $\mathrm{Aff}(q^2)$, all we need to show is that it is closed under multiplications and that inverses exist. So, if $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q, q^2)$, then

$$AB = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}.$$

Since a and c are non-zero and in $\mathbb{F}_q$, ac is nonzero ($\mathbb{F}_q$ is a field and contains no zero divisors). So, $AB \in \mathrm{Aff}(q, q^2)$, and $\mathrm{Aff}(q, q^2)$ is closed under the group operation (which is multiplication).

Next, we must show that inverses exist in $\mathrm{Aff}(q, q^2)$. So, if $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q, q^2)$, we must show there exists some $A^{-1} \in \mathrm{Aff}(q, q^2)$ such that $AA^{-1} = I$. Well, let $A' = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}$. Since $a \neq 0$, $a^{-1} \neq 0$, so $A' \in \mathrm{Aff}(q, q^2)$. Next, notice

$$AA' = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b - b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

Thus, $A' = A^{-1}$, inverses exist in $\mathrm{Aff}(q, q^2)$, and $\mathrm{Aff}(q, q^2)$ is a subgroup of $\mathrm{Aff}(q^2)$.

3.1 A better subgroup chain for Aff(q)

Next, let's calculate the order of $|\mathrm{Aff}(q, q^2)|$. There are $(q-1)$ possible diagonal entries (since it is in $\mathbb{F}_q$, and is non-zero) and q^2 possible non-diagonal entries (since it can be any element of $\mathbb{F}_{q^2}$, including zero). So, $|\mathrm{Aff}(q, q^2)| = (q-1)q^2$.

Notice that, in addition to $\mathrm{Aff}(q, q^2)$ being a subgroup of $\mathrm{Aff}(q^2)$, $\mathrm{Aff}(q)$ is a subgroup of $\mathrm{Aff}(q, q^2)$. Thus, we get a new subgroup chain

$$\mathrm{Aff}(q) < \mathrm{Aff}(q, q^2) < \mathrm{Aff}(q^2).$$

In the case where $q = p^{2^n}$, we can write

$$\mathrm{Aff}(p) < \mathrm{Aff}(p, p^2) < \mathrm{Aff}(p^2) < \ldots < \mathrm{Aff}(p^{2^{n-1}}, p^{2^n}) < \mathrm{Aff}(p^{2^n}).$$

3.2 The conjugacy classes of Aff(q, q^2)

For any group G, the number of inequivalent irreducible representations of G is equal to the number of conjugacy classes of G. So, we will first find the conjugacy classes of $\mathrm{Aff}(q, q^2)$ so that we can figure out its representations.

Consider any $A = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(q, q^2)$. We recall that A is precisely conjugate to the elements of $\mathrm{Aff}(q, q^2)$ of the form BAB^{-1}, where $B \in \mathrm{Aff}(q)$. So, for $B = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix}$,

$$BAB^{-1} = \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c^{-1} & -c^{-1}d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & cb + d(1-a) \\ 0 & 1 \end{pmatrix}.$$

From the definition of conjugacy, we see that the identity is in its own conjugacy class (it is only conjugate to itself). Next, if we let $a = 1$ and $b \neq 0$, the matrix is conjugate to matrices of the form

$$\begin{pmatrix} 1 & cb \\ 0 & 1 \end{pmatrix}$$

where $c \neq 0$ and $c \in \mathbb{F}_q$. Thus, this matrix is conjugate to $q-1$ matrices, since cb will be different for each choice of c. There are q^2 matrices with diagonal entry 1; there are $q^2 - 1$ of this form that aren't the identity. Each non-identity matrix with diagonal entry 1 is in a conjugacy class with $(q-1)$ other matrices of this form. Thus, there are $q+1$ conjugacy classes for these non-identity matrices with diagonal entry 1, or $q+2$ in total (including the identity).

Next, the matrix $A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $a \neq 1$ is conjugate to matrices of the form

$$\begin{pmatrix} a & d(1-a) \\ 0 & 1 \end{pmatrix}$$

where $d \in \mathbb{F}_q$. Since $(1-a) \neq 0$, we can choose $d = (1-a)^{-1}e$ where $e \in \mathbb{F}_{q^2}$, since d is any element of $\mathbb{F}_{q^2}$. So, $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is conjugate to *all elements of the form* $\begin{pmatrix} a & e \\ 0 & 1 \end{pmatrix}$. This completes our search for conjugacy class, and gives us $q-2$ more conjugacy classes, since there are $q-2$ nonzero and nonone choices for a. In total, there are $q + 2 + (q-2) = 2q$ conjugacy classes for $\mathrm{Aff}(q, q^2)$.

3.3 The representations of Aff$(3, 3^2)$

We will now restrict ourselves to the case of $\mathrm{Aff}(3, 3^2)$. After doing so, we will move to $\mathrm{Aff}(p, p^2)$, for prime p. Then, finally, we will discuss why the representations of $\mathrm{Aff}(q, q^2)$ for $q = p^n$ are hard to find.

By the above, there are $2q = 2 \times 3 = 6$ irreducible representations for $\mathrm{Aff}(3, 3^2)$. Then, since $|\mathrm{Aff}(3, 3^2)| = (3-1)3^2 = 18$, the sum of the squares of the representation is 18. Let $\sigma_1, \dots \sigma_6$ be the six irreducible representations of $\mathrm{Aff}(q, q^2)$ in increasing order of dimension (so, σ_1 has the highest degree, etc.). We can now figure out the degrees of the representation without too much more work. We know that

$$18 = \sum_{i=1}^{6} (\dim \sigma_i)^2$$

Assume for the sake of contradiction that $\dim \sigma_1 \geq 5$. Then,

$$18 = (\dim \sigma_1)^2 + \sum_{i=2}^{6} (\dim \sigma_i)^2 \geq 25,$$

which is a contradiction. Next, assume $\dim \sigma_1 = 4$. Then,

$$18 = (\dim \sigma_1)^2 + \sum_{i=2}^{6} (\dim \sigma_i)^2 = 16 + \sum_{i=2}^{6} (\dim \sigma_i)^2.$$

Since $\dim \sigma_i \geq 1$, this implies $18 = 16 + \sum_{i=2}^{6} (\dim \sigma_i)^2 \geq 16 + 5$, which is a contradiction. Next, suppose $\dim \sigma_1 = 3$. This implies

$$18 = 9 + \sum_{i=2}^{6} (\dim \sigma_i)^2.$$

Clearly $\dim \sigma_2 \neq 3$ and $\dim \sigma_2 \neq 1$ (since if $\dim \sigma_2 = 1$, $\dim \sigma_3 = \dim \sigma_4 = \dim \sigma_5 = \dim \sigma_6 = 1$, which would not allow that sum to be 18), so $\dim \sigma_2 = 2$. This implies $\sum_{i=3}^{6} (\dim \sigma_i)^2 = 5$. Again, this says that $\dim \sigma_3 = 2$, which quickly leads to a contradiction. So, $\dim \sigma_1 \leq 2$. We can't have $\dim \sigma_1 = 1$, since that would imply $\sigma_i = 1$ for all i. Thus, $\dim \sigma_1 = 2$. The only possible solution to the remaining equation is $\dim \sigma_1 = \dim \sigma_2 = \dim \sigma_3 = \dim \sigma_4 = 2$, and $\dim \sigma_5 = \dim \sigma_6 = 1$.

