TOPOLOGICAL ENTROPY OF SIMPLE BRAIDS

LUKE ROBITAILLE

Abstract. Mathematical objects called *braids* are formed from "strands" (like string or yarn) that intertwine. A certain collection of braids, called *simple braids*, correspond to permutations, depending on how the strands get permuted. We can think of braids as maps from a disc with some "punctures" to itself; using this idea, we can consider the *topological entropy* of a braid, which can be zero or positive. What proportion of simple braids have positive topological entropy? The main theorem of this project is that, in the limit as the number of strands increases, the proportion of simple braids that have positive topological entropy approaches 1. This can be proved by showing that we can almost always find a long cycle in the permutation that will enable us to get a braid with three strands that has positive topological entropy, yielding the theorem. Topological entropy of braids can have use beyond just being interesting mathematics, such as for considering how to stir fluids.

1. Introduction

Braids are important objects in mathematics, especially topology. What are braids? Informally, a braid is composed of some *strands* (like pieces of string or yarn) that intertwine with one another, where we only care about how they intertwine, not about exactly where they are positioned. (We will think of these strands as oriented vertically.)

For a positive integer n, the braids on n strands form a group, where the product $\beta_1\beta_2$ of two braids β_1 and β_2 is formed by putting β_1 above β_2 and then joining the ends of the strands at the bottom of β_1 with the ends of the strands at the top of β_2. We will call this group B_n. Another way to think about the group B_n is as the group generated by $n-1$ elements $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geq 2$ and $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for i with $1 \leq i \leq n-2$. Here σ_i is a braid in which a strand going directly from position $i+1$ on top to position i on the bottom passes in front of a strand going directly from position i on the top to position $i+1$ on the bottom, while a strand goes directly from position j on the top to position j on the bottom for $j \neq i, i+1$.

There is a natural map from B_n to S_n (the group of permutations of $\{1, \ldots, n\}$) in which σ_i maps to the transposition swapping i and $i+1$. There is a certain collection of $n!$ braids, the *simple braids*, that are natural preimages for the $n!$ elements of S_n. The simple braids are useful for solving group-theoretic computational problems in B_n, as discussed by Elrifai and Morton [3]. One important simple braid is the *half twist*, which corresponds to the permutation $i \mapsto n+1-i$. The square of the half twist, the *full twist*, generates the center of B_n for $n \geq 3$.

Another way to look at elements of B_n is as maps from a disk with n punctures to itself. (This is in a topological sense, so it is imprecise to say "maps"; "equivalence

Date: January 22, 2022.

classes of maps" is more accurate.) For example, the full twist yields the identity map on the punctured disk. This perspective lets us look at how a braid acts on "loops" that we could draw around some of the strands. Then we can look at how iterating the map acts on loops; by doing so, we can define the *topological entropy* of a braid; this will be a nonnegative real number. Topological entropy is related to real-world considerations involving mixing fluids.

This perspective of braids as maps of a punctured disk also relates to the *Nielsen-Thurston classification*. In the Nielsen-Thurston classification, braids are classified as *periodic*, *reducible* and not periodic, or *pseudo-Anosov*. A braid is *periodic* when the map of the punctured disk can be raised to some positive integer power to give the identity map; equivalently, a braid is periodic when some positive integer power of the braid equals some integer power of the full twist. (For example, the half twist is periodic.) A braid is *reducible* when there exists some family of nontrivial (i.e. enclosing at least two punctures, but not all of them), pairwise nonintersecting loops that is fixed under the action of the braid. (The action of the braid is allowed to permute the loops.) In such a case, we can think of the loops as "tubes," and then we have "reduced" the braid into the braid formed by the outside strands and the tubes, where we treat the tubes as strands, and the braids inside the tubes, so the name "reducible" makes sense. A *pseudo-Anosov* braid is a braid that is not periodic or reducible. (This is not the way that "pseudo-Anosov" is usually defined, but the usual definition is technical and unnecessary for our purposes.)

The Nielsen-Thurston classification is related to topological entropy. Specifically, periodic braids have topological entropy zero, and reducible braids that can, in a certain sense, be reduced into components that are all periodic, have topological entropy zero. On the other hand, pseudo-Anosov braids have positive topological entropy, as do the reducible braids that are not of the form in the previous sentence.

Our main theorem investigates when simple braids have positive topological entropy.

Theorem 1. *The proportion of simple braids in B_n that have positive topological entropy is $1 - o(1)$.*

Similar results have been proved in the past, but those results were concerned with the braid group on a fixed number of strands, and they considered braids which were the product of many factors, instead of considering the simple braids on a varying number of strands.

We also determine expressions for the images of the simple braids under a homomorphism, the *reduced Burau representation*, from B_n to $GL_{n-1}(\mathbb{Z}[t, t^{-1}])$. The Burau representation is related to the topological entropy of braids by a result of Fried and Kolev [5, 6].

Theorem 2. *For $n \geq 2$, suppose that $\beta \in B_n$ is a simple braid corresponding to the permutation π. Then we can explicitly determine the entries of the image of β under the Burau representation. Namely, consider arbitrary i and j with $1 \leq i, j \leq n-1$. Let u be the number of $k \in \{1, \ldots, n\}$ such that $k > j$ and $\pi^{-1}(k) \leq i$. (We let π^{-1} be the inverse of π.) Let $a_{i,j}$ be the (i, j) entry (i.e., in the ith row and jth column) of the image of β under the Burau representation. Then:*

- *if $\pi^{-1}(j) \leq i < \pi^{-1}(j+1)$, then $a_{i,j} = t^u$;*
- *if $\pi^{-1}(j+1) \leq i < \pi^{-1}(j)$, then $a_{i,j} = -t^u$;*
- *otherwise, $a_{i,j} = 0$.*

Section 2 gives technical background information. Section 3 contains the proof of Theorem 1, proceeding, as follows. Subsection 3.1 shows how, if we delete a strand from a braid of topological entropy zero, the resulting braid still has topological entropy zero; this lets us focus on one "cycle" of a braid. Subsection 3.2 contains a useful combinatorial result; roughly, as n grows large, almost all permutations in S_n have many long cycles with length divisible by 3. Subsection 3.3 lets us get a useful three-strand braid from a simple braid corresponding to a $3m$-cycle. Subsection 3.4 shows that at least a fixed positive proportion of a certain family of three-strand braids have positive topological entropy. Finally, Subsection 3.5 combines these results to prove Theorem 1. Section 4 contains the proof of Theorem 2. Section 5 presents further directions for potential future work.

2. Background

The braid group is a standard mathematical object.

