Orbits of the Braid Group Action on Rank m $\mathbb{F}_p$-Local Systems Over the n-Punctured Riemann Sphere

Sophia Liao

Under the direction of

Yonghwan Kim
Massachusetts Institute of Technology

Research Science Institute
July 30, 2024

Abstract

A local system describes the behavior of a multi-valued function around n punctures of a sphere. We can represent a rank m $\mathbb{F}_p$-local system as an n-tuple of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$, but this representation is not unique. In particular, we can relate the representations of these local systems under conjugation and the action of the braid group. In this paper, we explore the orbits of the braid group action on the conjugacy classes n-tuples of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$. Specifically, we find lower and upper bounds for the number of orbits, and we provide a description for the possible sizes of orbits when $n = 2$ and $n = 3$. In addition, we find explicit formulas for the number of orbits when $n = 2$, and we explore the nature of the orbits for particular cases when $n = 3$.

Summary

Consider a function which maps each point on a sphere to a single value. As we move around the sphere, the function outputs a different value, but if we revisit any point we have already been to, it will output the same value it did before. Instead of a single-valued function, we can also define a multi-valued function anchored at a particular point on the sphere called a "puncture." Now, this function can output multiple different values at the same point, but how do we know what the output will be? Let us imagine, instead of a flat surface around the puncture, a 3-dimensional spiral staircase centered around the puncture. As we move around the puncture back to the same spot, we end up changing flights on the spiral staircase, but if we move around without circling the puncture, we stay on the same flight. These different flights correspond to different outputs of the multi-valued function, and the behavior of such a staircase around a puncture is called a "monodromy." We can express types of multi-valued functions of n monodromies on the sphere as orbits of the braid group action on n-tuples of $m \times m$ matrices with entries modulo a prime. In this paper, we find bounds and formulas for the number of orbits when n and m are small.

1 Introduction

Braid groups generate a subgroup of the mapping class group of surfaces through Dehn twists, as described in detail in [1]. Braid groups arise in various areas of geometry under several guises [2–4]. In recent years, fascinating connections to arithmetic geometry are also beginning to be understood, such as in the works of [5–9]. One important reason why they appear is because they are closely related to the study of *local systems* over surfaces.

A local system of rank m over a disk with n punctures can be represented as an equivalence class of n-tuples of $m \times m$ matrices whose product is the identity. Each matrix can be considered as the monodromy of a rank m local system along the 1-cycles that the generators of the fundamental group represent. Such a local system can be identified with another through conjugation of each element in the tuple by another matrix. Now, the geometry of the base space—the disk with n punctures—allows us to define an action of the braid group on the set of local systems. As explained in [4], the mapping class group of the underlying surface acts on the equivalence classes of these local systems, and this action has surprising consequences in the field of Diophantine equations and the Gauss-Manin connection of certain algebraic systems.

Previous work, for example that of [10], which concerns the Painlevé VI equations, has focused on the algebraicity of the sections of the local systems, and thus have been confined to the case of $\mathbb{C}$-local systems. For this reason, it is natural to ask what happens for the case of $\mathbb{F}_p$-local systems, or in general, local systems with coefficients in a finite ring. In this paper, we explore the nature of the orbits of the braid group action on similar n-tuples of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$ whose product is the identity.

The paper is organized as follows: In Section 2, we formalize the problem we are studying and explain its geometric consequences. We also introduce notation which will be used throughout the paper. In Section 3, we establish general lower and upper bounds on the number of orbits of the braid group action on n-tuples of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$. In Section 4, we examine the nature of the orbits when the dimension of the matrices is 1, and express the number of orbits as a combinatorial problem about counting necklaces. In Section 5, we find a formula for the number of orbits of pairs of dimension 2 and 3 matrices under the braid group action and provide a general, but rather cumbersome method to calculate the number of orbits for matrices of an arbitrary dimension. In Section 6, we strengthen the general lower bound on the number of orbits for triples of matrices, and we provide the numbers and lengths of specific cases of triples of matrices under the braid group action.

2 Preliminaries

The concept of monodromy describes the behavior of a multi-valued function around a singularity, where "running around" the singularity in a closed path results in a different output of the multi-valued function, whereas a closed loop not containing the singularity maintains the same output. For example, consider the branched $2:1$ covering map between Riemann spheres $z \mapsto z^2 : \mathbb{CP}^1 \to \mathbb{CP}^1$ pictured in Figure 1, which has branch points over $z = 0$ and $z = \infty$. One can look at the monodromy along the closed loop from a point $re^{i\theta}$ to $re^{i\theta}$, which changes the output from $\sqrt{r}e^{i\frac{\theta}{2}}$ to $\sqrt{r}e^{i(\frac{\theta}{2}+\pi)}$, or vice versa. Consequently, we

say that the *monodromy transformation* at every point for $z^{\frac{1}{2}}$ around 0 is multiplication by $e^{i\pi}$.

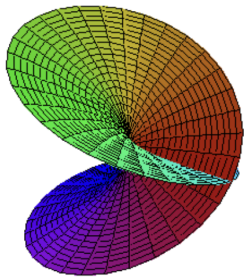

Figure 1: A 3-dimensional projection of the multi-valued function $z^{\frac{1}{2}}$ over $\mathbb{C} \setminus \{0\}$.

For our purposes, a local system is a multi-valued function on a disk with n punctured points which behaves as a single-valued function locally, but undergoes monodromy around punctured points, but a mathematically precise definition of local systems can be found in Farb and Margalit's book [1]. More formally, let $\pi_1(D^2 \setminus \{p_1, \ldots, p_n\})$ denote the fundamental group of a disk D^2 with n punctures, which is isomorphic to the free group on n generators, where each generator corresponds to the class of loops which enclose a single puncture. We can think of elements in the fundamental group as closed loops which start at a fixed point, where two loops are equivalent if we can smoothly deform one to another without crossing any punctures. We define a local system as a homomorphism $\rho : \pi_1(D^2 \setminus \{p_1, \ldots, p_n\}) \to \mathrm{GL}_m(\mathbb{F}_p)$, where ρ sends the loop around all punctures to the identity. Because the monodromy along the boundary of the unit disk is the identity, one can actually extend this local system over the point $\infty \in \mathbb{CP}^1$, shrinking the boundary to a removable singularity to form a Riemannian sphere.