This information can help our search quite a bit. First, we will find the one-dimensional representations and then the two-dimensional ones. But, first we will discuss the representations of the additive group of $\mathbb{F}_q$, $\mathbb{F}_q^+$.

3.3.1 The additive group of $\mathbb{F}_q$

The additive group of $\mathbb{F}_p$, $\mathbb{F}_p^+$, is cyclic, since it is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Say it has generator γ. So, each $x \in \mathbb{F}_p^+$ can be written as γj for $j \in \mathbb{Z}$ and $0 \leq j < p$. There are p irreducible one-dimensional representations of $\mathbb{F}_p^+$. Denote them by $\rho_k(y)$, for $0 \leq k < p$, and let

$$\rho_k(\gamma j) := e^{2\pi i jk/p}.$$

Since $q = p^n$, the index of the field extension $[\mathbb{F}_q : \mathbb{F}_p] = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. So, $\mathbb{F}_q$ can be seen as a vector space with n basis vectors from $\mathbb{F}_q$ and scalars coming from $\mathbb{F}_p$. Let $v_1, \ldots, v_n$ be those basis vectors. Consider any $x \in \mathbb{F}_q$. We can write

$$x = \sum_{i=1}^{n} x_i v_i$$

where $x_n \in \mathbb{F}_p$. For convenience, we also represent $x = (x_1, \ldots x_n)$.

For $j_1, \ldots j_n$ where $0 \leq j_i < p$, define the representation $\rho_{j_1,\ldots,j_n} : \mathbb{F}_q \to \mathbb{C}$ to be

$$\rho_{j_1,\ldots,j_n}(x) := \rho_{j_1}(x_1)\rho_{j_2}(x_2) \cdots \rho_{j_n}(x_n).$$

Since this is a one-dimensional representation, it is irreducible. Next, notice that if $\rho_{j_1,\ldots,j_n} = \rho_{j_1',\ldots,j_n'}$, all $j_i = j_i'$, since for $x = v_i$,

$$\rho_{j_i'}(1) = \rho_{j_1',\ldots,j_n'}(x)(v_i) = \rho_{j_1,\ldots,j_n}(x)(v_i) = \rho_{j_i}(1).$$

Thus, $j_i = j_i'$. We've found all p^n inequivalent irreducible one-dimensional representations of $\mathbb{F}_q^+$.

3.3.2 One-dimensional representations

The one-dimensional representations of $\mathrm{Aff}(q, q^2)$ are very similar to the one-dimensional representations found for $\mathrm{Aff}(q)$. In fact, they are essentially *the same*. Recall we defined

$$\chi_{k/(q-1)}\left(\begin{pmatrix}\gamma^j & b \\ 0 & 1\end{pmatrix}\right) := \chi_{k/(q-1)}(\gamma^j)$$

where

$$\chi_{k/(q-1)}(\gamma^j) := e^{2\pi i k j/(q-1)}.$$

We will define it exactly the same here! So, we define $\sigma_k : \mathrm{Aff}(3, 3^2) \to \mathbb{C}$ by

$$\sigma_k\left(\begin{pmatrix}\gamma^j & b \\ 0 & 1\end{pmatrix}\right) := \chi_{k/(3-1)}(\gamma^j)$$

for $k = 0$ and 1. Note that $\gamma = 2$. So, we have found the two one-dimensional representations of $\mathrm{Aff}(3, 3^2)$.

3.3.3 Two-dimensional representations

We will first define the subgroup, $H = \mathrm{Aff}(1, 3^2) \cong \mathbb{F}_{3^2}$ where

$$H := \left\{\begin{pmatrix}1 & y \\ 0 & 1\end{pmatrix}, y \in \mathbb{F}_{3^2}\right\}.$$

We can define nine irreducible representations of H using the nine irreducible representations of $\mathbb{F}_{3^2}^+$:

$$\rho_{j_1,j_2}\begin{pmatrix}1 & y \\ 0 & 1\end{pmatrix} := \rho_{j_1,j_2}(y).$$

Now, we will induce these to representations of $\mathrm{Aff}(3, 3^2)$. First, notice that we can use $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(3, 3^2)$ as our left coset reps, since

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} a & ay \\ 0 & 1 \end{pmatrix} \middle| y \in \mathbb{F}_{3^2} \right\} = \left\{ \begin{pmatrix} a & y \\ 0 & 1 \end{pmatrix} \middle| y \in \mathbb{F}_{3^2} \right\}.$$

Call $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $B_2 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

Consider any $A \in \mathrm{Aff}(3, 3^2)$. We see that $AB_i = B_j h$, for exactly one j and $h \in H$. So, if $B_j^{-1} AB_i \in H$, then there is an $h \in H$ so that $AB_i = B_j h$. Thus, $B_j^{-1} AB_i \in H$ for precisely one j.

We define our induced representation using the following. First, for $A \in \mathrm{Aff}(3, 3^2) - H$, define $\rho_{j_1,j_2}(g) = 0$. Then, our induced representation is

$$\rho_{j_1,j_2} \uparrow \mathrm{Aff}(3, 3^2)(A) := \begin{pmatrix} \rho_{j_1,j_2}(B_1^{-1}AB_1) & \rho_{j_1,j_2}(B_1^{-1}AB_2) \\ \rho_{j_1,j_2}(B_2^{-1}AB_1) & \rho_{j_1,j_2}(B_2^{-1}AB_2) \end{pmatrix}.$$

We know B_1 is the identity and $B_2 = B_2^{-1}$, so,

$$\rho_{j_1,j_2} \uparrow \mathrm{Aff}(3, 3^2)(A) = \begin{pmatrix} \rho_{j_1,j_2}(A) & \rho_{j_1,j_2}(AB_2) \\ \rho_{j_1,j_2}(B_2A) & \rho_{j_1,j_2}(B_2AB_2) \end{pmatrix}.$$

Now, we let $A = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ and consider the case where $x = 1$ and where $x = 2$ separately:

$x = 1$ **case** In this case,

$$\rho_{j_1,j_2} \uparrow \mathrm{Aff}(3, 3^2) \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \rho_{j_1,j_2}(y) & 0 \\ 0 & \rho_{j_1,j_2}(2y) \end{pmatrix}.$$

$x = 2$ **case** In this case,

$$\rho_{j_1,j_2} \uparrow \mathrm{Aff}(3, 3^2) \begin{pmatrix} 2 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \rho_{j_1,j_2}(y) \\ \rho_{j_1,j_2}(2y) & 0 \end{pmatrix}.$$

Next comes the question of whether this representation is irreducible. We see that the character of ρ_{j_1,j_2} is

$$\chi_{j_1,j_2} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \begin{cases} \rho_{j_1,j_2}(y) + \rho_{j_1,j_2}(2y) & x = 1 \\ 0 & x \neq 1 \end{cases}.$$

Consider some representation ρ with character χ. Recall that ρ is irreducible if and only if $\langle \chi, \chi \rangle = 1$. So, we will check whether $\left\langle \chi_{j_1,j_2}, \chi_{j_1,j_2} \right\rangle = 1$.