Definition 1. For a positive integer n, the *braid group on n strands* is the group generated by $n-1$ elements $\sigma_1, \ldots, \sigma_{n-1}$ subject to the relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geq 2$ and $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for i with $1 \leq i \leq n-2$.

Let ι be the identity element of B_n.

Definition 2. A braid is *positive* if it is the product of zero or more elements of the form σ_i.

The braid group B_n is isomorphic to a certain *mapping class group* of a disk. To make this group, we fix a set of n points $P_1, \ldots, P_n$ inside the disk. Then we consider orientation-preserving homeomorphisms from the disk to itself that fix the boundary pointwise and permute the set of P_i's. An element of the mapping class group that we wish to consider is an equivalence class of such maps, where two maps are equivalent if there is some map yielding an isotopy between them such the map fixes the boundary pointwise and fixes each P_i. To get the isomorphism, σ_i corresponds to switching P_i and P_{i+1} by moving them in a clockwise direction relative to one another as seen from above. This relates to seeing braids as having strands: we can make the points be in a row in order from P_1 on the left to P_n on the right and let the point that starts as P_i move as the strand that starts at position i moves as it goes from top to bottom. For a reference, see Farb and Margalit [4].

It will be useful to define Γ_n to be the map that sends any homeomorphism f of the disk that fixes the boundary pointwise and permutes the set of P_i's to the braid corresponding to the isotopy class of f in the mapping class group.

Let S_n be the group of permutations of $\{1, \ldots, n\}$ where multiplication is function composition (this is the *symmetric group*). We will compose functions left to right (so our convention for multiplication in S_n is the opposite of some sources' convention).

Definition 3. Let $\mu_n : B_n \to S_n$ be the group homomorphism such that, for $i = 1, \ldots, n-1$, we have that $\mu_n(\sigma_i)$ is the transposition τ_i swapping i and $i+1$.

Note that this homomorphism is well-defined, as $\tau_i\tau_j = \tau_j\tau_i$ for $|i-j| \geq 2$ and $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ for i with $1 \leq i \leq n-2$.We will usually abuse notation and refer to μ_n simply as μ. Note that in a braid β, the strand that starts at position i on the top ends at position $(\mu(\beta))(i)$ on the bottom.

There is more than one way to define simple braids. We follow the approach of Elrifai and Morton [3].

Definition 4. A *simple* braid is a positive braid that can be drawn so any two strands cross at most once.

(In [3] these are called "positive permutation braids.") Then Lemma 2.3 of [3] and its proof give the following.

Proposition 3. *For every permutation $p \in S_n$, there exists a unique simple braid β with $\mu(\beta) = p$. Moreover, any simple braid can be drawn so that whenever two strands cross, the strand that goes from being right on top to being left on bottom is in front of the other strand. (In* [3] *such a crossing is called a positive crossing.)*

Note that Proposition 3 gives a natural bijection between simple braids and elements of S_n.

As any braid in which all crossings are positive crossings is a positive braid by definition (a fact which [3] uses in proving their Lemma 2.3), we have the following result.

Proposition 4. *If we ignore some of the strands of a simple braid such that at least one strand remains and the remaining strands form a valid braid (i.e. the set of starting positions is the same as the set of ending positions), then this braid is a simple braid.*

Proof. Drawing the original braid as described in Proposition 3, the desired is immediate by definition. ☐

We also have the following result, which follows from Elrifai and Morton [3].

Proposition 5. *If we consider the $n!$ braids $(\sigma_{i_1} \cdot \cdots \cdot \sigma_2 \cdot \sigma_1) \cdot (\sigma_{i_2} \cdot \cdots \cdot \sigma_2) \cdot \cdots \cdot (\sigma_{i_{n-1}} \cdot \cdots \cdot \sigma_{n-1})$ where $j-1 \leq i_j \leq n-1$ for all j, then these braids are all simple braids, and they give every simple braid in B_n exactly once.*

Let the *half twist* be the simple braid corresponding to the permutation $i \mapsto n+1-i$, and let the *full twist* Φ be its square.

Definition 5. A braid β is *periodic* if $\beta^k = \Phi^m$ for some positive integer k and some integer m.

Adler, Konheim, and McAndrew [1] introduced the concept of topological entropy. This is a nonnegative real number assigned to a map from a compact topological space to itself. (The actual definition of topological entropy is technical and not needed for our purposes; we will only care about when it is zero or not.) Then we can consider the topological entropy of a braid as being the infimum of the topological entropies of the maps in the isotopy class in the mapping class group that corresponds to the braid.

We use certain standard properties of topological entropy.

Proposition 6. *(a) (from* [1]*) For a map β from a compact topological space to itself and a positive integer m, entropy$(\beta^m) = m \cdot$ entropy(β). (It follows directly that entropy$(\beta^k) \leq k \cdot$ entropy(β) for a braid β.)*

(b) The entropy of the identity braid is zero.

(c) (from [1]*) If two maps are conjugate, then they have the same entropy.*

Proof of part (b). Part (b) follows readily from part (a): by taking β to be the identity map in part (a), we get that the identity map has entropy zero; then the identity braid's entropy is at most that of the identity map, and is nonnegative, and thus is zero. □

We have a homomorphism from the braid group to $GL_{n-1}(\mathbb{Z}[t, t^{-1}])$. This is the *reduced Burau representation*. Specifically, it sends σ_i to the matrix whose (j, k) entry is t if $(j, k) = (i, i-1)$, $-t$ if $(j, k) = (i, i)$, 1 if $(j, k) = (i, i+1)$, and δ_{jk} otherwise. For example, for the reduced Burau representation of B_5, we have $\sigma_3 \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & t & -t & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$. Call this map ρ_n. We will usually abuse notation and just call it ρ.

We have the following result, due to Fried and Kolev [5, 6].

Proposition 7. *Let $\beta \in B_n$ be a braid. For any complex number z with $|z| = 1$, we can consider the maximum magnitude of the eigenvalues of $\rho_n(\beta)$ if we set $t = z$. Let λ be the supremum of this value over all such z. Then the natural logarithm of the entropy of β is greater than or equal to λ.*

Their result was actually for the so-called unreduced Burau representation, which is slightly different, but the unreduced Burau representation is isomorphic to a direct sum of the reduced Burau representation and a trivial one-dimensional representation (see Section 1.3 of Turaev [10]), so their result is equivalent to the result we want.

3. Proof of Theorem 1

3.1. **Deleting strands from braids.** Let β be a braid. Consider the cycle decomposition of the permutation $\mu(\beta)$. Suppose we have a cycle $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$. Then the set of strands starting at one of $a_1, \ldots, a_k$ is the same as the set of strands ending at one of $a_1, \ldots, a_k$, so we can consider just those strands to form a braid. (It is not hard to see that doing so is well-defined.) Call this braid β'.