We call $x \in D^2 \setminus \{p_1, \ldots, p_n\}$ a *base point* if it is on the boundary of the disk. Given a choice of x and an ordering of punctures, we can represent a local system as a tuple of matrices $(A_1, A_2, \ldots, A_n)$ such that $A_1 A_2 \cdots A_n = \mathrm{Id}$, where A_i is the monodromy transformation around the ith puncture at the point x. Let x' be a different choice of base point such that X is the transformation matrix from the point x' to x. Then, under the base point x' and the same ordering of punctures, we find the separate representation $(XA_1X^{-1}, XA_2X^{-1}, \ldots, XA_nX^{-1})$ of the local system. Switching the ordering of the i and $(i+1)$th punctures results in the tuple $(A_1, \ldots, A_iA_{i+1}A_i^{-1}, A_i, \ldots, A_n)$ or $(A_1, \ldots, A_{i+1}, A_{i+1}^{-1}A_iA_{i+1}, \ldots, A_n)$, which we we can describe using"under" and "over" adjacent twists in the braid group.

Definition 2.1. The *braid group* B_n on n strands is generated by the adjacent twists $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ which satisfy the relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $1 \leq i \leq n-2$ and $\sigma_k\sigma_\ell = \sigma_\ell\sigma_k$ for $|k - \ell| \geq 2$. That is,

$$B_n := \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \sigma_k\sigma_\ell = \sigma_\ell\sigma_k : |k - \ell| \geq 2 \rangle.$$

One can imagine an element of the braid group as a series of adjacent twists of n strands, where each generator σ_i of the braid group corresponds to twisting the ith strand over the

$(i+1)$th strand. This provides an intuitive understanding of the braid relations, which are illustrated in Figure 2.

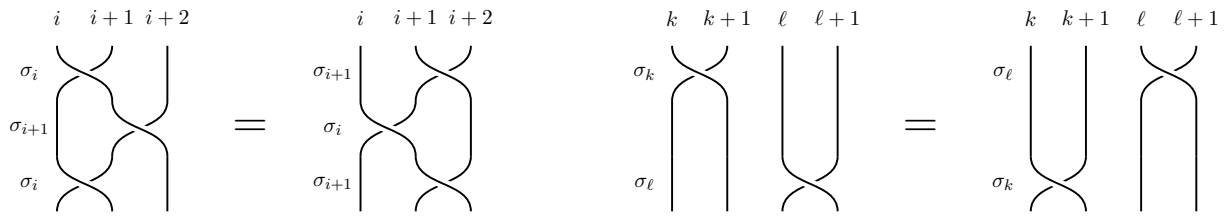

Figure 2: The braid relations.

We define the action of the braid group B_n on n-tuples of matrices as follows:

$$\sigma_i(A_1, A_2, \ldots, A_n) = (A_1, A_2, \ldots, A_i A_{i+1} A_i^{-1}, A_i, \ldots, A_n).$$

Let

$$S_{n,m,p} := \{(A_1, A_2, \ldots, A_n) \mid A_i \in \mathrm{GL}_m(\mathbb{F}_p), A_1 A_2 \cdots A_n = \mathrm{Id}\}$$

be the set of representations of local systems on a disk which fix a base point and the ordering of the punctured points. As a different choice of base point changes the representation by conjugation of some matrix over each element in the tuple, we consider the set of local systems $T_{n,m,p} := S_{n,m,p}/\sim$ where $(A_1, A_2, \ldots, A_n) \sim (A_1', A_2', \ldots, A_n')$ if there exists some $X \in \mathrm{GL}_m(\mathbb{F}_p)$ such that $(A_1, A_2, \ldots, A_n) = (XA_1'X^{-1}, XA_2'X^{-1}, \ldots, XA_n'X^{-1})$. The action of the braid group B_n relates n-tuples of $T_{n,m,p}$ which represent the same local system with respect to reordering the monodromies. In other words, if two n-tuples are in the same orbit, there is a diffeomorphism between the two local systems they represent.

Definition 2.2. The *orbit number* of $T_{n,m,p}$ is the number of orbits of the action of the braid group B_n on $T_{n,m,p}$, which we denote by $c_{n,m,p}$.

In this paper, we explore the nature of the orbit number $c_{n,m,p}$ for various values of n, m, and p, which counts the number of diffeomorphic rank m $\mathbb{F}_p$-local systems of spheres with n punctured points.

Before we begin, we recall shorthand notation which we will use throughout the paper. Let A be a matrix in $\mathrm{GL}_m(\mathbb{F}_p)$. We denote by $\mathrm{Cl}(A) := \{XAX^{-1} \mid X \in \mathrm{GL}_m(\mathbb{F}_p)\}$ the conjugacy class of A. Let $T \in T_{n,m,p}$ be an n-tuple of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$. We denote by $\mathrm{Orb}(T) := \{\sigma T \mid \sigma \in B_n\}$ the orbit of T under the braid group action B_n.

3 Initial Bounds

In this section, we provide lower and upper bounds for the number of orbits of the braid group action on $T_{n,m,p}$. Before we discuss these bounds, we introduce an important result about the nature of the braid group action.

Lemma 3.1. *Let $A := (A_1, \ldots, A_n) \in T_{n,m,p}$, and let $M := A_i A_{i+1}$ Then*

$$\sigma_i^{2k}(A) = (A_1, \ldots, M^k A_i M^{-k}, M^k A_{i+1} M^{-k}, \ldots, A_n) \tag{1}$$

and

$$\sigma_i^{2k+1}(A) = (A_1, \ldots, M^{k+1} A_{i+1} M^{-(k+1)}, M^k A_i M^{-k}, \ldots, A_n). \tag{2}$$

Proof. We proceed by induction. It follows by the definition of the braid group action that the identities hold when $k = 1$. Now, suppose the identities are true for some arbitrary k. Then, we have

$$\begin{aligned}\sigma_i^{2k+2}(A) &= (A_1, \ldots, (M^{k+1}A_{i+1}M^{-(k+1)})(M^kA_iM^{-k})(M^{k+1}A_{i+1}M^{-(k+1)})^{-1},\\ &\quad M^{k+1}A_{i+1}M^{-(k+1)}, \ldots, A_n)\\ &= (A_1, \ldots, M^{k+1}A_{i+1}M^{-1}A_iMA_{i+1}^{-1}M^{-(k+1)}, M^{k+1}A_{i+1}M^{-(k+1)}, \ldots, A_n)\\ &= (A_1, \ldots, M^{k+1}A_iM^{-(k+1)}, M^{k+1}A_{i+1}M^{-(k+1)}, \ldots, A_n),\end{aligned}$$

which implies that identity (1) holds for $k+1$. Using this derivation and applying the braid group action once more, we get

$$\begin{aligned}\sigma_i^{2(k+1)+1} &= (A_1, \ldots, (M^{k+1}A_iM^{-(k+1)})(M^{k+1}A_{i+1}M^{-(k+1)})(M^{k+1}A_iM^{-(k+1)})^{-1},\\ &\quad M^{k+1}A_iM^{-(k+1)}, \ldots, A_n)\\ &= (A_1, \ldots, (M^{k+1}A_iA_{i+1}A_i^{-1}M^{-(k+1)}, M^{k+1}A_iM^{-(k+1)}, \ldots, A_n)\\ &= (A_1, \ldots, M^{k+2}A_{i+1}M^{-(k+2)}, M^{k+1}A_iM^{-(k+1)}, \ldots, A_n),\end{aligned}$$