Notice the character is only nonzero at x if $x = 1$, or, in other words, $A \in H$. So, the inner product is

$$\left\langle \chi_{j_1,j_2}, \chi_{j_1,j_2} \right\rangle = \frac{1}{|\mathrm{Aff}(3,3^2)|} \sum_{A \in \mathrm{Aff}(3,3^2)} \chi_{j_1,j_2}(A)\overline{\chi_{j_1,j_2}(A)} = \frac{1}{18} \sum_{A \in H} \chi_{j_1,j_2}(A)\overline{\chi_{j_1,j_2}(A)}.$$

So, for $A = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$,

$$\left\langle \chi_{j_1,j_2}, \chi_{j_1,j_2} \right\rangle = \frac{1}{18} \sum_{y \in \mathbb{F}_{3^2}} \left(\rho_{j_1,j_2}(y) + \rho_{j_1,j_2}(2y)\right) \left(\overline{\rho_{j_1,j_2}(y) + \rho_{j_1,j_2}(2y)}\right).$$

For space, we will let $\rho_{j_1,j_2} = \rho$. We can expand this sum:

$$\left\langle \chi_{j_1,j_2}, \chi_{j_1,j_2} \right\rangle = \frac{1}{18} \sum_{y \in \mathbb{F}_{3^2}} \rho(y)\overline{\rho(y)} + \rho(2y)\overline{\rho(2y)} + \rho(y)\overline{\rho(2y)} + \rho(2y)\overline{\rho(y)}.$$

We know that, for any a, $a\bar{a} = |a|^2$. Thus, since $\rho(y)$ is a root of unity,

$$\rho(y)\overline{\rho(y)} = \rho(2y)\overline{\rho(2y)} = |\rho(y)|^2 = |\rho(2y)|^2 = 1.$$

So,

$$\begin{aligned} \left\langle \chi_{j_1,j_2}, \chi_{j_1,j_2} \right\rangle &= \frac{1}{18} \sum_{y \in \mathbb{F}_{3^2}} 2 + \rho(y)\overline{\rho(2y)} + \rho(2y)\overline{\rho(y)} \\ &= 1 + \frac{1}{18} \sum_{y \in \mathbb{F}_{3^2}} \rho(y)\overline{\rho(2y)} + \rho(2y)\overline{\rho(y)}. \end{aligned}$$

Thus, χ_{j_1,j_2} is irreducible if and only if $\sum_{y \in \mathbb{F}_{3^2}} \rho(y)\overline{\rho(2y)} = -\sum_{y \in \mathbb{F}_{3^2}} \rho(2y)\overline{\rho(y)}$. We will first consider the sum $\sum_{y \in \mathbb{F}_{3^2}} \rho(y)\overline{\rho(2y)}$. Recall that every $y \in \mathbb{F}_{3^2}$ can be viewed us $av_1 + bv_2$ where $a, b \in \mathbb{F}_3$ and v_1, v_2 are the basis vectors of the $\mathbb{F}_3$-linear vector space, $\mathbb{F}_{3^2}$. Then,

$$\rho(a,b) = \rho_{j_1}(a)\rho_{j_2}(b) = e^{2\pi i j_1 a/3} e^{2\pi i j_2 b/3} = e^{2\pi i (j_1 a + j_2 b)/3}$$

and, recall, $\overline{\rho(a,b)} = e^{2\pi i(-j_1 a - j_2 b)/3}$.

So,

$$\begin{aligned}\sum_{y\in\mathbb{F}_{3^2}} \rho(y)\overline{\rho(2y)} &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(j_1a+j_2b)/3}\overline{e^{2\pi i(2j_1a+2j_2b)/3}} \\ &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(j_1a+j_2b)/3}e^{2\pi i(-2j_1a-2j_2b)/3}.\end{aligned}$$

Recall that $-2 = 1$ in $\mathbb{F}_3$. So,

$$\begin{aligned}\sum_{y\in\mathbb{F}_{3^2}} \rho(y)\overline{\rho(2y)} &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(2j_1a+2j_2b)/3} \\ &= \sum_{a\in\mathbb{F}_3}\left(e^{2\pi i(2j_1a)/3}\sum_{b\in\mathbb{F}_3} e^{2\pi i(2j_2b)/3}\right)\end{aligned}$$

We see that unless $j_2 = 0$, $\sum_{b\in\mathbb{F}_3} e^{2\pi i(2j_2b)/3} = 0$, since the sum is just the sum of the third roots of unity. If $j_2 = 0$, then $\sum_{b\in\mathbb{F}_3} e^{2\pi i(2j_2b)/3} = 3$. Then, the outer sum will be zero unless $j_1 = 0$. If $j_1 = j_2 = 0$, it will sum to 9.

Similarly,

$$\begin{aligned}\sum_{y\in\mathbb{F}_{3^2}} \rho(2y)\overline{\rho(y)} &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(2j_1a+2j_2b)/3}\overline{e^{2\pi i(j_1a+j_2b)/3}} \\ &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(2j_1a+2j_2b)/3}e^{2\pi i(-j_1a-j_2b)/3} \\ &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(j_1a+j_2b)/3} \\ &= \sum_{(a,b)\in\mathbb{F}_{3^2}} e^{2\pi i(j_1a+j_2b)/3} \\ &= \sum_{a\in\mathbb{F}_3} e^{2\pi i(j_1a)/3}\sum_{b\in\mathbb{F}_3} e^{2\pi i(j_2b)/3}.\end{aligned}$$

Again, unless both of j_1 and j_2 is zero, this will sum to 0. If $j_1 = j_2 = 0$, it will sum to 9 again. So,

$$\langle \chi_{j_1,j_2}, \chi_{j_1,j_2}\rangle = \begin{cases} 2 & j_1 = j_2 = 0 \\ 1 & \text{else}\end{cases}$$

Thus, χ_{j_1,j_2} is irreducible if and only if one of j_1 and j_2 is non-zero. So, since there were 3 choices for each of j_1 and j_2, this leaves $3^2 - 1 = 8$ irreducible representations of this form. We are only looking for four representations, so some of these that we have found must not be unique. Recall that two representations are equivalent if they share the same character. So, when does $\chi_{a,b} = \chi_{c,d}$?