Proposition 8. *If we take β and β' as in the previous paragraph, if β has topological entropy zero, then β' has topological entropy zero.*

Proof. We can consider $D^2 - \{p_{a_1}, \ldots, p_{a_k}\}$ to be D_k. Then, for any orientation-preserving homeomorphism f of D^2 that fixes ∂D_n pointwise with $\Gamma_n(f) = \beta$, we will have that f fixes ∂D_k pointwise and $\Gamma_k(f) = \beta'$, so the entropy of β' is less than or equal to the entropy of f. As β has entropy zero, we can choose f with arbitrarily small nonnegative entropy; thus β' has entropy zero, as desired. □

3.2. **Some combinatorial results about cycles of permutations.** (In this section we are manipulating formal power series; we do not care about convergence or lack thereof.)

We make use of the following result, which is equation 5.30 from Enumerative Combinatorics, Volume 2 by Richard P. Stanley [9].

Proposition 9. *Let t_i be an indeterminate for all positive integers i. For every permutation π in S_n, if π has c_1 cycles of length 1, c_2 cycles of length 2, $\ldots$, c_n*

cycles of length n, then let $Z(\pi) = t_1^{c_1} t_2^{c_2} \dots t_n^{c_n}$. Let $\tilde{Z}(S_n) = \sum_{\pi \in S_n} Z(\pi)$. Let x be an indeterminate. Then

$$\sum_{n \geq 0} \tilde{Z}(S_n) \frac{x^n}{n!} = \exp\left(\sum_{i \geq 1} t_i \frac{x^i}{i} \right).$$

We will also need some simple inequalities.

Lemma 10. *Let $x \in [0,1]$ be a real number. For any nonnegative integer i, we have that $\binom{-x}{i}(-1)^i \geq 0$. Also, for all nonnegative integers i, we have that $\binom{-x}{i}(-1)^i \leq 2\binom{-x}{2i}(-1)^{2i}$.*

Proof. The first sentence is clear, as $\binom{-x}{i}(-1)^i = \frac{x(x+1)\dots(x+i-1)}{i!} \geq 0$. As for the second sentence, it's clear for $i = 0$ or $x = 0$; for $i > 0$ and $x > 0$, we need $1 \leq \frac{2(x+i)(x+i+1)\dots(x+2i-1)}{(i+1)\dots(2i)}$, which holds, as the right hand side equals $\frac{x+i+1}{i+1} \cdot \dots \frac{x+2i-1}{2i-1} \cdot \frac{2(x+i)}{2i}$, and every fraction in that product is greater than 1. □

Lemma 11. *If $p_0, p_1, p_2, \dots$ are nonnegative real numbers and $q_0, q_1, \dots, r_0, r_1, \dots$ are real numbers with $q_i \leq r_i$ for all i, then each coefficient of $(\sum_{j=0}^{\infty} p_j x^j)(\sum_{j=0}^{\infty} q_j x^j)$ is less than or equal to the corresponding coefficient of $(\sum_{j=0}^{\infty} p_j x^j)(\sum_{j=0}^{\infty} r_j x^j)$.*

Proof. This is clear, as $\sum_{j=0}^{k} p_j q_{k-j} \leq \sum_{j=0}^{k} p_j r_{k-j}$ for all k, as $p_j q_{k-j} \leq p_j r_{k-j}$ for all j and k with $0 \leq j \leq k$. □

The following result is standard; see [7], for example.

Lemma 12. *For a fixed real number a that is not a nonnegative integer,*

$$\binom{a}{n} = \Theta\left(\frac{(-1)^n}{\Gamma(-a) n^{1+a}} \right).$$

We can now show the following result.

Lemma 13. *Let k be a positive integer. Then the proportion of permutations of $\{1, \dots, n\}$ that have no cycle with length of the form $k(2m+1)$ for nonnegative integer m (i.e., no cycles of length $k, 3k, 5k, \dots$) is $O(n^{-1/(2k)})$.*

Proof. Let a_n be the number of such permutations of $\{1, \dots, n\}$, and let $c_n = \frac{a_n}{n!}$. Setting $t_{k(2m+1)} = 0$ for all nonnegative integers m and $t_i = 1$ for all other i in Proposition 9, we get

$$\sum_{n \geq 0} \frac{a_n}{n!} x^n = \exp\left(\sum_{i \geq 1, i \not\equiv k \pmod{2k}} \frac{x^i}{i} \right).$$

The right-hand side is equal to

$$\exp\left(\sum_{i \geq 1} \frac{x^i}{i} - \sum_{i \geq 1} \frac{x^{ki}}{ki} + \sum_{i \geq 1} \frac{x^{2ki}}{2ki} \right),$$

which equals $(1-x)^{-1}(1-x^k)^{1/k}(1-x^{2k})^{-1/(2k)}$. Thus we have that

$$\sum_{n \geq 0} \frac{a_n}{n!} x^n = (1-x)^{-1}(1-x^k)^{1/k}(1-x^{2k})^{-1/(2k)}.$$

Now

$$\begin{aligned}(1-x)^{-1}(1-x^k)^{1/k} &= (1+x+\cdots+x^{k-1})(1-x^k)^{(1/k)-1}\\ &= (1+x+\cdots+x^{k-1})\sum_{i\geq 0}\binom{(1/k)-1}{i}(-1)^i x^{ik};\end{aligned}$$

now both of the factors in that last product have nonnegative coefficients by Lemma 10, so $(1-x)^{-1}(1-x^k)^{1/k}$ has nonnegative coefficients. Now $(1-x^{2k})^{-1/(2k)}$ $= \sum_{i\geq 0}\binom{-1/(2k)}{i}(-1)^i x^{2ik}$. Note that the coefficients of this sum are, term by term, less than or equal to the coefficients of $2\sum_{i\geq 0}\binom{-1/(2k)}{2i}(-1)^{2i}x^{2ik}+$ $2\sum_{i\geq 0}\binom{-1/(2k)}{2i+1}(-1)^{2i+1}x^{(2i+1)k}$, as, by Lemma 10, we have $\binom{-1/(2k)}{i}(-1)^i \leq$ $2\binom{-1/(2k)}{2i}(-1)^{2i}$ and $0 \leq 2\binom{-1/(2k)}{2i+1}(-1)^{2i+1}$ for all nonnegative integers i. Thus, by Lemma 11, we have that each coefficient of $(1-x)^{-1}(1-x^k)^{1/k}(1-x^{2k})^{-1/(2k)}$ is less than or equal to the corresponding coefficient of $(1-x)^{-1}(1-x^k)^{1/k}(2\sum_{i\geq 0}\binom{-1/(2k)}{2i}(-1)^{2i}x^{2ik}+2\sum_{i\geq 0}\binom{-1/(2k)}{2i+1}(-1)^{2i+1}x^{(2i+1)k})$. Now this last product is equal to

