Glasgow Mathematical Journal (2023), 1–16
doi:10.1017/S0017089523000022

Glasgow Mathematical Journal

RESEARCH ARTICLE

Finite image homomorphisms of the braid group and its generalizations

Nancy Scherich[1] and Yvon Verberne[2,*]

[1]Department of Mathematics and Statistics, Elon University, Elon, NC 27244, United States of America
[2]Department of Mathematics, University of Toronto, Toronto, ON, Canada
*Corresponding author. E-mail: verberne.math@gmail.com

Received: 27 April 2022; **Revised:** 19 December 2022; **Accepted:** 6 January 2023

Keywords: Braid groups, virtual braids, welded braids, totally symmetric sets

2020 Mathematics Subject Classification: *Primary* - 20F36; *Secondary* - 57K12

Abstract
Using totally symmetric sets, Chudnovsky–Kordek–Li–Partin gave a superexponential lower bound on the cardinality of non-abelian finite quotients of the braid group. In this paper, we develop new techniques using *multiple* totally symmetric sets to count elements in non-abelian finite quotients of the braid group. Using these techniques, we improve the lower bound found by Chudnovsky et al. We exhibit totally symmetric sets in the virtual and welded braid groups and use our new techniques to find superexponential bounds for the finite quotients of the virtual and welded braid groups.

1. Introduction

The braid group, B_n, is a versatile mathematical object which plays an important role in both topology and algebra. In this paper, we focus on the size of the finite quotients of the braid group. Many useful applications of the braid group rely on facts about finite quotients of the braid group. For example, the structure of Jones representations of the braid group are understood due to the fact that B_n modulo the relation $\sigma_i^2 = 1$ is a finite group (the symmetric group, Σ_n) [13]. Another example is the use of braid group representations in models of topological quantum computing. To have a universal quantum gate set, it is important to know the size and structure of the image of the braid group representation [11].

A guiding theory which motivates the work found in this paper is profinite rigidity, or the idea of distinguishing groups by their finite quotients. More specifically, one would like to understand the circumstances which allow finitely generated *residually finite groups* to have isomorphic *profinite completions*. If a residually finite group G is isomorphic to its profinite completion, we say that the group G is *profinitely rigid*. In the context of braid groups and their generalizations, these groups are all residually finite, and the theory of profinite rigidity asks whether we can determine these groups by knowing only what their finite quotients are. One step for studying whether a group G is profinitely rigid is to determine which finite groups appear as finite quotients of the group G. The work done in this paper is a step toward solving which subgroups appear as finite quotients of the braid group and its generalizations as we are providing a lower bound on the size of the non-cyclic finite quotients. For more of an overview of recent work and progress on profinite rigidity, see [21].

To study finite quotients of the braid group, we consider homomorphisms $\phi : B_n \to G$, where G is a finite group. If G is a cyclic group, then the quotient of B_n will be a cyclic group. A homomorphism is called *cyclic* (resp. *abelian*) if its image is a cyclic group (resp. an abelian group). One main focus of this paper is to understand the non-cyclic quotients of B_n. Work by Chudnovsky–Kordek–Li–Partin [8], and more recently by Caplinger–Kordek [7], proves a lower bound for the size of non-cyclic quotients

of B_n. In this paper, we provide an improved lower bound for the size of non-cyclic quotients of B_n by a factor of n to the result of Caplinger–Kordek, as found in Theorem 1.1.

Theorem 1.1. *Let $n \geq 5$, and let $\phi : B_n \to G$ be a non-cyclic homomorphism to a finite group, G, so that $\phi(B_n)$ is not isomorphic to the symmetric group, Σ_n. Then,*

$$|\phi(B_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1 \right) \left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right) \left\lfloor \frac{n}{2} \right\rfloor !.$$

Moreover, if p is the smallest integer so that $\phi(\sigma_i)^p = \phi(\sigma_j)^p$ for any i, j, then

$$|\phi(B_n)| \geq \left((\mathrm{lpf}(p) - 1) \left\lfloor \frac{n-1}{2} \right\rfloor + 1 \right) \left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right) \left\lfloor \frac{n}{2} \right\rfloor !,$$

where $\mathrm{lpf}(p)$ *is the least integer greater than 1 that divides p.*

A secondary motivation for Theorem 1.1 is the following conjecture.

