WXML Final Report: Projective Actions over Finite Fields

Dan Bragg, Kristine Hampton, Justin Shyi, Andrew Yu

Winter 2017

1 Introduction

1.1 The initial problem

We began this project with the intention of generalizing our previous project analyzing the random behavior of the discrete logarithm over finite fields and extending our work with projective actions over finite fields. We began by proving conjectures we made last quarter and then attempting to generalize these results. We hoped to be able to quantify the random behavior of projective actions over finite fields.

1.2 Definition

$PSL_2(F_2)$ is defined to be action of invertible 2×2 matrices on lines.

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

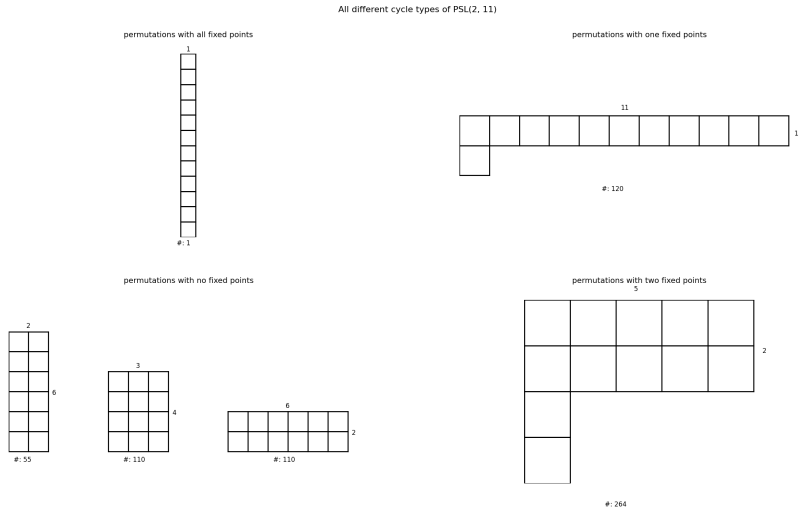
Consider $z = \frac{x}{y}$, then this action becomes

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \to \frac{az + b}{cz + d},$$

where $a, b, c, d \in F_q$ and $z \in P^1(F_q)$. Each z is sent to another number in $P^1(F_q)$, and this forms a permutation.

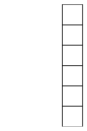
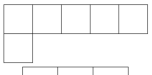
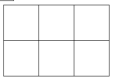
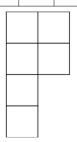
1.3 Ferrers Diagram

Given cycles in a permuations, we can view it as a partition of n integers. By doing this, we can represent permutations as Ferrers diagrams where the n^{th} row represents the length of n^{th} longest cycle. Below is an example of Ferrers Diagram for $PSL_2(F_{11})$. Notice that for some cycle type there could be various "shapes" of Ferrers Diagram, the amount of each is correlated.



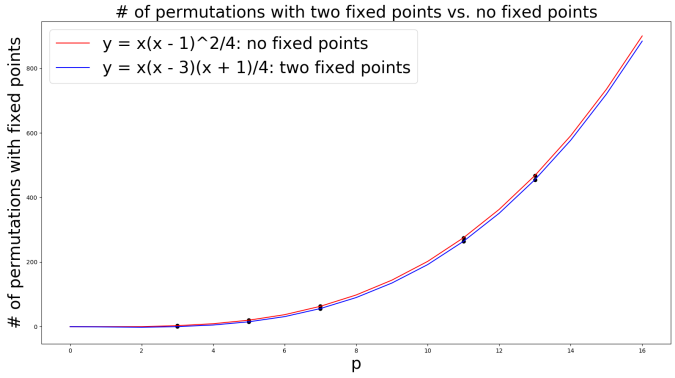
(1.1)

We then seek for the number of permutations of each cycle type. Below is a table summarizing different forms of permutations, and their counts.

# 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	$p(\frac{p-1}{2})^2 - p = \frac{p(p-3)(p+1)}{4}$	

(1.2) Statistics for different types of permutations.

We realized the counts of permutations that have two fixed points and that have no fixed points are very close, below is a plot of the two curves representing the number of permutations with two fixed points or no fixed points.



(1.3)

1.4 Comparison

Through comparison of the structure of cycle lengths with an average of Ferrers diagrams, we were able to notice an interesting result. When working in $PSL_2(\mathbb{F}_q), q \neq 2$, with the exception of a single fixed point and a q cycle, all cycles come in pairs of the same length with up to two fixed points. This is a highly nonrandom result and ultimately leads to $PSL_2(\mathbb{F}_q) \subset A_q$, the group of even permutations on q elements. The majority of our focus has been on attempting to explain this result.

2 Progress

2.1 Theoretical

By 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 $PSL_2(F_q)$ implies the matrices in that particular coset raised to the power of the length of the cycle will have eigenspace spanning the entire F_q^2. Hence matries raised to that power will be the identity matrix, forcing it to be the only cycle length for the coset.

2.2 Computational

By examining a large number of permutations, we were able to determine the number of each fixed point cycle type (zero, one or two fixed points) for varying prime powers and determine the possible cycle lengths that can appear in each permutation. This has led us to conjecture that the number of permutations in $PSL_2(\mathbb{F}_p)$ with 2 fixed points and cycle length m is $\frac{1}{2}\phi(m)p(p+1)$ While the number of permutations in $PSL_2(\mathbb{F}_p)$ with 0 fixed points and cycle length m is $\frac{1}{2}\phi(m)p(p-1)$ And that the sums of the number of all possible such permutations differ by p, as seen in (1.1).

3 Future directions

Next quarter, we will continue to explore the structure of cycle lengths and Ferrers diagrams, specifically looking for a limit curve and exploring higher n. We are also interested in looking at how sets of points, as opposed to singeltons, are acted upon.