$$\begin{aligned}&(1-x)^{-1}(1-x^k)^{1/k}\cdot 2(1-x^k)^{-1/(2k)}\\ &= 2(1-x)^{-1}(1-x^k)^{1/(2k)}\\ &= 2(1+x+\cdots+x^{k-1})(1-x^k)^{1/(2k)-1}\\ &= 2(1+x+\cdots+x^{k-1})\sum_{i\geq 0}\binom{1/(2k)-1}{i}(-1)^i x^{ik}\\ &= \sum_{i\geq 0}2\binom{1/(2k)-1}{\lfloor i/k\rfloor}(-1)^{\lfloor i/k\rfloor}x^i.\end{aligned}$$

Thus, for all nonnegative integers n, we have that

$$\frac{a_n}{n!} \leq 2\binom{\frac{1}{2k}-1}{\lfloor\frac{n}{k}\rfloor}(-1)^{\lfloor\frac{n}{k}\rfloor}.$$

Then the desired result follows from Lemma 12, as it is a standard result that the gamma function is well-defined at inputs that are not nonpositive integers and is never zero, and one can check that combining Lemma 10 and Lemma 12 yields $\Gamma(1-1/(2k)) > 0$ (which alternatively can be immediately deduced from standard properties of the gamma function). □

Using this lemma, the following is immediate.

Proposition 14. *For any positive integer r, the proportion of permutations of $\{1,\ldots,n\}$ that have at least r cycles whose lengths are at least 63 and are divisible by 3 is $1-o(1)$.*

Proof. By Lemma 13, for each $i = 0,\ldots,r-1$, the proportion of permutations of $\{1,\ldots,n\}$ that do not have a cycle whose length is of the form $63\cdot 2^i\cdot(2m+1)$ for some nonnegative integer m is $o(1)$. Thus the proportion of permutations of $\{1,\ldots,n\}$ that have cycles of all those forms is $1-o(1)$, and any such permutation works (because no two of the cycles can be the same). □

3.3. **Reducing to consideration of three-strand braids.** Let m be a positive integer. Let P_m be the set of m-tuples $(\beta_1, \dots \beta_m)$ of simple braids on three strands such that the product $\beta_1 \dots \beta_m$ maps to a non-identity three-cycle under μ.

Lemma 15. *The number of elements of P_m is $2 \cdot 6^{m-1}$.*

Proof. For each of the 6^{m-1} possible choices of β_1 through β_{m-1}, there are two choices for β_m. □

Let C_m be the set of all permutations of $\{1, \dots, 3m\}$ that are $3m$-cycles. It is well-known (and easy to see) that C_m has $(3m-1)!$ elements. For any $\pi \in C_m$, we can consider some ordering $a_1, \dots, a_{3m}$ of $1, \dots, 3m$ defined by setting $a_1 = 1$ and $\pi(a_i) = a_{i+1}$ for $i = 1, \dots, 3m-1$. For convenience, let $a_{3m+1} = \pi(a_{3m}) = a_1$. Let $\beta \in B_{3m}$ be the simple braid corresponding to π.

Define an m-tuple $(\beta_1, \dots, \beta_m)$ of simple braids on three strands as follows. For each i with $1 \le i \le m$, consider the permutation of $\{1, 2, 3\}$ where we

- map $\{1, 2, 3\}$ to $\{a_i, a_{m+i}, a_{2m+i}\}$ where 1 maps to the smallest element of the latter set, 2 to the second-smallest, and 3 to the largest; then
- map $\{a_i, a_{m+i}, a_{2m+i}\}$ to $\{a_{i+1}, a_{m+i+1}, a_{2m+i+1}\}$ where $a_k \mapsto a_{k+1}$ for $k = i, m+i, 2m+i$; then
- map $\{a_{i+1}, a_{m+i+1}, a_{2m+i+1}\}$ to $\{1, 2, 3\}$ where the smallest element of the former set maps to 1, the second-smallest to 2, and the largest to 3.

Let β_i be the simple braid on three strands corresponding to that permutation.

Lemma 16. *We have that $(\beta_1, \dots, \beta_m)$ is an element of P_m.*

Proof. We have that the β_i are all simple braids on three strands. To see that $\mu(\beta_1 \cdot \dots \cdot \beta_m)$ is a three-cycle, note that $\mu(\beta_1 \cdot \dots \cdot \beta_m)$ is the following permutation (recalling that μ is a homomorphism, that $a_{3m+1} = a_1$, and that function composition goes right-to-left):

- map $\{1, 2, 3\}$ to $\{a_1, a_{m+1}, a_{2m+1}\}$ where 1 maps to the smallest element of the latter set, 2 to the second-smallest, and 3 to the largest; then
- map $\{a_1, a_{m+1}, a_{2m+1}\}$ to itself, where $a_1 \mapsto a_{m+1} \mapsto a_{2m+1} \mapsto a_1$; then
- map $\{a_1, a_{m+1}, a_{2m+1}\}$ to $\{1, 2, 3\}$ where the smallest element of the former set maps to 1, the second-smallest to 2, and the largest to 3.

Thus, as $a_1 = 1 < a_{m+1}, a_{2m+1}$, we can see that $\mu(\beta_1 \cdot \dots \cdot \beta_m)$ is $1 \mapsto 2 \mapsto 3 \mapsto 1$ if $a_{m+1} < a_{2m+1}$ and $1 \mapsto 3 \mapsto 2 \mapsto 1$ otherwise; in any case, we have the desired. □

Thus we have a map from C_m to P_m. Call this map ψ.

Lemma 17. *For any $(\beta_1, \dots, \beta_m) \in P_m$, the number of $\pi \in C_m$ such that $\psi(\pi) = (\beta_1, \dots, \beta_m)$ is $\frac{(3m-1)!}{2 \cdot 6^{m-1}}$.*

Proof. Let the cycle π be $1 = a_1 \mapsto a_2 \mapsto \dots \mapsto a_{3m} \mapsto a_1$. Consider the ordered m-tuple of sets $(\{a_{m+1}, a_{2m+1}\}, \{a_2, a_{m+2}, a_{2m+2}\}, \dots, \{a_m, a_{2m}, a_{3m}\})$. (Note that the first coordinate has two elements, while every other coordinate has three.) Note that each m-tuple corresponds to $2 \cdot 6^{m-1}$ possible cycles, so there are $\frac{(3m-1)!}{2 \cdot 6^{m-1}}$ possible m-tuples. Let us show that, for each of these possible m-tuples, there is exactly one choice for π that will correspond to it and will have $\psi(\pi) = (\beta_1, \dots, \beta_m)$.