Theorem 1.1, and the results by Chudnovsky–Kordek–Li–Partin and Caplinger–Kordek, attempt to rule out smaller possible non-cyclic quotients of B_n. When $n = 5, 6$, and 7, Caplinger–Kordek used the classification of finite groups to conclude that a non-cyclic quotient of B_n has size at least $n!$ [7]. Since Theorem 1.1 gives a lower bound on the size of the image of a non-cyclic homomorphism for $n \geq 5$, it gives the tightest known lower bound for the size of a finite non-cyclic quotient of B_n for $n \geq 8$.

Theorem 1.1 shows that the existence of a non-cyclic homomorphism $\phi : B_n \to G$ requires the group G to be quite large or complicated. To see this, recall that all finite groups embed in a large enough symmetric group, Σ_k, which implies that we can consider the target group G in Theorem 1.1 to be Σ_k. When $n \geq 6$, and $k < n$, homomorphisms $B_n \to \Sigma_k$ must be cyclic [1]. Therefore, if the group G embeds into a small enough symmetric group, the image of ϕ is cyclic. However, less is known when $k \geq n$. One step to understand the case where $k \geq n$ was provided by Lin who showed that for $6 < n < k < 2n$, all transitive homomorphisms $B_n \to \Sigma_k$ are cyclic [20]. Since there exist cyclic maps $B_n \to \Sigma_k$ with $k > n$, one could ask which other types of non-cyclic homomorphisms can exist.

We prove Theorem 1.1 using totally symmetric sets inside B_n. A *totally symmetric set* is a commutative set that satisfies a highly symmetric conjugation relation. The theory of totally symmetric sets was first introduced by Kordek and Margalit when studying homomorphisms of the commutator subgroup of B_n [19]. More recently, totally symmetric sets were used by Caplinger–Kordek [7] and Chudnovsky–Kordek–Li–Partin [8] when studying finite quotients of the braid group. Totally, symmetric sets are useful for counting arguments since the image of a totally symmetric set S under a homomorphism ϕ has size $|\phi(S)| = |S|$ or $|\phi(S)| = 1$. In this paper, our approach is novel in the sense that we create counting arguments using multiple totally symmetric sets at once.

There is a topological generalization of knot theory in S^3 to knot theory in a thickened surface of higher genus, known as *virtual knot theory*. Virtual knot theory was introduced by Louis H. Kauffman in the 1990s [17, 18]. From this perspective, B_n can be generalized to the *virtual braid group*, vB_n, where every virtual knot is ambient isotopic to the closure of a virtual braid [15]. One way to think of vB_n is as an extension of B_n by the symmetric group Σ_n, where the added permutations are the virtual crossings. The *welded braid group*, wB_n, is an infinite quotient of vB_n and was first described by Fenn–Rimányi–Rourke in [10]. Similar to the pure braid group, the virtual and welded braid groups have "pure" subgroups, denoted PvB_n and PwB_n, respectively, which fix the strands of the braids pointwise. Inside both the virtual and welded braid groups, we find totally symmetric sets. One particularly useful type of totally symmetric set in wB_n is denoted by A_i in the theorems below; see Section 4.2.1. Using the totally symmetric sets, A_i, we proved classification theorems on the size of finite images of homomorphisms for both the virtual and welded braid groups. First, we state the classification theorem for the

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

welded braid group, wB_n. We hope that this is the first step in classifying non-cyclic homomorphisms $wB_n \to G$.

Theorem 1.2. *Let $n \geq 5$, and let $\phi : wB_n \to G$ be a group homomorphism to a finite group, G, so that $\phi(wB_n)$ is not isomorphic to the symmetric group, Σ_n. One of the following must be true:*

(1) ϕ is abelian.
(2) ϕ restricted to PwB_n is cyclic.
(3) $|\phi(wB_n)| \geq 2^{n-2}(n-1)!$
(4) For all i and j, ϕ maps each A_i to a single element with $\phi(A_i)^2 \neq \phi(A_j)^2$, and

$$|\phi(wB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor !.$$

For the case of the virtual braid group, Bellingeri and Paris classified all homomorphisms from $vB_n \to \Sigma_k$ where $n \geq 5$, $k \geq 2$ and $n \geq k$ [4]. However, similar to the story for B_n, not much is known about non-cyclic homomorphisms $vB_n \to \Sigma_k$ when $k > n$. Theorem 1.3 is a step in the right direction toward this classification as it provides a necessary condition for the existence of a non-abelian homomorphism $vB_n \to G$.