as desired, which proves identity (2). □

To establish a lower bound, we consider the case of simultaneously diagonalizable n-tuples. When a tuple of matrices $(A_1, A_2, \ldots, A_n)$ is simultaneously diagonalizable, the braid group acts by permutation, as one can see from the computation

$$\begin{aligned}\sigma_i(A_1, \ldots, A_i, A_{i+1}, \ldots, A_n) &= (A_1, \ldots, A_iA_{i+1}A_i^{-1}, A_i, \ldots, A_n)\\ &= (A_1, \ldots, (X^{-1}D_iX)(X^{-1}D_{i+1}X)(X^{-1}D_i^{-1}X), A_i, \ldots, A_n)\\ &= (A_1, \ldots, X^{-1}D_iD_{i+1}D_i^{-1}X, A_i, \ldots, A_n)\\ &= (A_1, \ldots, A_{i+1}, A_i, \ldots, A_n)\end{aligned}$$

where $D_k = XA_kX^{-1}$ is a diagonal matrix for all k.

Lemma 3.2. *Let $(A_1, A_2, \ldots, A_n) \in \mathrm{GL}_m(\mathbb{F}_p)$ be simultaneously diagonalizable. Then the orbit of $(A_1, A_2, \ldots, A_n)$ under the action of the braid group B_n consists of the union of the conjugacy classes of all permutations of $(A_1, A_2, \ldots, A_n)$.*

Proof. Since a generator of the braid group σ_i acts by swapping the adjacent matrices A_i and A_{i+1} and adjacent transpositions generate all permutations, any permutation of $(A_1, A_2, \ldots, A_n)$ is in the orbit of $(A_1, A_2, \ldots, A_n)$. As each element in B_n can be written as a composition of transpositions, the only tuples in the orbit of $(A_1, A_2, \ldots, A_n)$ are in the conjugacy classes of its permutations. □

If two simultaneously diagonalizable tuples in $T_{n,m,p}$ are not in the same conjugacy class under permutation, they are not in the same orbit, so the number of unordered tuples of diagonal matrices whose product is the identity is a lower bound on the orbit number $c_{n,m,p}$.

Proposition 3.3. *The number of orbits $c_{n,m,p}$ of the action of the braid group B_n on $T_{n,m,p}$ is bounded below by*

$$\frac{1}{n-1}\binom{\binom{p+m-2}{m}+n-2}{n-1} \leq c_{n,m,p}.$$

Proof. Let N denote the number of unordered tuples of diagonal matrices whose product is the identity. We show that

$$\frac{1}{n-1}\binom{\binom{p+m-2}{m}+n-2}{n-1} \leq N.$$

As diagonal matrices are conjugate to each other by permutation of the entries in the diagonal, by the "stars and bars" technique, there are $\binom{(p-2)+m}{m}$ conjugacy classes which contain a diagonal matrix. Since the product of the matrices in an n-tuple must be the identity, a choice of the first $n-1$ entries determines the final matrix. Again using the "stars and bars" technique, we find $\binom{\binom{p+m-2}{m}+n-2}{n-1}$ unordered $(n-1)$-tuples of diagonal matrices whose product is not necessarily the identity. By completing the last entry of these $(n-1)$-tuples, we get our desired set of n-tuples whose product is the identity. However, we are overcounting, as it is possible that at most $n-1$ such n-tuples are equal under permutation, so dividing by $n-1$ yields a lower bound for N. □

As n-tuples in the same conjugacy class are by definition in the same orbit, the number of conjugacy classes in $T_{n,m,p}$ provides an upper bound on the number of orbits. To count the number of such conjugacy classes, we use a known result about the number of conjugacy classes of $\mathrm{GL}_m(\mathbb{F}_p)$.

Lemma 3.4. *[11] The number of conjugacy classes $C_{m,p}$ of $\mathrm{GL}_m(\mathbb{F}_p)$ is given by the generating function*

$$\sum_{m=1}^{\infty} C_{m,p}x^m = \prod_{k=1}^{\infty} \frac{1-x^k}{1-px^k}.$$

Proposition 3.5. *The number of conjugacy classes of n-tuples in $T_{n,m,p}$ is*

$$|C_{m,p}| \cdot |\mathrm{GL}_m(\mathbb{F}_p)|^{n-2}.$$

Proof. For each conjugacy class C of $\mathrm{GL}_m(\mathbb{F}_p)$, pick a representative M_C. This choice gives rise to a representative of each conjugacy class of n-tuples, as we can uniquely write an n-tuple whose first matrix is in the conjugacy class C as $(M_C, A_2, \ldots, A_n)$ for matrices $A_2, \ldots, A_n \in \mathrm{GL}_m(\mathbb{F}_p)$. There are $|C_{m,p}| \cdot |\mathrm{GL}_m(\mathbb{F}_p)|^{n-2}$ tuples of this form, since n-tuples in $T_{n,m,p}$ must multiply to the identity, which determines the final matrix A_n. □

Corollary 3.6. *The number of orbits $c_{n,m,p}$ of the action of the braid group B_n on $T_{n,m,p}$ is bounded above by*

$$c_{n,m,p} \leq |C_{m,p}| \cdot |\mathrm{GL}_m(\mathbb{F}_p)|^{n-2}.$$

The bounds provided in Proposition 3.3 and Corollary 3.6 are not tight, as the lower bound grows as a polynomial function of p, whereas the upper bound is on the order of $p^m \cdot (p^{m^2})^{n-2} = p^{m^2n-2m^2+m}$.

4 The Orbits for $m = 1$

In this section we discuss the orbits of the action of the braid group B_n on n-tuples of 1×1 matrices. As these matrices commute with each other, elements of B_n act by permutation

on n-tuples. Consequently, counting the number of orbits is equivalent to the combinatorial problem of counting how many unordered n-tuples of integers there are from 1 to $p-1$ whose product is 1 modulo p. This problem is surprisingly difficult, and there seems to be no closed-form solution.

Remark. Since for any prime p, there exists a primitive root g such that $\{g, g^2, \ldots, g^{p-1}\} = \{1, 2, \ldots, p-1\}$ modulo p, the orbit number $c_{n,m,p}$ is equivalent to the number of partitions of multiples of $p-1$ with n parts of size less than or equal to $p-1$.

Our computations suggest that the number of orbits is also equivalent to a combinatorial problem of counting *necklaces*, which are arrangements of colored beads considered to be equivalent under rotation.