If $\chi_{a,b} = \chi_{c,d}$, we have that for all $y \in \mathbb{F}_{3^2}$,

$$\rho_{a,b}(y) + \rho_{a,b}(2y) = \chi_{a,b}(y) = \chi_{c,d}(y) = \rho_{c,d}(y) + \rho_{c,d}(2y).$$

Recall that, since $y \in \mathbb{F}_{3^2}$, we can write $y = y_1v_1 + y_2v_2$ where $y_1, y_2 \in \mathbb{F}_3$. So,

$$\rho_{a,b}(y) + \rho_{a,b}(2y) = \rho_{a,b}(y_1, y_2) + \rho_{a,b}(2y_1, 2y_2) = e^{2\pi i/3(ay_1+by_2)} + e^{2\pi i/3(2ay_1+2by_2)}$$

$$= e^{2\pi i/3(ay_1+by_2)} + e^{-2\pi i/3(ay_1+by_2)} = 2\mathrm{Re}\left(e^{2\pi i/3(ay_1+by_2)}\right)$$

We can apply the same argument to $\chi_{c,d}$. Thus,

$$2\mathrm{Re}\left(e^{2\pi i/3(ay_1+by_2)}\right) = 2\mathrm{Re}\left(e^{2\pi i/3(cy_1+dy_2)}\right).$$

If we set $y_2 = 0$ and $y_1 = 1$, we see that $\mathrm{Re}\left(e^{2\pi i/3(a)}\right) = \mathrm{Re}\left(e^{2\pi i/3(c)}\right)$, or $a = \pm c$. A similar argument show that $b = \pm d$. Imagine $a = c \neq 0$ and $0 \neq b = -d$. Then, for $y_1 = y_2 = 1$,

$$\mathrm{Re}\left(e^{2\pi i/3(a+b)}\right) = \mathrm{Re}\left(e^{2\pi i/3(a+d)}\right),$$

which is not possible. Similarly, if $b = d \neq 0$, then $a = c$. So, we see that $\chi_{a,b} = \chi_{c,d}$ iff and only if either $(a, b) = (c, d)$ or $(-a, -b) = (c, d)$. So, out of the eight irreducible representations we found earlier, there were four inequivalent irreducible two-dimensional representations. We have found all six irreducible representations of $\mathrm{Aff}(q, q^2)$. Figure 3.1 shows the branching diagram for $\mathrm{Aff}(3^2) > \mathrm{Aff}(3, 3^2) > \mathrm{Aff}(3) > \{1\}$.

3.4 Representations of Aff(p, p^2)

By the above, $\mathrm{Aff}(p, p^2)$ has $2p$ irreducible representations. By Garling (1986), we know $\mathbb{F}_{p^2}$ forms a $\mathbb{F}_p$-linear vector space with 2 basis vectors, v_1 and v_2.

First, we will concentrate on the one-dimensional ones. Just like in the above, we inherit our one-dimensional representations from $\mathrm{Aff}(p)$. We define

$$\sigma_k\left(\begin{pmatrix}\gamma^j & b \\ 0 & 1\end{pmatrix}\right) := \chi_{k/(p-1)}(\gamma^j)$$

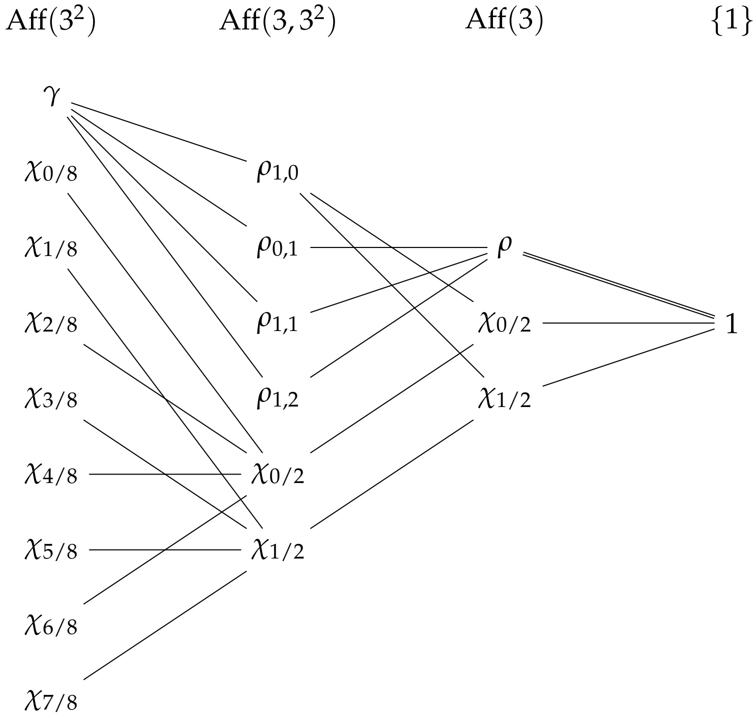

Figure 3.1 Branching Diagram for Aff$(3^2) >$ Aff$(3, 3^2) >$ Aff$(3) > \{1\}$

for $0 \leq k \leq p-1$. So, we have found $p-1$ one-dimensional representations of $\mathrm{Aff}(p, p^2)$.

Let $H \leq \mathrm{Aff}(p, p^2)$ be the subgroup of elements with 1 as the diagonal entry. First, notice that the set $\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(p, p^2) \right\}$ is a complete set of left coset representatives, since

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} H = \left\{ \begin{pmatrix} a & ay \\ 0 & 1 \end{pmatrix} \middle| \, y \in \mathbb{F}_{p^2} \right\} = \left\{ \begin{pmatrix} a & y \\ 0 & 1 \end{pmatrix} \middle| \, y \in \mathbb{F}_{p^2} \right\}$$

and thus each $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ is in its own coset, and each $\begin{pmatrix} a & y \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(p, p^2)$ is in the same coset as $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Thus, $\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right\}$ is a valid complete set of left coset representatives. Let $g_1, \ldots g_{q-1}$ denote these coset representatives, where $g_i = \begin{pmatrix} a_i & 0 \\ 0 & 1 \end{pmatrix}$ for some $a_i \in \mathbb{F}_p^\times$.

