WXML Final Report: Projective Actions over Finite Fields

Dan Bragg, Kristine Hampton, Manar Riman, Justin Shyi

Spring 2017

1 Introduction

1.1 The initial problem

This project began as a generalization of an attempt to analyze the random behavior of the discrete logarithm over finite fields. To do this, we examined the behavior of projective actions over finite fields, in particular over prime fields. We began this quarter by attempting to generalize and prove our results from previous quarters.

1.2 Definition

$PSL_2(\mathbb{F}_2)$ is defined to be action of invertible 2 × 2 matrices on lines.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

Consider $z = \frac{x}{y}$ and the action

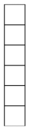
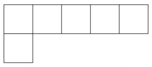
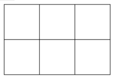
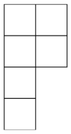
$$z \to \frac{az+b}{cz+d},$$

where $a, b, c, d \in \mathbb{F}_q$ and $z \in P^1(\mathbb{F}_q)$. As $P^1(\mathbb{F}_q)$ is multiplicatively and additively closed, each z is sent to another number in $P^1(\mathbb{F}_q)$. This action thus forms a permutation on $q + 1$ elements.

1.3 Ferrers Diagram

Given a permutation, we can analyze the cycle structure for random behavior. In particular, we can view each cycle as a partition of integers. By doing this, we can represent permutations as Ferrers diagrams where the n^{th} row represents the length of n^{th} longest cycle.

We can then attempt to determine the number of permutations of each cycle type. Below is a table summarizing the cycle structure for permutations arrizing from the action of $PSL_2(\mathbb{F}_p)$ on $P^1(\mathbb{F}_p)$ with the associated number of permutations of each type and the Ferrers shape of the permutation.

# of permutations	number	shape
has all fixed points	1	
has 1 fixed point	$p^2 - 1$	
has 0 fixed points	$p(\frac{p-1}{2})^2$	
has 2 fixed points	$p(\frac{p-1}{2})^2 - p = \frac{p(p-3)(p+1)}{4}$	

(1.1) Statistics for different cycle types

Note that the number of permutations with no fixed points differs only by p from the number of permutations with two fixed points. This table totally summarized the possible permutations that can arise from this action, any permutation with more than two fixed points must be the identity. Additionally, if a permutation has a cycle of length m with $m > 1$, the permutation is composed entirely of m-cycles and at most two fixed points. As a result, each permutation of this action is even. From this, we were able to determine additional restraints upon cycle structure. In particular, when working with matrices in $PSL_2(\mathbb{F}_p)$, we can determine the possible cycle lengths and the corresponding number of permutations with this cycle structure.

2 Progress

The bulk of our computational work and theoretical discoveries were done in previous quarters, this quarter we largely focused upon proving the results. By previously approaching the problem in terms of linear algebra, we were able to make the observation that each element in a cycle were actually an eigenspace of the matrices in the cosets raised to the power of length of the cycle. With that observation, we showed that because each element in a cycle must share the same eigenvalue, any cycle of length greater than 2 for $PSL_2(\mathbb{F}_q)$ implies the matrices in that particular coset raised to the power of the length of the cycle will have eigenspace spanning the entire $\mathbb{F}_q^2$. Hence matrices raised to that power will be the identity matrix, forcing it to be the only cycle length for the coset.

As many of our results relied upon counting, we were also able to employ a variety of results from combinatorics in our proofs. Similarly, as the underlying structure of the problem lies in group theory, many results from group theory were applied. This was particularly helpful when generalizing results to higher dimensions.

3 Future directions

In the time that this project has existed, the majority of the team working upon it have graduated. As such, likely this project will not continue in official capacity. However, we still have a variety of results we have become quite interested in and are attempting to prove. As such, work has continued in the form of a paper summarizing our results. Most likely, any future work done will be in expanding this paper.