WXML Final Report: Projective Actions over Finite Fields

Jayadev Athreya, Dan Bragg, Kristine Hampton, Andrew Yu

Spring 2016

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. We began by gathering statistics on the group actions and comparing to random permutations. 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.

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

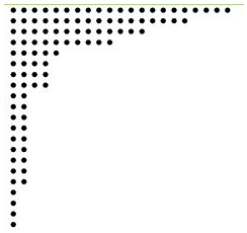
Consider $z = \frac{x}{y}$, then this action becomes

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

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.

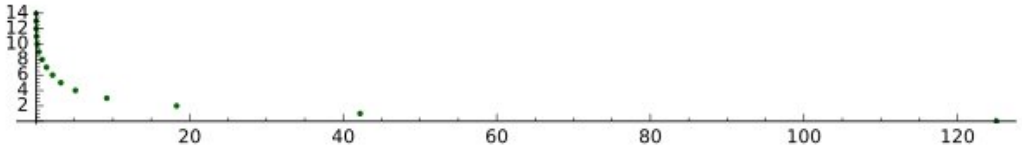
1.3 Ferrers Diagram

Given cycles in a permuations, we can view it as a partition of n integers. The n^{th} row represents the length of n^{th} longest cycle. A typical Ferrers Diagram is shown in (1.1).



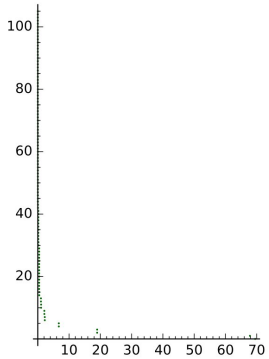
(1.1) An example of Ferrers Diagram

Given a random permutation, the average length of cycles can be statcially computed and is shown in (1.2):



(1.2) An asymptotic curve for cycles in a 200-element permutation

We tend to discover the curve trend for $PSL_2(F_211)$, whose field has a similar size to a 200-element permutation, and is shown in (1.3):



(1.3)

1.4 Comparation

Through comparison of the structure of cycle lengths with an average of Ferrer diagrams, we were able to notice an interesting result. When working in $PSL_2(F_q), q \neq 2$, with the exception of a single fixed point and a q cycle, all cycles come in pairs of the same length. This is a highly nonrandom result and ultimately leads to $PSL_2(F_q) \subset A_q$, 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 Computational

We have had some trouble computationally this quarter, the escalating sizes of our group often made computations slow. As such, we were often restricted to low primes and 2×2 matrices. Hopefully, access to a faster server will lead to even more interesting patterns and results next quarter.

2.2 Theoretical

We have a proof that the expected number of fixed points is the number of orbits of the action of $SL_2(F_q)$ on $P^1(F_q)$, it follows from the Orbit-Stabilizer Theorem. As the actions we have looked at so far have been transitive, this provides a nice comparison to random permutations, the expected number of fixed points of which is one. We also have a proof that $PSL_2(F_p) \subset A_p$ by explicitly checking the order of the generators. We hope, however, to find a more satisfying proof that explains the mechanism behind being in the alternating group. We are also working on finding a closed form for Ferrer's curve and comparing our curve with it.

3 Future directions

Next quarter, we will continue to explore the structure of cycle lengths and Ferrer diagrams. We are also interested in looking at how sets of points, as opposed to singeltons, are acted upon.