Conjecture 4.1. *The orbit number $c_{n,m,p}$ is the number of necklaces with n white beads and $p-1$ black beads.*

We provide a bijection between the set of orbits and the set of necklaces for when n and $p-1$ are coprime.

Theorem 4.2. *Suppose* $\gcd(n, p-1) = 1$. *Then the orbit number $c_{n,m,p}$ is the number of necklaces with n white beads and $p-1$ black beads.*

Proof. We construct a bijection between the unordered n-tuples of integers from 1 to $p-1$ whose product is 1 modulo p and the necklaces with n black beads and $p-1$ white beads. Let g be a primitive root modulo p, and let $T := (g^{a_1}, g^{a_2}, \ldots, g^{a_n})$ be an unordered tuple such that $g^{a_1} g^{a_2} \cdots g^{a_n} = 1$. Let the necklace which corresponds to this tuple be $(b, w^{c(1)}, b, w^{c(2)}, b, \ldots, b, w^{c(n)})$ where $c(i)$ denotes the number of occurrences of the element g^i in T. It is easy to see that each necklace has a corresponding tuple. To see that this map is injective, observe that if two tuples correspond to the same necklace, we may write them as $(g^{a_1}, g^{a_2}, \ldots, g^{a_n})$ and $(g^{a_1+k}, g^{a_2+k}, \ldots, g^{a_n+k})$ for some $1 \leq k \leq p-2$. Since the product of each tuple is 1, we have that $g^{nk} = 1$, which is only true if $k = p-1$ when n and $p-1$ are coprime, a contradiction. □

5 The Orbits for $n = 2$

In this section, we discuss the case where the number of punctures n equals 2. We find a closed formula for the number of orbits of $T_{2,2,p}$ and $T_{2,3,p}$, and we provide a method for calculating the number of orbits for $T_{2,m,p}$ for any m given the decomposition of the conjugacy classes of $\mathrm{GL}_m(\mathbb{F}_p)$.

We begin by noting that because tuples in $T_{n,m,p}$ multiply in order to the identity, we can write the final matrix A_n in $(A_1, A_2, \ldots, A_{n-1}, A_n) \in T_{n,m,p}$ as $A_{n-1}^{-1} A_{n-2}^{-1} \cdots A_1^{-1}$. In particular, we can write the tuples of $T_{2,m,p}$ in the form (A, A^{-1}). We discover that the braid group acts by permutation on these tuples, so the length of each orbit is at most 2.

Proposition 5.1. *Let (A, A^{-1}) be an element of $T_{2,m,p}$. Then*

1. $|\mathrm{Orb}((A, A^{-1}))| = 1$ *if* $A^{-1} \in \mathrm{Cl}(A)$;
2. $|\mathrm{Orb}((A, A^{-1}))| = 2$ *if* $A^{-1} \notin \mathrm{Cl}(A)$.

Proof. Suppose $A^{-1} \in \mathrm{Cl}(A)$. Then

$$\begin{aligned}\sigma_1(A, A^{-1}) &= (AA^{-1}A^{-1}, A)\\ &= (A^{-1}, A)\\ &\sim (A, A^{-1}).\end{aligned}$$

In this case, σ_1 acts as the identity, so (A, A^{-1}) is the only element in $\mathrm{Orb}((A, A^{-1}))$.

Now, suppose that $A^{-1} \notin \mathrm{Cl}(A)$. Then, $\sigma_1(A, A^{-1}) = (A^{-1}, A) \not\sim (A, A^{-1})$, so there are at least two elements in $\mathrm{Orb}((A, A^{-1}))$. Since

$$\begin{aligned}\sigma_1^2(A, A^{-1}) &= \sigma_1(A^{-1}, A)\\ &= (A, A^{-1}),\end{aligned}$$

the group element σ_1^2 acts as the identity, and therefore, $\mathrm{Orb}((A, A^{-1}))$ has exactly two elements. □

As $\mathrm{Cl}(A^{-1}) = \{M^{-1} \mid M \in \mathrm{Cl}(A)\}$, a conjugacy class can be identified with its "inverse conjugacy class." The orbits of $T_{n,m,p}$ collapse conjugacy classes with their inverse conjugacy class. Consequently, the number of orbits of $T_{n,m,p}$ under the braid group action is sum of the number of conjugacy classes of $\mathrm{GL}_m(\mathbb{F}_p)$ whose inverse is itself and half of the remaining conjugacy classes. More formally, let

$$C_{\mathrm{inv}} := \{\mathrm{Cl}(A) \mid \mathrm{Cl}(A^{-1}) = \mathrm{Cl}(A), A \in \mathrm{GL}_m(\mathbb{F}_p)\},$$

and let

$$C_{\neg\mathrm{inv}} := \{\mathrm{Cl}(A) \mid \mathrm{Cl}(A^{-1}) \neq \mathrm{Cl}(A), A \in \mathrm{GL}_m(\mathbb{F}_p)\}.$$

Corollary 5.2. *The orbit number $c_{2,m,p}$ is given by*

$$|C_{inv}| + \frac{1}{2}|C_{\neg inv}|.$$

The problem of counting the number of orbits of the action of B_2 on $T_{2,m,p}$ now reduces to identifying the number of conjugacy classes whose inverse conjugacy class is itself. We do this by considering whether the inverse of a representative element of each conjugacy class under the field extension $\mathbb{F}_{p^m}$ is in the same class.

In general, polynomials in $\mathbb{F}_p[x]$ do not factor into linear terms. However, it is known that a polynomial of degree m splits completely under the field extension $\mathbb{F}_{p^m}[x]$. As a Jordan normal form for a matrix exists when its characteristic polynomial factors completely, for any $M \in \mathrm{GL}_m(\mathbb{F}_p)$, there exists $P, J \in \mathrm{GL}_m(\mathbb{F}_{p^m})$ such that $J = PMP^{-1}$ and J is in Jordan normal form. Accordingly, we consider the Jordan normal form representatives for each conjugacy classes in the field extension $\mathrm{GL}_m(\mathbb{F}_{p^m})$.

The distribution of conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$ is a known result, as we here describe.

Lemma 5.3. *[12] The conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$ are given in Table 1, where the count refers to the number of conjugacy classes with a Jordan normal form representative in $\mathrm{GL}_2(\mathbb{F}_{p^2})$ ($a \neq b \in \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$).*

Theorem 5.4. *The number of orbits of the action of the braid group B_2 on $T_{2,2,p}$ is given in Table 2, for $p > 2$.*

Representative	Count
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$p-1$
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$p-1$
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\binom{p-1}{2}$
$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}$	$\frac{p^2-p}{2}$

Table 1: The distribution of conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_p)$.