Theorem 1.3. *Let $n \geq 5$, and let $\phi : vB_n \to G$ be a group homomorphism to a finite group, G, so that $\phi(vB_n)$ is not isomorphic to the symmetric group, Σ_n. One of the following must be true:*

(1) ϕ is abelian.
(2) ϕ factors through wB_n, and either

a. ϕ restricted to PwB_n is cyclic.
b. $|\phi(vB_n)| \geq 2^{n-2}(n-1)!$
c. For all i and j, ϕ does not split A_i, $\phi(A_i)^2 \neq \phi(A_j)^2$, and

$$|\phi(vB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor !.$$

(3) ϕ does not factor through wB_n and

$$|\phi(vB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor !.$$

Outline of the paper. Section 2 provides the background information about totally symmetric sets. Section 3 applies these ideas to B_n and gives a proof of Theorem 1.1. Section 4 provides the background about the virtual and welded braid groups and introduces some totally symmetric sets inside of these groups. Section 5 contains the proofs of Theorems 1.2 and 1.3.

2. Totally symmetric sets

Kordek and Margalit introduced the theory of totally symmetric sets to give a complete classification of homomorphisms $B'_n \to B'_n$ for $n \geq 7$, where B'_n is the commutator subgroup of B_n [19]. Totally symmetric sets are useful because they behave predictably under homomorphisms and group closures, as will be described in detail below.

Definition 2.1. *A totally symmetric set of a group G is a nonempty finite subset $\{g_1, \ldots, g_n\}$ of G which satisfies the following two relations:*

(1) The elements g_i pairwise commute *(Commutativity Condition)*
(2) For every permutation σ, there exists an element $h_\sigma \in G$ so that for each i, $h_\sigma g_i h_\sigma^{-1} = g_{\sigma(i)}$ *(Conjugation Condition)*

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

Remark. *While in our context we consider only finite totally symmetric sets, we note that totally symmetric sets need not be finite as seen in* [19].

The conjugation condition states that each permutation of $\{g_1, \ldots, g_n\}$ can be achieved via the conjugation of an element in G. An important fact about totally symmetric sets is that if $f : G \to H$ is a homomorphism and S is a totally symmetric set of G, then $f(S)$ is a totally symmetric set of H.

A standard example of a group which contains totally symmetric sets is the braid group [19]. We begin by defining the braid group.

Definition 2.2. *The braid group on n strands, B_n, is the group generated by the half-twists $\sigma_1, \ldots, \sigma_{n-1}$ with the following two relations:*

(1) $\sigma_i\sigma_j = \sigma_j\sigma_i$ *if* $|i-j| \geq 2$ *(Far Commutativity)*
(2) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ *if* $1 \leq i \leq n-2$ *(Braid Relation)*

In B_n, the subsets $S_{odd} = \{\sigma_{2i-1}\}_{i=1}^{\lfloor n/2 \rfloor}$ and $S_{even} = \{\sigma_{2i}\}_{i=1}^{\lfloor (n-1)/2 \rfloor}$ are both totally symmetric sets [8, 19].

Remark. *The braid group is equivalent to the mapping class group of an n-times punctured disk. As the elements of S_{odd} (resp. S_{even}) have disjoint domains, we can apply the change-of-coordinates principle to see that the conjugation condition holds for each of the two sets. See Section* 1.3 *of "A primer on mapping class groups" for a detailed discussion* [9].

2.1. The image of a totally symmetric set

The following lemma, due to Kordek and Margalit [19] (Lemma 2.1), is the crux of how totally symmetric sets are used throughout this paper.

Lemma 2.3 (Kordek−Margalit). *Let $f : G \to H$ be a group homomorphism. Suppose that $S \subseteq G$ is a totally symmetric set of size k. Then $|f(S)|$ is equal to either* 1 *or k.*

In this paper, we often consider whether $|\phi(S)| = |S|$ or not. We say that ϕ *splits* S if $|\phi(S)| = |S|$.

Remark. *By Lemma* 2.3*, if $|S| > 1$, then ϕ splits S if and only if $|\phi(S)| > 1$.*

Remark. *The proof by Kordek and Margalit of Lemma* 2.3 *only makes use of the conjugation condition from the definition of a totally symmetric set. Therefore, Lemma* 2.3 *holds for all sets which satisfy the conjugation condition from the definition of a totally symmetric set. For a set that only satisfies the conjugation condition, it makes sense to say whether ϕ splits the set or not.*

2.2. Totally symmetric sets with finite order elements

Let $S = \{s_i\}_{i=1}^n$ be a totally symmetric subset of a group G. Since all elements of S are conjugate, every element of S has the same order. Therefore, if one element of S has finite order $k \in \mathbb{N}$, every element of S has order k.