It follows from the proof of Lemma 16 that we can determine whether a_{m+1} is less than or greater than a_{2m+1} depending on what $\mu(\beta_1 \cdot \dots \cdot \beta_m)$ is. Thus we can determine what the ordered triple (a_1, a_{m+1}, a_{2m+1}) is. Then we can inductively use

β_i to uniquely determine $\{a_{i+1}, a_{m+i+1}, a_{2m+i+1}\}$ from $\{a_i, a_{m+i}, a_{2m+i}\}$ for $i = 1, \ldots, n-1$. Hence, all the a_i are uniquely determined, so π is uniquely determined. To see that the resulting π does indeed satisfy the equation $\psi(\pi) = (\beta_1, \ldots, \beta_m)$, we proceed as follows. Let $\psi(\pi) = (\beta'_1, \ldots, \beta'_m)$. Then $\beta'_i = \beta_i$ for $i = 1, \ldots, m-1$ by definition. Also, we know $\mu(\beta'_1 \cdot \ldots \beta'_m) = \mu(\beta_1 \cdot \ldots \beta_m)$ (using the proof of Lemma 16); then, as $\beta'_i = \beta_i$ for $i = 1, \ldots, m-1$, we get $\mu(\beta'_m) = \mu(\beta_m)$, so $\beta'_m = \beta_m$ (as β'_m and β_m are simple braids). Therefore, $\beta'_i = \beta_i$ for $i = 1, \ldots, m$, so we indeed have $\psi(\pi) = (\beta_1, \ldots, \beta_m)$. Now the claim is shown; the Lemma immediately follows. □

Why do we care about this seemingly arbitrary map ψ? The following proposition shows how ψ can be useful: it lets us consider the topological entropy of three-strand braids instead of the topological entropy of braids on many strands. For any element $(\beta_1, \ldots, \beta_m)$ of P_m, let $\xi((\beta_1, \ldots, \beta_m)) = \beta_1 \cdot \cdots \cdot \beta_m$.

Proposition 18. *Let π be an element of C_m, and let β be the simple braid on $3m$ strands corresponding to π. Let $\psi(\pi) = (\beta_1, \ldots, \beta_m)$, and let $\gamma = \xi(\psi(\pi))$. If γ has positive topological entropy, then β has positive topological entropy.*

Proof. Suppose for contradiction that β has topological entropy zero. Let π be the permutation $a_1 \mapsto \cdots \mapsto a_{3m} \mapsto a_1$ with $a_1 = 1$, as earlier. Consider the braid β^m; this has topological entropy zero by Proposition 6. Now $\mu(\beta^m)$ contains the three-cycle $a_1 \mapsto a_{m+1} \mapsto a_{2m+1} \mapsto a_1$. Deleting all strands of β^m but those three, we get a braid that we will call ζ. By Proposition 8, ζ has topological entropy zero. If we draw strands from positions $\{1, 2, 3\}$ to $\{a_1, a_{m+1}, a_{2m+1}\}$ increasing order at the top, and vice versa at the bottom, then we have a three-strand braid ζ' which has topological entropy zero since ζ does, by part (c) of Proposition 6. But now, using facts from earlier about simple braids, one can see that $\zeta' = \gamma$; this is a contradiction, so we are done.

□

3.4. **A useful result about three-strand braids.** By taking $t = -1$ in the Burau representation of B_3, we get a homomorphism, which we will call f, from B_3 to $SL_2(\mathbb{Z})$, under which $\sigma_1 \mapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\sigma_2 \mapsto \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$. Note that $\det(f(\sigma_1)) = \det(f(\sigma_2)) = 1$, so we have $\det(M) = 1$ for all $M \in B_3$.

We have the following result.

Lemma 19. *For any $\beta \in B_3$, if $|\mathrm{tr}(f(\beta))| > 2$, then β has positive topological entropy.*

Proof. Let $M = f(\beta)$, and let $t = \mathrm{tr}(M)$. We have $\det(M) = 1$. Then the characteristic polynomial $\det(xI - M)$ of M is $x^2 - tx + 1$. Then the eigenvalues of M are $\frac{t \pm \sqrt{t^2-4}}{2}$. (Note that these eigenvalues are not equal to each other, as $t \neq \pm 2$.) Now if $t > 2$, then $\frac{t+\sqrt{t^2-4}}{2} > 1$; if $t < -2$, then $\frac{t-\sqrt{t^2-4}}{2} < -1$. Either way, M has an eigenvalue of magnitude greater than 1. Then Proposition 7 yields the desired. □

We can use this to prove the following result. (Note that the constant 21 in this result can likely be improved, but doing so is not necessary for our purposes.)

Proposition 20. *For any positive integer $m \geq 21$, the number of elements $(\beta_1, \ldots, \beta_m)$ to P_m that map to a braid of positive topological entropy under ξ is at least $2 \cdot 6^{m-21}$.*

Proof. We shall show that, for any choice of $\beta_1, \ldots, \beta_{m-21}$, there exist at least two possible choices of $\beta_{m-20}, \ldots, \beta_m$ such that $\beta_1 \cdot \cdots \cdot \beta_m$ has positive topological entropy.

Let us choose β_{m-20} so that $\mu(\beta_1 \cdot \cdots \cdot \beta_{m-20})$ is a three-cycle; clearly, this can be done in two ways (for each of the two three-cycles, there is a unique choice for what $\mu(\beta_{m-20})$ should be, and thus a unique choice for what β_{m-20} should be). For each of those choices we will find suitable $\beta_{m-19}, \ldots, \beta_m$.

Let $\beta = \beta_1 \cdot \cdots \cdot \beta_{m-20}$. Consider the following choices for $(\beta_{m-19}, \ldots, \beta_m)$:

- $(\iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota)$,
- $(\sigma_1, \sigma_1, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota)$,
- $(\sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_1, \sigma_1, \sigma_1, \sigma_1, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota, \iota)$, or
- $(\sigma_1, \sigma_1, \sigma_1, \sigma_1, \sigma_1, \sigma_1, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_2, \sigma_1, \sigma_1, \sigma_1, \sigma_1, \sigma_2, \sigma_2)$.