We define, for $0 \leq a, b < p$, the representation $p_{a,b} : H \to \mathbb{C}$ by

$$p_{a,b} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} := \rho_{a,b}(y),$$

using the representations we know for the additive group $\mathbb{F}_{p^2}^+$. That is, if $y = y_1 v_1 + y_2 v_2$,

$$\rho_{a,b}(y) = \rho_a(y_1)\rho_b(y_2) = e^{2\pi i a y_1 / p} e^{2\pi i a y_2 / p}.$$

As we've done before, we will induce this representation to the entire group. Let $\rho_{a,b} = p_{a,b} \uparrow \mathrm{Aff}(p, p^2)$. By definition,

$$\rho_{a,b}(g) = p_{a,b} \uparrow \mathrm{Aff}(q)(g) := \begin{pmatrix} p_{a,b}(g_1^{-1} g g_1) & p_{a,b}(g_1^{-1} g g_2) & \cdots & p_{a,b}(g_1^{-1} g g_{q-1}) \\ p_{a,b}(g_2^{-1} g g_1) & p_{a,b}(g_2^{-1} g g_2) & \cdots & p_{a,b}(g_2^{-1} g g_{q-1}) \\ \vdots & \vdots & \ddots & \vdots \\ p_{a,b}(g_{q-1}^{-1} g g_1) & p_{a,b}(g_{q-1}^{-1} g g_2) & \cdots & p_{a,b}(g_{q-1}^{-1} g g_{q-1}) \end{pmatrix}.$$

The character of this representation is

$$\chi_{a,b} \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} = \begin{cases} \sum_{z \in \mathbb{F}_p^\times} \rho_{a,b}(zy) & x = 1 \\ 0 & x \neq 1 \end{cases}$$

since $g_i^{-1}gg_i \in H$ if and only if $g \in H$, and thus $p_{a,b}(g_i^{-1}gg_i) = 0$ if $g \notin H$. When $g = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in H$, $p_{a,b}(g_i^{-1}gg_i) = \rho_{a,b}(y)$. Thus, $\chi_{a,b} = \sum_{a_i \in \mathbb{F}_p^\times} \rho_{a,b}(a_i y)$.

We can write $y = y_1 v_1 + y_2 v_2$, where y_1 and y_2 are in $\mathbb{F}_p$. We defined

$$\rho_{a,b}(y_1, y_2) = \rho_a(y_1)\rho_b(y_2) = e^{2\pi i a y_1/p} e^{2\pi i b y_2/p} = e^{2\pi i(ay_1+by_2)/p}.$$

We first need to show when $\rho_{a,b}$ is equivalent to $\rho_{c,d}$. Recall this is the case if and only if $\chi_{a,b} = \chi_{c,d}$.

Assume $\chi_{a,b} = \chi_{c,d}$. Then, they are equal for each $y = y_1 v_1 + y_2 v_2 \in \mathbb{F}_{p,p^2}$. So, we see that

$$\sum_{z \in \mathbb{F}_p^\times} \rho_{a,b}(zy) = \sum_{z \in \mathbb{F}_p^\times} \rho_{c,d}(zy),$$

and thus

$$\sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(ay_1+by_2)/p} = \sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(cy_1+dy_2)/p}.$$

Assume $ay_1 + by_2 = A \neq 0$. Since $a, y_1, b, y_2 \in \mathbb{F}_p$, $A \in \mathbb{F}_p^\times$. The sum

$$\sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(ay_1+by_2)/p} = \sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(A)/p}$$

is simply

$$\sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(ay_1+by_2)/p} = \sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z/p}.$$

This is the sum of the pth roots of unity except when $z = 0$. Thus,

$$\sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(ay_1+by_2)/p} = -1 + \sum_{z \in \mathbb{F}_p} e^{2\pi i z/p} = -1.$$

However, when $ay_1 + by_2 = 0$, then

$$\sum_{z \in \mathbb{F}_p^\times} e^{2\pi i z(ay_1+by_2)/p} = \sum_{z \in \mathbb{F}_p^\times} e^0 = p - 1.$$

So, $\chi_{a,b} = \chi_{c,d}$ if and only if $ay_1 + by_2 = 0$ for the exactly same $y = y_1 v_1 + y_2 v_2$ as when $cy_1 + dy_2 = 0$. If $ay_1 + by_2 = 0$, this would imply $ay_1 = -by_2$. If $a = 0$, this implies $c = 0$ (notice if $y = v_1$, $cy_1 + dy_2 = c$ and $0y_1 + by_2 = 0$) and b and d can both be zero or both be non-zero. Otherwise, we can write $y_1 = -\frac{b}{a}y_2 = -\frac{d}{c}y_2$. So, $\frac{b}{a} = \frac{d}{c}$. Thus, $\chi_{a,b} = \chi_{c,d}$ if there exists a $z \in \mathbb{F}_p^\times$ such that $c = za$ and $d = za$. So, each $\rho_{a,b}$ is equivalent to $p-1$ other $\rho_{c,d}$.

Next, we check whether these $\rho_{a,b}$ are irreducible. Recall that $\langle \chi_{a,b}, \chi_{a,b} \rangle = 1$ if and only if $\rho_{a,b}$ is irreducible. We see

$$\begin{aligned}\langle \chi_{a,b}, \chi_{a,b} \rangle &= \frac{1}{p^2(p-1)} \sum_{y \in \mathbb{F}_{p^2}} \chi_{a,b}(zy)\overline{\chi_{a,b}(zy)} \\ &= \frac{1}{p^2(p-1)} \sum_{y \in \mathbb{F}_{p^2}} \left(\sum_{z \in \mathbb{F}_p^\times} \rho_{a,b}(zy) \right) \overline{\left(\sum_{z \in \mathbb{F}_p^\times} \rho_{a,b}(zy) \right)}.\end{aligned}$$

As we argued above, $\chi_{a,b}(y_1, y_2) = -1$ when $ay_1 + by_2 \neq 0$, and it equals $p-1$ otherwise. First, assume $a = 0$ and $b = 0$. Then, $ay_1 + by_2 = 0$ always, and our character is $p-1$ for all $y \in \mathbb{F}_{p^2}$. So,

$$\langle \chi_{0,0}, \chi_{0,0} \rangle = \frac{1}{p^2(p-1)} \sum_{y \in \mathbb{F}_{p^2}} (p-1)\,\overline{(p-1)} = p-1.$$

If $a = 0$ and $b \neq 0$, then $ay_1 + by_2 = by_2 = 0$ precisely when $y_2 = 0$. So

$$\begin{aligned}\langle \chi_{a,b}, \chi_{a,b} \rangle &= \frac{1}{p^2(p-1)} \sum_{y_1 \in \mathbb{F}_p} \left(\sum_{y_2 = 0} (p-1)^2 + \sum_{y_2 \in \mathbb{F}_p^\times} (-1)^2 \right) \\ &= \frac{1}{p^2(p-1)} p\left((p-1)^2 + p - 1\right) = \frac{p^2(p-1)}{p^2(p-1)} = 1.\end{aligned}$$

That argument is equivalent in the case where $a \neq 0$ and $b = 0$. Next, let $a \neq 0$ and $b \neq 0$. Then $ay_1 + by_2 = 0$ precisely when $y_1 = -\frac{b}{a}y_2$. So,

$$\begin{aligned}\langle \chi_{a,b}, \chi_{a,b} \rangle = \frac{1}{p^2(p-1)} \sum_{y_1 \in \mathbb{F}_p} \sum_{y_2 = -\frac{a}{b}y_1} \chi_{a,b}(zy)\overline{\chi_{a,b}(zy)} + \sum_{\mathbb{F}_p \ni y_2 \neq -\frac{a}{b}y_1} \chi_{a,b}(zy)\overline{\chi_{a,b}(zy)} \\ = \frac{1}{p^2(p-1)} \sum_{y_1 \in \mathbb{F}_p} (p-1)^2(1) + (p-1)(1) = 1.\end{aligned}$$

Thus, $\chi_{a,b}$ is reducible if and only if $a = b = 0$.