Remark. *In fact, if there exists p so that $s_i^p = s_j^p$ for any i, j, then $s_i^p = s_j^p$ for all i, j. This follows immediately from the conjugation condition in the definition of a totally symmetric set and is also true in noncommutative sets which satisfy the conjugation condition.*

Since the elements of a totally symmetric set commute, if a totally symmetric set consists of a finite number of elements each of finite order, then $\langle S \rangle$ is a finite group. The following lemma gives a lower bound of the size of this group. A first bound was obtained by Chen, Kordek, and Margalit (a proof

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

of which can be found in [8]), but we will use an improvement of this bound by Caplinger–Kordek [7] (Lemma 6).

Lemma 2.4 (Caplinger−Kordek). *Let S be a totally symmetric set of size k in a group, G. Suppose further that each element of S has finite order and let p be the minimal integer such that $s_i^p = s_j^p$ for all $s_i, s_j \in S$. Then, $\langle S \rangle$ is a finite group and $|\langle S \rangle| \geq p^{k-1}$.*

Combining Lemma 2.4 with work of Chudnovsky–Kordek–Li–Partin, one obtains a lower bound on the size of a group based on the size of a totally symmetric subset consisting of finite order elements [8].

Proposition 2.5 (Chudnovsky–Kordek−Li−Partin, Caplinger−Kordek). *Let S be a totally symmetric set of size k in a group, G. If the elements of S have finite order and p is the minimal integer such that $s_i^p = s_j^p$ for all $s_i, s_j \in S$, then $|G| \geq p^{k-1}k!$.*

A restatement of Proposition 2.5 in terms of group homomorphisms is the following: let S be a totally symmetric set of a group G and $\phi : G \to H$ a group homomorphism to a finite group H. If ϕ splits S, then $|\phi(G)| \geq p^{|S|-1}|S|!$, where p is the minimal integer such that $s_i^p = s_j^p$ for all $s_i, s_j \in S$.

3. Applications to the braid group

In this section, we utilize totally symmetric sets to determine a necessary condition for the existence of a non-cyclic homomorphism from the braid group into a finite group. We begin with an overview of existing results and then we discuss how to strengthen previous results.

3.1. Precursory results

Recall the two totally symmetric sets in B_n of $S_{odd} = \{\sigma_{2i-1}\}_{i=1}^{\lfloor n/2 \rfloor}$ and $S_{even} = \{\sigma_{2i}\}_{i=1}^{\lfloor (n-1)/2 \rfloor}$. Chudnovsky, Kordek, Li, and Partin used these totally symmetric sets to determine a necessary condition for the existence of a non-cyclic homomorphism of the braid group [8]. Recently, Caplinger and Kordek obtained a stronger necessary condition than the one found by Chudnovsky–Kordek–Li–Partin [7].

Lemma 3.1 (Caplinger−Kordek). *Let G be a finite group and let $n \geq 5$. If the homomorphism $B_n \to G$ is non-cyclic, then,*

$$|G| \geq 3^{\lfloor n/2 \rfloor - 1} (\lfloor n/2 \rfloor)!.$$

In Section 3.2, we strengthen the lower bound found in Lemma 3.1. Before we strengthen this lower bound, we introduce the following well-known facts about the braid group, which can be found in [1]. This lemma provides sufficient conditions for when then image of a homomorphism of the braid group is cyclic.

Lemma 3.2. *For $n \geq 5$, and let $\phi : B_n \to G$ be a group homomorphism where G is any group. If there exists $i, i+1 \leq n-1$ so that $\phi(\sigma_i)$ commutes with $\phi(\sigma_{i+1})$ then ϕ is cyclic.*

Lemma 3.3. *For $n \geq 5$, if $\phi : B_n \to G$ is a non-cyclic group homomorphism, then ϕ must split both S_{even} and S_{odd}.*

Proof. Since $n \geq 5$, both S_{even} and S_{odd} have cardinality at least 2. Suppose that ϕ does not split S_{even}. Then $\phi(\sigma_2) = \phi(\sigma_4)$. Since σ_4 commutes with σ_1, then $\phi(\sigma_2)$ commutes with $\phi(\sigma_1)$. By Lemma 3.2, ϕ must be cyclic, a contradiction.