Representative	# Elements of C_{inv}	# Elements of $C_{\neg inv}$	# Orbits
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	2	$p-3$	$\frac{p+1}{2}$
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	2	$p-3$	$\frac{p+1}{2}$
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$	$\frac{p-1}{2}$	$\frac{p^2-4p+3}{2}$	$\frac{(p-1)^2}{4}$
$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^p \end{pmatrix}$	$\frac{p-1}{2}$	$\frac{p^2-2p+1}{2}$	$\frac{p^2-1}{4}$

Table 2: The number of orbits of $B_2 \curvearrowright T_{2,2,p}$ by conjugacy class.

Proof. We tackle each case individually by finding the number of conjugacy classes whose inverse conjugacy class is itself. Since $X\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)X^{-1} = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ for all $X \in \mathrm{GL}_2(\mathbb{F}_p)$, a matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ is in its inverse class precisely when $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$, which occurs when $a = \pm 1$, so there are 2 conjugacy classes of this type in C_{inv}.

Since the inverse of the matrix $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ is $\left(\begin{smallmatrix} a^{-1} & -a^{-2} \\ 0 & a^{-1} \end{smallmatrix}\right)$ which is conjugate to $\left(\begin{smallmatrix} a^{-1} & 1 \\ 0 & a^{-1} \end{smallmatrix}\right)$, we again find 2 conjugacy classes which are stable under inversion, when $a = \pm 1$.

The only diagonal matrices in $\mathrm{Cl}\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ are $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} b & 0 \\ 0 & a \end{smallmatrix}\right)$, so the inverse of $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ is conjugate to itself when $a = a^{-1}$ and $b = b^{-1}$ or $a = b^{-1}$. Since a and b must be different and order does not matter, we count 1 possibility for the former case (when $a = 1$ and $b = -1$) and $\frac{p-3}{2}$ possibilities for the latter case, which yields $\frac{p-1}{2}$ possibilities in total.

As the inverse of $A := \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^p \end{smallmatrix}\right)$ must also have an irreducible characteristic polynomial and each conjugacy class of this type has a different characteristic polynomial, these conjugacy classes are stable under inversion when the characteristic polynomial is stable under inversion. That is, when

$$\begin{aligned} x^2 - \mathrm{Tr}(A)x + \det(A) &= x^2 - \mathrm{Tr}\big(A^{-1}\big)x + \det\big(A^{-1}\big) \\ &= x^2 - \frac{\mathrm{Tr}(A)}{\det(A)}x + \frac{1}{\det(A)}. \end{aligned}$$

The equations $\mathrm{Tr}(A) = \frac{\mathrm{Tr}(A)}{\det(A)}$ and $\det(A) = \frac{1}{\det(A)}$ hold when either $\det(A) = 1$ or $\mathrm{Tr}(A) = 0$ and $\det(A) = -1$. If the latter were true, the characteristic polynomial would be $x^2 - 1$, which is always reducible for every p. Hence, the number of conjugacy classes which are

Representative	Count	Representative	Count
$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$	$p-1$	$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}$	$(p-1)(p-2)$
$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$	$p-1$	$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$	$\binom{p-1}{3}$
$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$	$p-1$	$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & a \end{pmatrix}$	$\frac{p^2-p}{2} \cdot (p-1)$
$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}$	$(p-1)(p-2)$	$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & \alpha^{p^2} \end{pmatrix}$	$\frac{p^3-p}{3}$

Table 3: The distribution of conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_p)$.

stable under inversion is the number of irreducible polynomials $x^2 + kx + 1$. Since there are p total polynomials of this form and $\frac{p+1}{2}$ distinct possibilities for the value $r + r^{-1}$, which correspond to the possible reducible polynomials $(x - r)(x - r^{-1}) = x^2 - (r + r^{-1})x + 1$, there are $\frac{p-1}{2}$ irreducible polynomials of the form $x^2 + kx + 1$.

Each entry of the second column of Table 2 follows from the first column and Lemma 5.3, and we find the number of orbits for each conjugacy class type in the third column using the formula given in Corollary 5.2. □

We arrive at a formula for the total number of orbits by taking the sum of the third column of Table 2

Corollary 5.5. *The orbit number* $c_{2,2,p} = \frac{p^2+p+2}{2}$*, for* $p > 2$*.*

To find the number of orbits of the action of the braid group B_2 on $T_{2,3,p}$, we perform a similar analysis on the conjugacy classes of $\mathrm{GL}_3(\mathbb{F}_p)$.

Lemma 5.6. *[13] The conjugacy classes of* $\mathrm{GL}_3(\mathbb{F}_p)$ *are given in Table 3, where the count refers to the number of conjugacy classes with a Jordan normal form representative in* $\mathrm{GL}_2(\mathbb{F}_{p^3})$ *($a \neq b \neq c \in \mathbb{F}_p$ and $\alpha \in \mathbb{F}_{p^3} \setminus \mathbb{F}_p$).*

Theorem 5.7. *The number of orbits of the action of the braid group B_2 on $T_{2,3,p}$ is given in Table 4, for $p > 2$.*

Proof. The arguments for the conjugacy classes represented by $\left(\begin{smallmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{smallmatrix}\right)$ are symmetric to the arguments for the conjugacy classes with representatives $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ in Theorem 5.4, so for the sake of concision, we omit the argument here.

Representative	# Elements of C_{inv}	# Elements of $C_{\neg inv}$	# Orbits
$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$	2	$p-3$	$\frac{p+1}{2}$
$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$	2	$p-3$	$\frac{p+1}{2}$
$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$	2	$p-3$	$\frac{p+1}{2}$
$\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}$	2	p^2-3p	$\frac{p^2-3p+4}{2}$
$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & b \end{pmatrix}$	2	p^2-3p	$\frac{p^2-3p+4}{2}$
$\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$	$p-3$	$\frac{p^3-6p^2+5p+12}{6}$	$\frac{p^3-6p^2+17p-24}{12}$
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & a \end{pmatrix}$	$p-1$	$\frac{p^3-2p^2+p-2}{2}$	$\frac{p^3-2p^2+3p-2}{4}$
$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & \alpha^{p^2} \end{pmatrix}$	0	$\frac{p^3-p}{3}$	$\frac{p^3-p}{6}$

Table 4: The number of orbits of $B_2 \curvearrowright T_{2,3,p}$ by conjugacy class.

Since the diagonal matrices in the same conjugacy class as $\left(\begin{smallmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{smallmatrix}\right)$ are just the matrices with a, b, and c permuted and $a \neq b \neq c$, we find without loss of generality that $a = a^{-1}$ and $b = c^{-1}$, of which there are $2 \cdot \frac{p-3}{2} = p - 3$ conjugacy classes of this type whose inverse is itself.

The number of Jordan blocks $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^p \end{smallmatrix}\right)$ which are fixed under inversion is $\frac{p-1}{2}$ by Table 2, and since $a = \pm 1$, there are $\frac{p-1}{2} \cdot 2 = p - 1$ conjugacy classes with representative $\left(\begin{smallmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & a \end{smallmatrix}\right)$ which are stable under inversion.