All $\chi_{a,b}$ are irreducible except for when $a = b = 0$. Thus, we found $p^2 - 1$ irreducible representations. We showed that each representation was equivalent to $p-1$ representations. So, we found $p+1$ unique irreducible $(p-1)$-dimensional representations. Since we already found $p-1$

one-dimensional representations, we have found all $2p$ irreducible representations of this group. To verify, we see that the sum of the squares of the dimensions is

$$(p-1)1+(p+1)(p-1)^2 = (p-1)(1+p^2-1) = |\mathrm{Aff}(p,p^2)|.$$

3.5 Representations of Aff(q, q^2)

For $q = p^n$, the irreducible representations are much more difficult to pin down. It is unclear whether the representations of Aff(q, q^2) have a nice, general form. Figuring them out could help the multiplication step of the Cooley-Tukey algorithm (see below). See Chapter 4 for more information on the efforts to fine the irreducible representations of Aff(q, q^2).

3.6 Cooley-Tukey Algorithm

To calculate the DFT of some $a \in \mathbb{C}\mathrm{Aff}(q^2)$, we will use the Cooley-Tukey algorithm described in the introduction and used in the previous chapter. Here, we will use the subgroup chain $\mathrm{Aff}(q^2) \geq \mathrm{Aff}(q,q^2) \geq \mathrm{Aff}(q) \geq \ldots$.

If $a = \sum_{g\in \mathrm{Aff}(q^2)} a_g g$ (where each $a_g \in \mathbb{C}$), then

$$D(a) = D\left(\sum_{g\in \mathrm{Aff}(q^2)} a_g g\right) = \sum_{g\in \mathrm{Aff}(q^2)} a_g D(g).$$

If $\{g_1, \ldots g_s\}$ are a complete set of left coset representatives of H in G (for $H \leq G$), then

$$\begin{aligned} D(a) &= \sum_{g\in G} a_g D(g) \\ &= \sum_{i=1}^{s} \sum_{g\in g_i H} a_g D(g) \\ &= \sum_{i=1}^{s} D(g_i) \sum_{h\in H} a_{g_i h} D(h) \\ &= \sum_{i=1}^{s} D(g_i) D(a_i) \end{aligned}$$

for $a_i = \sum_{h\in H} a_{g_i h} D(h)$. When we let $G = \mathrm{Aff}(q^2)$ and $H = \mathrm{Aff}(q, q^2)$, we get a helpful relation. In this case, to evaluate $D(a)$, we need to evaluate $D(a_i)$ for $s = |\mathrm{Aff}(q^2) : \mathrm{Aff}(q,q^2)| = (q+1)$ i's, as well as take the s products $D(g_i)D(a_i)$, and then do the $s-1$ sums between the terms.

This analysis was what we used in 2.4, but it will not fully suffice here. The relation of $L(\mathrm{Aff}(q,q^2))$ to $L(\mathrm{Aff}(q))$ could be very different, and we will need to understand it as well in order to figure out the asymptotic running time. So, in the equation above, when we set $G = \mathrm{Aff}(q,q^2)$ and $H = \mathrm{Aff}(q)$, we have our index equal to $s' = |\mathrm{Aff}(q,q^2) : \mathrm{Aff}(q)| = q$, leaving us s' evaluations of $D(a_i)$, s' products $D(g_i)D(a_i)$ and $s'-1$ sums between terms.

We will calculate the operations required for each step in the calculations of $L(\mathrm{Aff}(q^2))$ and $L(\mathrm{Aff}(q,q^2))$. We will split

$$L(\mathrm{Aff}(q^2)) \in \mathcal{O}\left(A+P+S\right)$$

and

$$L(\mathrm{Aff}(q,q^2)) \in \mathcal{O}\left(A'+P'+S'\right)$$

where A is the time to calculate $L(\mathrm{Aff}(q^2))$'s $D(a_i)$s (and A' is the same for $L(\mathrm{Aff}(q,q^2))$'s $D(a_i)$s), P is the time to calculate the products $D(g_i) \times D(a_i)$ (P' is the same for $L(\mathrm{Aff}(q,q^2))$'s $D(g_i) \times D(a_i)$s), and S is the time to calculate the sums of the terms $D(g_i)D(a_i)$ (S' is the same for $L(\mathrm{Aff}(q,q^2))$'s $D(g_i)D(a_i)$s).

Evaluating $D(a_i)$ We will cover each case below.

$L(\mathbf{Aff}(q^2))$ Time time to calculate $D(a_i)$ is $L(\mathrm{Aff}(q,q^2))$ by our definition. We need to calculate this for each of the s a_i's. So,

$$A = sL(\mathrm{Aff}(q,q^2)) \in \mathcal{O}\left(qL(\mathrm{Aff}(q,q^2))\right).$$

$L(\mathbf{Aff}(q,q^2))$ By the same logic, $D(a_i)$ is calculated in time $L(\mathrm{Aff}(q))$. So,

$$A' \in s'L(\mathrm{Aff}(q)) \in \mathcal{O}\left(qL(\mathrm{Aff}(q))\right).$$

Evaluating the product $D(g_i) \times D(a_i)$ We will cover each case below.

$L(\mathbf{Aff}(q^2))$ Let $\delta_1 = \sum_i d_i$ be the sum of the dimensions of the irreducible representations of $\mathrm{Aff}(q^2)$.

Both $D(g_i)$ and $D(a_i)$ will have up to $|\mathrm{Aff}(q^2)|$ non-zero entries (in the same locations) arranged in a block diagonal $\delta_1 \times \delta_1$ matrix. Each block of size d_i will take d_i^3 operations to multiply. So, the entire multiplication $D(g_i) \times D(a_i)$ takes $\delta_3 = \sum_i d_i^3$. Recall that $\mathrm{Aff}(q^2)$ has q^2-1 one-dimensional representations and

1 q^2-1 dimensional representation. Thus, $\delta_3 = (q^2-1)1^3 + 1(q^2-1)^3 = q^2(q^2-1)^2 \in \mathcal{O}(q^6)$. We need to perform s of these multiplications, so the multiplication requires

$$P = sq^2(q^2-1)^2 = (q+1)q^2(q^2-1)^2 \in \mathcal{O}\left(q^7\right)$$

operations.