Note that, for each of these 20-tuples, we have $\mu(\beta_{m-19} \cdot \cdots \cdot \beta_m)$ is the identity permutation, as $\mu(\sigma_1^2) = \mu(\sigma_2^2) = \mu(\iota)$ is the identity permutation. Thus, for each of these 20-tuples, we have that $(\beta_1, \ldots, \beta_m) \in P_m$ (as $\mu(\beta_1 \cdot \cdots \cdot \beta_{m-20})$ is a three-cycle, and μ is a homomorphism).

One can compute (with the help of Magma [8]) that the values of $f(\beta_{m-19} \cdot \cdots \cdot \beta_m)$ for the above 20-tuples are, respectively, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $\begin{bmatrix} -15 & 4 \\ -4 & 1 \end{bmatrix}$, $\begin{bmatrix} 1 & 4 \\ -4 & -15 \end{bmatrix}$, and $\begin{bmatrix} 317 & -182 \\ 54 & -31 \end{bmatrix}$.

Let us show that at least one of those will yield a braid $\beta_1 \cdot \cdots \cdot \beta_m$ of positive topological entropy. Suppose for the sake of contradiction that none of them do. Let $f(\beta) = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$. The four choices above for $(\beta_{m-19}, \ldots, \beta_m)$ yield values for $f(\beta_1 \cdot \cdots \cdot \beta_m)$, of, respectively, $\begin{bmatrix} w & x \\ y & z \end{bmatrix}$, $\begin{bmatrix} -15w - 4x & 4w + x \\ -15y - 4z & 4y + z \end{bmatrix}$, $\begin{bmatrix} w - 4x & 4w - 15x \\ y - 4z & 4y - 15z \end{bmatrix}$, and $\begin{bmatrix} 317w + 54x & -182w - 31x \\ 317y + 54z & -182y - 31z \end{bmatrix}$. Since none of the options for $\beta_1 \cdot \cdots \cdot \beta_m$ have positive topological entropy, we can see by Lemma 19 that we must have

- $|w + z| \leq 2$,
- $|-15w - 4x + 4y + z| \leq 2$,
- $|w - 4x + 4y - 15z| \leq 2$, and
- $|317w + 54x - 182y - 31z| \leq 2$.

Also, we know $f(\beta) \in SL_2(\mathbb{Z})$ and $\det(f(\beta)) = 1$, so w, x, y, and z are integers, and $wz - xy = 1$. We shall use all these conditions on w, x, y, and z to derive a contradiction.

We have

$$\begin{aligned} 16|w - z| &= |(w - 4x + 4y - 15z) + (-(-15w - 4x + 4y + z))| \\ &\leq |w - 4x + 4y - 15z| + |-(-15w - 4x + 4y + z)| \\ &\leq 2 + 2 = 4, \end{aligned}$$

so, as $|w - z|$ is a nonnegative integer, we have $|w - z| = 0$, so $w = z$. Then $2|w| = |w + z| \leq 2$, so $w = 1, 0$, or -1. If $w = 0$, then we have $z = w = 0$, so $4|y - x| = |-15w - 4x + 4y + z| \leq 2$, so $y = x$, but then $-x^2 = wz - xy = 1$. This is a contradiction. Thus we must have $w = 1$ or -1. Then $xy = wz - 1 = w^2 - 1 = 0$, so $x = 0$ or $z = 0$. Then, as $w = z = 1$ or -1, and $x = 0$ or $z = 0$, we can simplify

$|317w + 54x - 182y - 31z| \leq 2$ into one of four inequalities, depending on which case we have. Specifically, one of the inequalities $|54x - 286| \leq 2$, $|54x + 286| \leq 2$, $|-182y + 286| \leq 2$, and $|-182y - 286| \leq 2$ must hold. However, as x and y are integers, we can easily check that none of those inequalities can hold (as none of $284, 285, 286, 287$, and 288 is a multiple of 54 or 182). Thus we have a contradiction.

Thus a choice for $(\beta_{m-19}, \ldots, \beta_m)$ that works exists, so the Proposition holds. □

3.5. **Finishing the proof of the theorem.** We can now readily prove Theorem 1.

Proof of Theorem 1. Choose any $\varepsilon > 0$. We shall show that, for all sufficiently large n, at least a proportion of greater than $1 - \varepsilon$ of the simple braids in B_n have positive topological entropy. Of course, if $\varepsilon > 1$ then this is clear, so assume $\varepsilon \leq 1$.

For convenience, say that a cycle in a permutation where the length of the cycle is a multiple of 3 that is at least 63 is a *good* cycle. Choose a positive integer r that is large enough so that $(1 - \frac{\varepsilon}{2})(1 - (1 - \frac{1}{6^{20}})^r) > 1 - \varepsilon$. Choose N sufficiently large such that, for all $n \geq N$, we have that, if we consider the proportion of permutations in S_n that have at least r good cycles, then this proportion is greater than $1 - \frac{\varepsilon}{2}$. (Such N clearly exists, by Proposition 14.) We claim that, for all positive integers $n \geq N$, the proportion of simple braids in B_n that have positive topological entropy is greater than $1 - \varepsilon$.

Among the $n!$ elements of S_n, let p be the number that have at least r good cycles. We have $p > (1 - \frac{\varepsilon}{2})(n!) > 0$. Let S be the set of these permutations. Consider a notion of equivalence on S where two permutations s_1 and s_2 in S are equivalent if and only if

- they have the same non-good cycles as one another, and
- two elements of $\{1, \ldots, n\}$ are in the same good cycle (i.e., they are in the same cycle, and that cycle is good) in s_1 if and only if they are in the same good cycle in s_2.

Clearly this is indeed an equivalence relation, so it partitions S into equivalence classes. Consider any such equivalence class. Consider any set of elements of $\{1, \ldots, n\}$ that need to be the elements of a good cycle in some order. Note that by using part (c) of Proposition 6, and other results from earlier, we can treat the set as if it were $\{1, \ldots, 3m\}$ for some $m \geq 21$ (corresponding the elements to those of $\{1, \ldots, 3m\}$ in increasing order). Consider the $(3m-1)!$ possible cycles. There are at least $2 \cdot 6^{m-21}$ elements of P_m that map to some element with positive topological entropy under ξ, so at least $(3m-1)! \cdot \frac{1}{6^{20}}$ cycles map to some element with positive topological entropy under ψ then ξ. Then, if there are r' good cycles in the elements of this equivalence class, then the proportion in which none of the good cycles map to an element of positive topological entropy under ψ then ξ is at most $\left(1 - \frac{1}{6^{20}}\right)^s \leq \left(1 - \frac{1}{6^{20}}\right)^r$.