Following the argument in Theorem 5.4, we find when the characteristic polynomial $p(x) = x^3 + a_2x^2 + a_1x + a_0$ of $\left(\begin{smallmatrix} \alpha & 0 & 0 \\ 0 & \alpha^p & 0 \\ 0 & 0 & \alpha^{p^2} \end{smallmatrix}\right)$ is the same as the characteristic polynomial of its inverse. That is, when

$$x^3 + a_2x^2 + a_1x + a_0 = x^3 + \frac{a_1}{a_0}x^2 + \frac{a_2}{a_0}x + \frac{1}{a_0},$$

which occurs either when $p(x) = x^3 + a_1x^2 + a_1x + 1$ or $p(x) = x^3 - a_1x^2 + a_1x - 1$. In the former case, we have $p(x) = (x+1)(x^2 + (a_1 - 1)x + 1)$, and in the latter, $p(x) = (x-1)(x^2 - (a_1 - 1)x + 1)$. As such, the characteristic polynomial is always reducible, which yields no possible conjugacy classes of this type which are fixed under inversion. □

Corollary 5.8. *The orbit number $c_{2,3,p} = \frac{p^3+p+6}{2}$, for $p > 2$.*

The explicit formulas in Corollary 5.5 and Corollary 5.8 are corroborated by the computational results in Table 7, which can be found in Appendix A.

In general, given a Jordan normal form representative which has at least two Jordan blocks from a conjugacy class of $\mathrm{GL}_m(\mathbb{F}_p)$, we can deduce the number of conjugacy classes which are stable under inversion by taking the product of the number of stable conjugacy classes for each Jordan block, which have smaller dimension. This gives us a recursive procedure for creating all entries of an orbit decomposition table of $B_2 \curvearrowright T_{2,m,p}$ by conjugacy class (except for when there is a single Jordan block with roots in the field extension) based on orbit decomposition tables for smaller m. If the dimension m is odd, we provide a formula for the number of orbits of the conjugacy classes with one Jordan block with roots in the field extension.

Proposition 5.9. *Let C_α be the conjugacy class in $\mathrm{GL}_m(\mathbb{F}_p)$ whose elements are conjugate to the representative*

$$A_\alpha := \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \alpha^{p^m} \end{pmatrix}$$

in the field extension $\mathbb{F}_{p^m}$. There are $\frac{p^m-p}{2m}$ orbits in $T_{2,m,p}$ under the action of the braid group B_n whose elements are of the form (A, A^{-1}) where $A \in C_\alpha$ for any $\alpha \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$.

Proof. We first note that there are $\frac{p^m-p}{m}$ conjugacy classes C_α, since we have $p^m - p$ choices of $\alpha \in \mathbb{F}_{p^m} \setminus \mathbb{F}_p$, but we divide by m, as for each α, the choice α^{p^i} corresponds to the same conjugacy class. It is known that given A_α's characteristic polynomial

$$\chi(A_\alpha) := x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0,$$

the characteristic polynomial of A_α^{-1} is given by

$$\chi(A_\alpha^{-1}) := x^m + \frac{a_1}{a_0}x^{m-1} + \cdots + \frac{a_{m-1}}{a_0}x + \frac{1}{a_0}.$$

As a result, C_α is stable under inversion when the following equations hold:

$$\begin{aligned} a_0 &= \frac{1}{a_0}, \\ a_1 &= \frac{a_{m-1}}{a_0}, \\ &\vdots \\ a_{m-1} &= \frac{a_1}{a_0}. \end{aligned}$$

As $a_0 = \pm 1$, we have two cases. If $a_0 = 1$, then we have

$$\begin{aligned} \chi(A_\alpha) = \chi(A_\alpha^{-1}) &= x^m + a_1x^{m-1} + a_2x^{m-2} + \cdots + a_2x^2 + a_1x + 1 \\ &= (x^m + 1) + a_1x(x^{m-2} + 1) + a_2x^2(x^{m-4} + 1) + \cdots + a_{\frac{m-1}{2}}x^{\frac{m-1}{2}}(x + 1) \\ &= (x + 1)\left(\sum_{k=0}^{m-1}(-x)^k + a_1x\sum_{k=0}^{m-3}(-x)^k + a_2x^2\sum_{k=0}^{m-5}(-x)^k + \cdots + a_{\frac{m-1}{2}}x^{\frac{m-1}{2}}\right) \end{aligned}$$

and if $a_0 = -1$, then we have

$$\begin{aligned} \chi(A_\alpha) = \chi(A_\alpha^{-1}) &= x^m - a_1x^{m-1} - a_2x^{m-2} - \cdots + a_2x^2 + a_1x - 1 \\ &= (x^m - 1) - a_1x(x^{m-2} - 1) - a_2x^2(x^{m-4} - 1) - \cdots - a_{\frac{m-1}{2}}x^{\frac{m-1}{2}}(x - 1) \\ &= (x - 1)\left(\sum_{k=0}^{m-1}x^k - a_1x\sum_{k=0}^{m-3}x^k - a_2x^2\sum_{k=0}^{m-5}x^k - \cdots - a_{\frac{m-1}{2}}x^{\frac{m-1}{2}}\right). \end{aligned}$$

Either way, the characteristic polynomial is reducible, which is a contradiction. Thus, there are no conjugacy classes C_α which are fixed under inversion. Thus, all $\frac{p^m-p}{m}$ conjugacy classes move under the braid group action B_2, so there are $\frac{p^m-p}{2m}$ orbits in $T_{2,m,p}$ of the form (A, A^{-1}) for some $A \in C_\alpha$. □

For odd m, given the orbit decomposition tables for $B_2 \curvearrowright T_{2,k,p}$ for $k < m$, we can now count the orbits of $B_2 \curvearrowright T_{2,m,p}$ given the distribution of conjugacy classes of $\mathrm{GL}_m(\mathbb{F}_p)$.

6 The Orbits for $n = 3$

In this section, we consider the case when the number of matrices n equals 3. We provide a bound on the lengths of orbits and classify the numbers and lengths of the orbits generated by n-tuples of 2×2 matrices which contain matrices of the form $a \cdot \mathrm{Id}$ where $a \in \mathbb{F}_p$.

We begin with a description of the orbits $T_{3,2,2}$ under the action of the braid group B_3.