$L(\mathbf{Aff}(q,q^2))$ Next, let $\delta_1' = \sum_i d_i$ be the sum of the dimensions of the irreducible representations of $\text{Aff}(q,q^2)$.

Both $D(g_i)$ and $D(a_i)$ will have up to $|\text{Aff}(q,q^2)|$ non-zero entries (in the same locations) arranged in a block diagonal $\delta_1' \times \delta_1'$ matrix. Each block of size d_i will take d_i^3 operations to multiply. So, the entire multiplication $D(g_i) \times D(a_i)$ takes $\delta_3' = \sum_i d_i^3$. We do not know the irreducible representations for $\text{Aff}(q,q^2)$ beside the $q-1$ one-dimensional ones we inherit from $\text{Aff}(q^2)$, but we can bound δ_3'. The largest δ_3' can be is when all but one of the remaining representations is 1 dimensional and the other has as large dimension as possible. The sum of the squares of the representations is $\delta_2' = \sum_i d_i^2 = |\text{Aff}(q,q^2)|$. Thus, if $d_i = 1$ for $i \neq 2q$,

$$d_{2q}^2 = |\text{Aff}(q,q^2)| - (2q-1) = (q-1)q^2 - (2q-1) \in \mathcal{O}(q^3).$$

So, $\delta_3' \in \mathcal{O}((q^3)^{3/2}) = \mathcal{O}(q^{9/2})$. We need to do s' multiplications. So,

$$P' \in \mathcal{O}(sq^{9/2}) = \mathcal{O}(q^{11/2}).$$

Evaluating the sums $D(g_i)D(a_i) + D(g_{i+1})D(a_{i+1})$ We will cover each case below.

$L(\mathbf{Aff}(q^2))$ In general, it should be hard to make $L(\text{Aff}(q^2))$'s terms of the form $D(g_i)D(a_i)$ sum nicely, since $D(b)$ (for $b \in \mathbb{C}\text{Aff}(q^2)$) has approximately $|\text{Aff}(q^2)| = q^2(q^2-1)$ non-zero entries.

In the worst case, $\sum_{i=1}^m D(g_i)D(a_i)$ and $D(g_{i+1})D(a_{i+1})$ both have $|\text{Aff}(q^2)| = q^2(q^2-1)$ non-zero entries (in the same positions), so the sum will take $|\text{Aff}(q^2)| = q^2(q^2-1)$ operations. We need to perform this sum $s-1=q$ times, no matter how we split it up. Our total number of equal-cost operations is then

$$S = (s-1)|\text{Aff}(q^2)| \in \mathcal{O}\left(q^5\right).$$

Aff(q, q^2) By the same logic, it should be hard to make the summands of$L(\mathrm{Aff}(q, q^2))$ sum nicely, since $D(b)$, for $b \in \mathbb{C}\mathrm{Aff}(q, q^2)$, has approximately $|\mathrm{Aff}(q, q^2)| = q^2(q-1)$ non-zero entries. In the worst case, $\sum_{i=1}^{m} D(g_i)D(a_i)$ and $D(g_{i+1})D(a_{i+1})$ both have $|\mathrm{Aff}(q, q^2)| = q^2(q-1)$ non-zero entries in the same positions, so the sum will take $|\mathrm{Aff}(q, q^2)| = q^2(q-1)$ operations. We need to perform this sum $s' - 1 = q - 1$ times, no matter how we split it up. Our total number of equal-cost operations is then

$$S' = (s'-1)|\mathrm{Aff}(q, q^2)| \in \mathcal{O}\left(q^4\right).$$

So, in total, we have

$$\begin{aligned} L(\mathrm{Aff}(q^2)) &\in \mathcal{O}\left(A + P + S\right) \\ &\in \mathcal{O}\left(qL(\mathrm{Aff}(q, q^2)) + q^7 + q^5\right) \\ &\in \mathcal{O}\left(qL(\mathrm{Aff}(q, q^2)) + q^7\right) \end{aligned}$$

and

$$\begin{aligned} L(\mathrm{Aff}(q, q^2)) &\in \mathcal{O}\left(A' + P' + S'\right) \\ &\in \mathcal{O}\left(qL(\mathrm{Aff}(q)) + q^{11/2} + q^4\right) \\ &\in \mathcal{O}\left(qL(\mathrm{Aff}(q)) + q^{11/2}\right). \end{aligned}$$

This recurrence relation inspires more hope than the one from $\mathrm{Aff}(q^2) \geq \mathrm{Aff}(q)$. We know we can calculate $L(\mathrm{Aff}(p))$ by brute force so $L(\mathrm{Aff}(p)) \in \mathcal{O}(|\mathrm{Aff}(p)|^2) = \mathcal{O}(p^4)$. Then, since $|\mathrm{Aff}(p)| = (p-1)p$, $|\mathrm{Aff}(p, p^2)| = (p-1)p^2$, and $|\mathrm{Aff}(p^2)| = (p^2-1)p^2$,

$$\begin{aligned} L(\mathrm{Aff}(p, p^2)) &\in \mathcal{O}\left(pL(\mathrm{Aff}(p)) + p^{11/2}\right) \\ &\in \mathcal{O}\left(p^5 + p^{11/2}\right) \\ &\in \mathcal{O}\left(p^{11/2}\right). \end{aligned}$$

and

$$\begin{aligned} L(\mathrm{Aff}(p^2)) &\in \mathcal{O}\left(pL(\mathrm{Aff}(p, p^2)) + p^7\right) \\ &\in \mathcal{O}\left(p^{13/2} + p^7\right) \\ &\in \mathcal{O}\left(p^7\right). \end{aligned}$$

I claim that

$$L(\mathrm{Aff}(p^{2^{i+1}})) \in \mathcal{O}(p^{7\cdot 2^i}) = \mathcal{O}\left(|\mathrm{Aff}(p^{2^{i+1}})|^{7/4}\right)$$

and

$$L(\mathrm{Aff}(p^{2^i}, p^{2^{i+1}})) \in \mathcal{O}(p^{11\cdot 2^{i-1}}) = \mathcal{O}\left(|\mathrm{Aff}(p^{2^i}, p^{2^{i+1}})|^{11/6}\right)$$

for $i \geq 1$. First, when $i = 1$, notice

$$\begin{aligned} L(\mathrm{Aff}(p^2, p^4)) &\in \mathcal{O}\left(p^2 L(\mathrm{Aff}(p^2)) + p^{11}\right) \\ &\in \mathcal{O}\left(p^{11}\right) \end{aligned}$$

and

$$\begin{aligned} L(\mathrm{Aff}(p^4)) &\in \mathcal{O}\left(p^2 L(\mathrm{Aff}(p^2, p^4)) + p^{14}\right) \\ &\in \mathcal{O}\left(p^{14}\right). \end{aligned}$$