Thus the proportion of elements of S_n that contain a good cycle that maps to some element of positive topological entropy under ψ then ξ (again, pretending that the relevant $3m$-element set is $\{1, \ldots, 3m\}$) is at least $(1 - \frac{\varepsilon}{2})\left(1 - \frac{1}{6^{20}}\right)^r > 1 - \varepsilon$. For any such braid, if it has topological entropy zero, then the braid we get by only keeping a good cycle as in the previous sentence has topological entropy zero; this will contradict Proposition 18. Thus all those braids have positive topological entropy, so we are done. □

4. Proof of Theorem 2

We now prove Theorem 2. We proceed by strong induction on n. The base cases $n = 2$ and $n = 3$ are easy to check.

Consider a permutation braid σ corresponding to a permutation π. We know from Proposition 5 that we can write σ as $(\sigma_{i_1} \cdot \dots \cdot \sigma_2 \cdot \sigma_1) \cdot (\sigma_{i_2} \cdot \dots \cdot \sigma_2) \cdot \dots \cdot (\sigma_{i_{n-1}} \cdot \dots \cdot \sigma_{n-1})$ for some values i_j with $j - 1 \leq i_j \leq n - 1$. (Having $i_j = j - 1$ means that the corresponding product is empty.)

Lemma 21. *For any $k > 0$, we have that the (i, j) entry of $\rho(\sigma_k \dots \sigma_1)$ is as follows:*

- *if $j = 1$, then $a_{ij} = -t^i$ if $i \leq k$ and $a_{ij} = 0$ otherwise;*
- *if $j > 1$, then, if $j - 1 = i \leq k$ or $j = i > k$, then $a_{ij} = 1$; otherwise $a_{ij} = 0$.*

Proof. This can be directly checked by induction on k. □

Lemma 22. *Consider the map f_n from $GL_{n-2}(\mathbb{Z}[t, t^{-1}])$ to $GL_{n-1}(\mathbb{Z}[t, t^{-1}])$ defined as follows: for $M \in GL_{n-2}(\mathbb{Z}[t, t^{-1}])$, we let $f_n(M)$ be the $n \times n$ matrix for which the $(1, 1)$ element is 1, all other elements in the first row and column are zero, and the matrix formed by deleting the first row and column of $f_n(M)$ is M. Then f_n is well-defined and is a homomorphism; furthermore, we have $f_n(\rho_{n-1}(\sigma_i)) = \rho_n(\sigma_{i+1})$ for $i \geq 2$.*

Proof. One can easily check that $f_n(X)f_n(Y) = f_n(XY)$ for all $X, Y \in GL_{n-2}(\mathbb{Z}[t, t^{-1}])$. Then one can check $f_n(X) \in GL_{n-1}(\mathbb{Z}[t, t^{-1}])$ for all $X \in GL_{n-2}(\mathbb{Z}[t, t^{-1}])$. Then f_n is a well-defined homomorphism; finally, the last assertion is clear. □

For any $n \times n$ matrix X, let $g_n(X)$ be the $(n-1) \times (n-1)$ matrix formed by deleting the first row and column of X. Note that, in general, $g_n(XY) \neq g_n(X)g_n(Y)$.

Lemma 23. *For $k \geq 0$, let $M_1, \dots, M_k$ be matrices in which all entries in the first row other than the $(1, 1)$ entry are zero. Let $N_i = g_n(M_i)$ for $i = 1, \dots k$. Let $M = M_1 \dots M_k$. Then all entries in the first row of M other than the $(1, 1)$ entry are zero, and $g_n(M) = N_1 \dots N_k$.*

Proof. This is easily verified for $k = 2$; then the desired statement follows easily by induction on k (with base case $k = 0$). □

Let $\beta' \in B_{n-1}$ be the braid $(\sigma_{i_3-1} \cdot \dots \cdot \sigma_3 \cdot \sigma_2) \cdot (\sigma_{i_4-1} \cdot \dots \cdot \sigma_3) \cdot \dots \cdot (\sigma_{i_{n-1}-1} \cdot \dots \cdot \sigma_{n-2})$. We have $\rho_n(\beta) = \rho_n(\sigma_{i_1} \cdot \dots \cdot \sigma_2 \cdot \sigma_1) \cdot \rho_n(\sigma_{i_2} \cdot \dots \cdot \sigma_2) \cdot f_n(\rho_{n-1}(\beta'))$. Let $M = \rho_n(\sigma_{i_1} \cdot \dots \cdot \sigma_2 \cdot \sigma_1)$ and $M' = \rho_n(\sigma_{i_2} \cdot \dots \cdot \sigma_2)$.

Note that we can apply Lemma 23 to M', as, for $j \geq 2$, we have that all entries of the first row of $\rho_n(\sigma_j)$ other than the $(1, 1)$ entry are zero; furthermore, we have that $g_n(\rho_n(\sigma_j)) = \rho_{n-1}(\sigma_{j-1})$. Thus all entries of the first row of M' other than the $(1, 1)$ entry are zero, and $g_n(M') = \rho_{n-1}(\sigma_{i_2-1} \cdot \dots \cdot \sigma_1)$. Now we can apply Lemma 23 to the product $M' \cdot f_n(\rho_{n-1}(\beta'))$. We get that all entries of the first row of $M' \cdot f_n(\rho_{n-1}(\beta'))$ other than the $(1, 1)$ entry are zero, and $g_n(M' \cdot f_n(\rho_{n-1}(\beta'))) = g_n(M')g_n(f_n(\rho_{n-1}(\beta')) = \rho_{n-1}(\sigma_{i_2-1} \cdot \dots \cdot \sigma_1)\rho_{n-1}(\beta') = \rho_{n-1}(\sigma_{i_2-1} \cdot \dots \cdot \sigma_1 \cdot \beta')$. Let $\beta'' = \sigma_{i_2-1} \cdot \dots \cdot \sigma_1 \cdot \beta'$. We can see that β'' is a permutation braid in B_{n-1}. Specifically, β'' is the permutation braid that corresponds to the permutation $\pi' \in S_{n-1}$ defined as $(\tau_{i_2-1} \cdot \dots \cdot \tau_1) \cdot (\tau_{i_3-1} \cdot \dots \cdot \tau_2) \cdot \dots \cdot (\tau_{i_{n-1}-1} \cdot \dots \cdot \tau_{n-2})$.