Example 6.1. There are 6 elements in $\mathrm{GL}(2, \mathbb{F}_2)$, generated by two elements (which we call σ and τ):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \sigma\tau\sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \sigma\tau = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Representative	Count
$(1,1,1)$	1
$(1,\sigma\tau,\tau\sigma)$	2
$(\sigma\tau,1,\tau\sigma)$	2
$(\sigma\tau,\tau\sigma,1)$	2
$(\sigma\tau,\sigma\tau,\sigma\tau)$	2
$(1,\sigma,\sigma)$	3
$(\sigma,1,\sigma)$	3
$(\sigma,\sigma,1)$	3
$(\sigma,\sigma\tau,\tau)$	6
$(\sigma,\tau,\tau\sigma)$	6
$(\tau\sigma,\sigma,\tau)$	6

Table 5: The conjugacy classes of $T_{3,2,2}$.

Orbits				
$(1,1,1)$	$(1,\sigma\tau,\tau\sigma)$ $(\sigma\tau,1,\tau\sigma)$ $(\sigma\tau,\tau\sigma,1)$	$(\sigma\tau,\sigma\tau,\sigma\tau)$	$(1,\sigma,\sigma)$ $(\sigma,1,\sigma)$ $(\sigma,\sigma,1)$	$(\sigma,\sigma\tau,\tau)$ $(\sigma,\tau,\tau\sigma)$ $(\tau\sigma,\sigma,\tau)$

Table 6: The orbits of $B_3 \curvearrowright T_{3,2,2}$.

Observe that this group is isomorphic to S_3, and our generators σ, τ are transpositions. There are 3 conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_2)$: (Id), $(\sigma, \tau, \sigma\tau\sigma)$, and $(\sigma\tau, \tau\sigma)$.

As illustrated in Table 5, there are 36 ordered triples of elements in $\mathrm{GL}_2(\mathbb{F}_2)$ whose product is the identity, but only 11 equivalence classes under conjugation.

Under the action of B_3, these 11 conjugacy classes collapse into 5 orbits, as shown in Table 6.

When $p > 2$, there are a substantial number of cases when one of the matrices of the 3-tuple contains a matrix of the form $a \cdot \mathrm{Id}$. We turn to describe the orbit counts and lengths for some of these cases.

Theorem 6.1. *Let $(A, B, B^{-1}A^{-1}) \in T_{3,2,p}$ such that $A = a \cdot \mathrm{Id}$ for some $a \in \mathbb{F}_p$. Let OL_ℓ denote the number of orbits of length ℓ. The following are true:*

1. *Suppose $B = b \cdot \mathrm{Id}$ for some $b \in \mathbb{F}_p$. Then,*

$$\begin{cases} OL_1 = 3, OL_3 = p-4 & \text{if } p \equiv 1 \mod 3 \\ OL_1 = 1, OL_3 = p-2 & \text{if } p \equiv 2 \mod 3 \end{cases}$$

   and $OL_6 = \frac{(p-2)(p-3}{6}$.

2. *Suppose B is conjugate to $\left(\begin{smallmatrix} b & 1 \\ 0 & b \end{smallmatrix}\right)$ for some $b \in \mathbb{F}_p$. Then, $OL_1 = 0$, $OL_3 = p-1$, and $OL_6 = \frac{(p-1)(p-2)}{2}$.*

It is not only the case that the lengths of the orbits are either 1,3, or 6 when one of the matrices in the triple is of the form $a \cdot \mathrm{Id}$. In fact, for triples of matrices in $T_{3,m,p}$, orbits can only have length 1, 3, or 6.

Theorem 6.2. *Let* $(A_1, A_2, A_2^{-1}A_1^{-1}) \in T_{3,m,p}$. *Then* $|\mathrm{Orb}((A_1, A_2, A_2^{-1}A_1^{-1}))| \in \{1, 3, 6\}$.

Proof. Using Lemma 3.1(1), we find that

$$\begin{aligned}\sigma_1^2(A_1, A_2, A_2^{-1}A_1^{-1}) &= (A_1A_2A_1A_2^{-1}A_1^{-1}, A_1A_2A_1^{-1}, A_2^{-1}A_1^{-1}) \\ &\sim (A_2A_1A_2, A_2, A^{-1}A_2^{-1}) \\ &\sim (A_1, A_2, A_2^{-1}A_1^{-1})\end{aligned}$$

and

$$\begin{aligned}\sigma_2^2(A_1, A_2, A_2^{-1}A_1^{-1}) &= (A_1, A_1^{-1}A_2A_1, A_1^{-1}A_2^{-1}) \\ &\sim (A_1, A_2, A_2^{-1}A_1^{-1}).\end{aligned}$$

Therefore, $\sigma_1^2 = \sigma_2^2 = 1$ when we consider the action of the braid group B_3 on tuples in $T_{3,m,p}$. As a result, since $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$, there are at most 6 unique braid actions: $B_3 = \{1, \sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1\}$, which implies that there are at most 6 elements in any orbit.

If there are less than 6 elements in $\mathrm{Orb}((A_1, A_2, A_2^{-1}A_1^{-1}))$, then one of the braid group actions $\sigma_1, \sigma_2, \sigma_1\sigma_2, \sigma_2\sigma_1, \sigma_1\sigma_2\sigma_1$ must act as the identity. If $\sigma_1\sigma_2\sigma_1 = 1$, then $\sigma_2\sigma_1\sigma_2 = 1$ as well, so $\sigma_1 = \sigma_2 = 1$, which implies that $|\mathrm{Orb}((A_1, A_2, A_2^{-1}A_1^{-1}))| = 1$. If $\sigma_1 = 1$, then $B_3 = \{1, \sigma_2, \sigma_1\sigma_2\}$. In this case, if either $\sigma_2 = 1$ or $\sigma_1\sigma_2 = 1$, then $B_3 = \{1\}$, so we must have $|\mathrm{Orb}((A_1, A_2, A_2^{-1}A_1^{-1}))| \in \{1, 3\}$. The proof is symmetric the case when σ_2 acts as the identity. □

Using the upper bound of 6 on the length of orbits in $T_{3,m,p}$ in conjunction with upper bound of the number of conjugacy classes of triples of matrices as formulated in Proposition 3.5, we arrive at a tight bound on the number of orbits of the braid group action on $T_{3,m,p}$.

Corollary 6.3. *The number of orbits* $c_{3,m,p}$ *of the action of the braid group* B_3 *on* $T_{3,m,p}$ *is bounded as follows:*

$$\frac{1}{6}|C_{m,p}| \cdot |\mathrm{GL}_m(\mathbb{F}_p)| \leq c_{3,m,p} \leq |C_{m,p}| \cdot |\mathrm{GL}_m(\mathbb{F}_p)|.$$

In Section 5, we found that the length of any orbit of $T_{2,m,p}$ is at most 2, so that the number of orbits for $n = 2$ is bounded below by half of the number of conjugacy classes. For both $n = 2$ and $n = 3$, computational data (Table 7 and Table 8 in Appendix A) suggest that as p grows large, the ratio of the number of conjugacy classes to the number of orbits of $T_{n,m,p}$ approaches $n!$. Intuitively, this means that most of the orbits of $T_{n,m,p}$ have maximal length (2 when $n = 2$ and 6 when $n = 3$).