We see these properties hold for the base case when $i = 0$. Assume it holds for $L(\mathrm{Aff}(p^{2^n}, p^{2^{n+1}}))$; that is, assume $L(\mathrm{Aff}(p^{2^n}, p^{2^{n+1}})) \in \mathcal{O}(p^{11\cdot 2^{i-1}})$. Then,

$$\begin{aligned} L(\mathrm{Aff}(p^{2^{n+1}})) &\in \mathcal{O}\left(p^{2^n} L(\mathrm{Aff}(p^{2^n}, p^{2^{n+1}})) + p^{7\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{2^n} p^{11\cdot 2^{n-1}} + p^{7\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{13\cdot 2^{n-1}} + p^{7\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{7\cdot 2^n}\right) \\ &\in \mathcal{O}\left(|\mathrm{Aff}(p^{2^{n+1}})|^{7/4}\right), \end{aligned}$$

as desired. Next, we must show the other step works. Assume it holds for $L(\mathrm{Aff}(p^{2^{n+1}}))$; that is, assume $L(\mathrm{Aff}(p^{2^{n+1}})) \in \mathcal{O}(p^{7\cdot 2^n})$. Then,

$$\begin{aligned} L(\mathrm{Aff}(p^{2^{n+1}}, p^{2^{n+2}})) &\in \mathcal{O}\left(p^{2^{n+1}} L(\mathrm{Aff}(p^{2^{n+1}})) + p^{11\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{2^{n+1}} p^{7\cdot 2^n} + p^{11\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{9\cdot 2^n} + p^{11\cdot 2^n}\right) \\ &\in \mathcal{O}\left(p^{11\cdot 2^n}\right) \\ &\in \mathcal{O}\left(|\mathrm{Aff}(p^{2^{n+1}}, p^{2^{n+2}})|^{11/6}\right). \end{aligned}$$

So, by induction, these forms hold for all n.

3.7 Conclusion

In Section 2, we showed that using the subgroup chain $\mathrm{Aff}(p) \leq \mathrm{Aff}(p^2) \leq \cdots \leq \mathrm{Aff}(p^{2^{n+1}})$, one could obtain a running time of

$$L(\mathrm{Aff}(p^{2^{n+1}})) \in \mathcal{O}\left(p^{4 \cdot 2^{n+1}}\right) = \mathcal{O}\left(|\mathrm{Aff}(p^{2^{n+1}})|^2\right).$$

In this section, we have used a smarter subgroup chain, $\mathrm{Aff}(p) \leq \mathrm{Aff}(p, p^2) \leq \mathrm{Aff}(p^2) \leq \cdots \leq \mathrm{Aff}(p^{2^{n+1}})$. This gave a running time of

$$L(\mathrm{Aff}(p^{2^{n+1}})) \in \mathcal{O}\left(p^{7 \cdot 2^{n}}\right) = \mathcal{O}\left(|\mathrm{Aff}(p^{2^{n+1}})|^{7/4}\right).$$

This is a faster result asymptotically. The goal in the creation of this intermediate affine group was to refine the $\mathrm{Aff}(p) \leq \mathrm{Aff}(p^2) \leq \cdots \leq \mathrm{Aff}(p^{2^{n+1}})$ subgroup chain, since the index of successive subgroups seemed to be too large. This subgroup chain lends to a more efficient fast Fourier transform for $\mathrm{Aff}(q)$.

Chapter 4

Future work

Originally, my results seemed to be far more substantial. At first, it seemed like the multiplication step (called P and P') in the Cooley-Tukey algorithm would go much more quickly. Terras (1999) suggests that the degree $q-1$ representation of $\mathrm{Aff}(q)$ can be represented as a monomial $(q-1) \times (q-1)$ matrix, and this seemed like something we could exploit at first. However, it is not obvious that the basis that allows this nice form for the degree $(q-1)$ representation is the same as the adapted one we need for our subgroup chain. If we can show these basis are the same, or at least very closely related, we might be able to dramatically decrease the number of operations needed for the multiplication step. So, one question is how the $D(a_i)$ matrices can be represented so multiplication is more efficient?

The irreducible representations of $\mathrm{Aff}(q, q^2)$ proved difficult to find. I attempted to create the representations in the same way we did for $\mathrm{Aff}(q)$, but showing they were irreducible and pairwise inequivalent was more difficult than I expected. It would be helpful to better understand the representations of the group $\mathbb{F}_q^+$, since inducing these representations seemed like a good strategy. $\mathrm{Aff}(q)$'s degree $q-1$ representation was found by inducing the trace, which is a representation of $\mathbb{F}_q^+$; what about the others?

I also attempted to restrict the degree q^2-1 irreducible representation down to $\mathrm{Aff}(q, q^2)$. By rearranging the rows, it is possible to make this representation a block diagonal matrix. I believe these blocks are equal to the irreducible representations of $\mathrm{Aff}(q, q^2)$, but I was not able to prove this. How does the q^2-1 representation restrict to $\mathrm{Aff}(q, q^2)$?

Finding the irreducible representations of $\mathrm{Aff}(q, q^2)$, or even just their dimensions, would really help this algorithm. When calculating P', the time to compute the multiplications for $\mathrm{Aff}(q, q^2)$, we assumed the worst about the dimensions of the remaining representations. So, if we could figure these out, we would have a much better idea about the size of the block-diagonal blocks are in the DFT, which would allow us to better understand the running time.

The group $\mathrm{Aff}(q, q^2)$ can be viewed as a semidirect product between two subgroups. The representations of semidirect products are well studied. This may be another avenue to explore.

Bibliography

Clausen, Michael, and Ulrich Baum. 1993. *Fast Fourier transforms*. Mannheim: Bibliographisches Institut.

Dummit, David S., and Richard M. Foote. 2004. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, 3rd ed.

Emerencia, Ando. 2007. Multiplying huge integers using fourier transforms. Online slides. URL http://www.cs.rug.nl/~ando/pdfs/Ando_Emerencia_multiplying_huge_integers_using_fourier_transforms_presentation.pdf.

Garling, D. J. H. 1986. *A course in Galois theory*. Cambridge University Press, Cambridge.

Spaide, Theodore. 2009. Branching diagrams for group inclusions induced by field inclusions. Harvey Mudd College Senior Thesis.

Terras, Audrey. 1999. *Fourier analysis on finite groups and applications*, *London Mathematical Society Student Texts*, vol. 43. Cambridge: Cambridge University Press.