Lemma 24. *For k with $1 \le k \le n-1$, we have that, in $\rho_n(\sigma_k \cdot \sigma_2)$, the entries of the first column are as follows: for any j with $1 \le j \le n-1$, the $(j,1)$ entry is t^{j-1} if $j \le k$ and is 0 otherwise.*

Proof. This can be directly verified by induction on k (with base case $k = 1$). □

Now, as the first column of $f_n(\rho_{n-1}(\beta'))$ has $(1,1)$ entry 1 and all other entries zero, we can see that the first column of $M' \cdot f_n(\rho_{n-1}(\beta'))$ is equal to the first column of M', which is given by Lemma 24 with $k = i_2$. The discussion after the proof of Lemma 23 describes what all the other entries of $M' \cdot f_n(\rho_{n-1}(\beta'))$ are (note that we can use the inductive hypothesis to determine what the entries of $g_n(M' \cdot f_n(\rho_{n-1}(\beta'))) = \rho_{n-1}(\beta'')$ are). Thus all the entries of $M' \cdot f_n(\rho_{n-1}(\beta'))$ are (informally speaking) accounted for. Also, we know what the entries of M are by Lemma 21 with $k = i_1$. Then, as $\rho_n(\beta) = M \cdot (M' \cdot f_n(\rho_{n-1}(\beta')))$, we can combine information about M and $M' \cdot f_n(\rho_{n-1}(\beta'))$ to get the desired result about the entries of $\rho_n(\beta)$. Specifically, we can do the following.

Let $\varpi \in S_n$ be $(\tau_{i_2} \cdot \dots \cdot \tau_2) \cdot (\tau_{i_3} \cdot \dots \cdot \tau_3) \cdot \dots \cdot (\tau_{i_{n-1}} \cdot \dots \cdot \tau_{n-1})$. We have $\pi = \tau_{i_1} \dots \tau_1 \varpi$. Then one can check that $\pi(i) = \varpi(i+1)$ for i with $1 \le i \le i_1$, $\pi(i_1+1) = \varpi(1)$, and $\pi(i) = \varpi(i)$ for $i > i_1 + 1$. Also, we have that $\varpi(1) = 1$, and, for i with $1 \le i \le n-1$, we have $\varpi(i+1) = \pi'(i) + 1$. Thus, we have that $\pi(i) = \pi'(i) + 1$ for $1 \le i \le i_1$, $\pi(i_1+1) = 1$, and $\pi(i) = \pi'(i-1) + 1$ for $i > i_1 + 1$.

Now let us consider $\rho_n(\beta)$. The first column is M times the first column of $M' \cdot f_n(\rho_{n-1}(\beta'))$, and we know that the first column of $M' \cdot f_n(\rho_{n-1}(\beta'))$ is the same as the first column of M'. We know the entries of M from Lemma 21 with $k = i_1$, and we know the first column of M' from Lemma 24 with $k = i_2$, combining these will give that the first column of $\rho_n(\beta)$ is as desired. For the other columns of $\rho_n(\beta)$, one can see that this essentially amounts to duplicating one of the rows of $M' \cdot f_n(\rho_{n-1}(\beta'))$, so one can get that the desired result holds, using the earlier information about the relation between π and π'.

5. Future directions

It may be interesting to try to use Theorem 2 to obtain information about the eigenvalues of the images of simple braids under the Burau representation, and then to combine that information with Proposition 7 to obtain an improved version of Theorem 1. However, it may be difficult to do so, as the characteristic polynomials of matrices described by Theorem 2 do not seem easy to work with. More generally, it may be interesting to try to improve Theorem 1. If we let z_n be the number of simple braids in B_n that have topological entropy zero, then Theorem 2 says that $z_n = o(n!)$. By being careful with the bounds, the arguments in this paper show that, in fact $z_n = O\left(\frac{n!}{\ln \ln n}\right)$. It is likely that the combinatorics in Section 3.2 could be improved so that a bound of $z_n = O\left(\frac{n!}{\ln n}\right)$ results. Perhaps, a bound of the form $z_n = O(c^n)$ could be shown. (We note that no better asymptotic can be shown, as $z_n \ge 2^{\lfloor n/2 \rfloor}$, since one can check that, for any subset of $\{\tau_1, \tau_3, \tau_5, \dots, \tau_{2\lfloor n/2 \rfloor - 1}\}$, the product of its elements (which commute) gives a permutation that corresponds to a simple braid with topological entropy zero, and these $2^{\lfloor n/2 \rfloor}$ all give different permutations.) It may be interesting to try to determine, not just an asymptotic, but an exact formula for z_n, or some means of computing it.

It also may be interesting to consider a generalization of simple braids. Specifically, denote the half twist by Δ. Then, for integers j and k with $j < k$, one can consider the set of braids β for which $\beta\Delta^{-j}$ and $\Delta^k\beta^{-1}$ are positive. The set of simple braids is the special case of $j = 0$ and $k = 1$; the case of $j = -1$ and $k = 1$ is also of independent interest. What statements hold about the proportion of braids with positive topological entropy in such sets?

6. Acknowledgments

I greatly thank my mentor, Dr. Minh-Tam Trinh, for all his help. I thank the MIT PRIMES program for the opportunity to do this research; in particular, I thank them for connecting me with my mentor, and I thank Dr. Tanya Khovanova and Dr. Kent Vashaw for proofreading this paper. I thank Prof. Stephen Bigelow for answering our questions about the Burau representation, and I thank Prof. Benson Farb and Dr. Reid Harris for answering our questions about entropy.

References

[1] Adler, R.L., A.G. Konheim, and M.H. McAndrew. “Topological Entropy.” *Trans. of the Amer. Math. Soc.*, vol. 114, 1965, pp. 309–319.
[2] Band, Gavin, and Philip Boyland. “The Burau Estimate for the Entropy of a Braid.” *Algebr. Geom. Topol.*, vol. 7, 2007, pp. 1345–1378.
[3] Elrifai, Elsayed A., and H.R. Morton. “Algorithms for Positive Braids.” *The Quarterly Journal of Math.*, vol. 45, iss. 4, Dec. 1994, pp. 479–497.
[4] Farb, Benson and Dan Margalit. *A Primer on Mapping Class Groups.* Princeton University Press (2012).
[5] Fried, David. “Entropy and Twisted Cohomology.” *Topology*, vol. 25, no. 4, 1986, pp. 455–470.
[6] Kolev, Boris. “Topological Entropy and Burau Representation.” Preprint (2003). arxiv.org/abs/math/0304105v1.
[7] Levrie, Paul. “The Asymptotic Behavior of the Binomial Coefficients.” *Mathematics Magazine*, vol. 90, no. 2, Apr. 2017, pp. 119–123.
[8] *Magma.* magma.maths.usyd.edu.au/calc/.
[9] Stanley, Richard P. *Enumerative Combinatorics, Volume 2.* Cambridge University Press (1999).
[10] Turaev, Vladimir. “Faithful Linear Representations of the Braid Groups.” Séminaire Bourbaki, vol. 1999/2000, exposés 865–879, Astérique, no. 276 (2002), exposé no.878, pp. 389–409.