Conjecture 6.4. *Suppose* $n = 2$ *or* $n = 3$, *and fix* m. *Then,*

$$\lim_{p\to\infty} \frac{C(T_{n,m,p})}{c_{n,m,p}} = n!,$$

where $C(T_{n,m,p})$ *denotes the number of conjugacy classes of* n*-tuples of matrices in* $T_{n,m,p}$.

We also propose a generalization of this conjecture, but we are less confident about its validity, because it is unclear whether the action of the braid group B_n on the n-tuples of matrices $T_{n,m,p}$ is finite for $n \geq 4$. Even for $n = 4$, we do not have enough computational data to trust that this conjecture generalizes.

Conjecture 6.5. *Fix n and m. Then,*

$$\lim_{p\to\infty} \frac{C(T_{n,m,p})}{c_{n,m,p}} = n!,$$

where $C(T_{n,m,p})$ denotes the number of conjugacy classes of n-tuples of matrices in $T_{n,m,p}$.

We conclude with the observation that the results Proposition 5.1, Theorem 6.2, and Corollary 6.3 do not depend on the dimensions of our matrices or which field they belong to. In fact, these results generalize to give us a bound on the lengths and numbers of orbits of rank m K-local systems with 2 and 3 punctures, where K describes an arbitrary field, such as $\mathbb{R}, \mathbb{C}$, or $\mathbb{F}_q$.

7 Conclusion

For small cases, we have managed to provide a strategy in which we can classify the orbits of n-tuples of matrices in $\mathrm{GL}_m(\mathbb{F}_p)$ under the action of the braid group. However, it seems that our strategies are insufficient for a complete classification when $n \geq 3$. For example, one question left for future work is to identify the necessary and sufficient conditions for when the length of a given orbit is $1, 3$, or 6. Another possible question would be to carry on the classification for $n = 4$, which is the case that generalizes the Painlevé VI equation.

8 Acknowledgments

I kindly thank my mentor Yonghwan Kim for his invaluable guidance, patience, and dedication throughout the research process. I would like to thank Dr. Aaron Landesmann for suggesting this project, and Professor Paul Seidel for helpful comments. I would like to thank Dr. Tanya Khovanova for her insightful feedback on early renditions of my paper. I am also grateful towards Professor David Jerison and Dr. Jonathan Bloom for their thoughtful suggestions on how to present my work. In addition, I extend my gratitude to my tutor Dr. Jenny Sendova for her countless words of advice throughout the program. I am grateful to Allen Lin and Victor Kolev for listening to me explain my research and providing feedback on the flow of my paper. Lastly, I am thankful to RSI, CEE, MIT, my sponsor Sam Leung, and my funding organization D.E. Shaw & Co., L.P. for making this opportunity possible.

References

[1] B. Farb and D. Margalit. *A Primer on Mapping Class Groups*. Princeton Univ. Press, 2011.

[2] W. M. Goldman. Mapping class group dynamics on surface group representations. *Proceedings of Symposia in Pure Mathematics*, p. 189–214, 2006. doi:10.1090/pspum/074/2264541.

[3] M. Khovanov and P. Seidel. Quivers, Floer cohomology, and braid group actions. *Journal of the American Mathematical Society*, 15(1):p. 203–271, 2001. doi:10.1090/s0894-0347-01-00374-5.

[4] D. Litt. Motives, mapping class groups, and monodromy. *Current Developments in Mathematics*, 2024. *To appear*.

[5] Y.-W. Fan and J. P. Whang. Stokes matrices and exceptional isomorphisms. *Mathematische Annalen*, 2024. doi:10.1007/s00208-024-02850-8.

[6] Y. H. J. Lam, A. Landesmann, and D. Litt. Finite braid group orbits on $\mathfrak{sl}_2$-character varieties. *https://arxiv.org/abs/2308.01376*, 2023.

[7] A. Landesman and D. Litt. Canonical representations of surface groups. *Annals of Mathematics*, 199(2), 2024. doi:10.4007/annals.2024.199.2.6.

[8] A. N. Shankar. The p-curvature conjecture and monodromy around simple closed loops. *Duke Mathematical Journal*, 167(10), 2018. doi:10.1215/00127094-2018-0008.

[9] J. P. Whang. Global geometry on moduli of local systems for surfaces with boundary. *Compositio Mathematica*, 156(8):p. 1517–1559, 2020. doi:10.1112/s0010437x20007241.

[10] B. Dubrovin and M. Mazzocco. Monodromy of certain painlevé–vi transcendents and reflection groups. *Inventiones mathematicae*, 141(1):p. 55–147, 2000. doi:10.1007/pl00005790.

[11] K. S. (https://math.stackexchange.com/users/404616/kenta s). Conjugacy classes in matrix groups $\mathrm{GL}_n(k)$ and rings $m_n(k)$. Mathematics Stack Exchange. URL `https://math.stackexchange.com/q/4357113`. URL:https://math.stackexchange.com/q/4357113 (version: 2022-01-15), `https://math.stackexchange.com/q/4357113`.

[12] H. Cooper. The conjugacy classes of $\mathrm{GL}(2, \mathbb{F}_q)$. URL `https://math.mit.edu/~dav/gl2conj.pdf`.

[13] M. a. Ali, C. Hering, and J. Schäeffer. On the conjugacy classes of the general linear group $\mathrm{GL}(3, q)$. *Bulletin Mathématique de La Société Des Sciences Mathématiques de Roumanie*, 38(86):pp. 105–111, 1994.

A Computations of Conjugacy Classes and Orbits

Using depth-first search in the programming language Julia, we computationally find the number of conjugacy classes and orbits when 2-, 3-, 4-, and 5-tuples of $m \times m$ matrices with entries in $\mathbb{F}_p$ for small values of m and p. Specifically, we list [# conjugacy classes]/[# orbits] for $T_{2,m,p}$ in Table 7, for $T_{3,m,p}$ in Table 8, $T_{4,m,p}$ in Table 9, and $T_{5,m,p}$ in Table 10.

$p \setminus m$	2	3
2	3/3	6/5
3	8/7	24/18
5	24/16	120/-
7	48/29	
11	120/67	

Table 7: Conjugacy classes and orbits when $n = 2$.

$p \setminus m$	2	3
2	11/5	197/53
3	136/36	
5	2336/451	

Table 8: Conjugacy classes and orbits when $n = 3$.

$p \setminus m$	2
2	49/9
3	4888/-

Table 9: Conjugacy classes and orbits when $n = 4$.

$p \setminus m$	2
2	251/12

Table 10: Conjugacy classes and orbits when $n = 5$.