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

By a similar computation, if ϕ does not split S_{odd}, then $\phi(\sigma_4)$ commutes with $\phi(\sigma_3)$, ultimately forcing ϕ to be cyclic. □

Notice that both Lemmas 3.2 and 3.3 fail for $n = 4$ as there exists the folding homomorphism from $B_4 \to B_3$ which maps $\sigma_1, \sigma_3 \mapsto \sigma_1$ and $\sigma_2 \mapsto \sigma_2$.

3.2. Proof of Theorem 1.1

In this section, we prove Theorem 1.1, which provides a strengthened lower bound for the smallest non-cyclic finite quotient of B_n.

We begin by following the proof of Chudnovsky–Kordek–Li–Partin, then further their ideas by applying Lemma 3.2.

Theorem 1. *Let $n \geq 5$, and let $\phi : B_n \to G$ be a non-cyclic homomorphism to a finite group, G, so that $\phi(B_n)$ is not isomorphic to the symmetric group, Σ_n. Then,*

$$|\phi(B_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor!.$$

Moreover, if p is the smallest integer so that $\phi(\sigma_i)^p = \phi(\sigma_j)^p$ for any i, j, then

$$|\phi(B_n)| \geq \left((\mathrm{lpf}(p) - 1)\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor!,$$

where $\mathrm{lpf}(p)$ *is the least integer greater than* 1 *that divides* p.

Proof of Theorem 1.1. Denote $\mathscr{O}_\phi = \phi(S_{odd})$, $\mathscr{E}_\phi = \phi(S_{even})$, $s_i = \phi(\sigma_i)$, $k = \lfloor n/2 \rfloor$, $\mathscr{B} = \phi(B_n)$, let d be the order of the s_i's and let p be the smallest integer so that $\phi(\sigma_i)^p = \phi(\sigma_j)^p$ for any i, j.

Since we aim for a lower bound, we may assume that $\phi(B_n)$ is the smallest possible quotient not isomorphic to Σ_n. In this case, Caplinger and Kordek prove that $p = d$ in Lemma 7 of [7]. If $d = 1$, then ϕ is trivial (hence cyclic). If $d = 2$, ϕ factors through the symmetric group Σ_n, and the image is either Σ_n or cyclic (since the alternating group is the only proper normal subgroup of Σ_n for $n \geq 5$).

Therefore, we may assume that $d = p \geq 3$.

As ϕ is not cyclic and $n \geq 5$, each s_i is distinct by Lemma 3.3. Thus, $\mathscr{O}_\phi$ is a totally symmetric subset of size k in $\mathscr{B}$ as the injective image of a totally symmetric subset of size k in B_n.

Notice that $\mathscr{B}$ acts by conjugation on the set of totally symmetric subsets of $\mathscr{B}$ of size k, and let $\Gamma = \mathrm{Fix}_{\mathscr{B}}(\mathscr{O}_\phi)$. This gives us a surjection $\psi : \Gamma \to \Sigma_k$, where Σ_k is the symmetric group on k elements.

Under this action by $\mathscr{B}$, $\mathscr{O}_\phi$ fixes $\mathscr{O}_\phi$ pointwise since the elements of a totally symmetric set pairwise commute. This shows that $\langle \mathscr{O}_\phi \rangle \subseteq \Gamma$ and, in fact, $\langle \mathscr{O}_\phi \rangle \subseteq \ker(\psi)$. By Lemma 2.4, we have that $|\langle \mathscr{O}_\phi \rangle| \geq p^{k-1}$, and since $p \geq 3$, $|\ker(\psi)| \geq 3^{k-1}$. It follows that

$$|\mathscr{B}| \geq |\Gamma| = |\Sigma_k| \cdot |\ker(\psi)| \geq k!(|\langle \mathscr{O}_\phi \rangle|) \geq k!3^{k-1}. \tag{3.1}$$

We now begin improving the bound on $|\mathscr{B}|$. Notice that $\mathscr{E}_\phi = \{s_{2i}\}_{i=1}^{\lfloor (n-1)/2 \rfloor}$ is a second totally symmetric set which consists of the images of the remaining generators of B_n. The elements in $\mathscr{E}_\phi$ are currently not accounted for in Equation 3.1. To include these elements in the bound of $|\mathscr{B}|$, we consider when elements of $\langle \mathscr{E}_\phi \rangle$ are not in Γ. The following observations lead us to find elements of $\langle \mathscr{E}_\phi \rangle$ that are not in Γ. We then count distinct cosets of Γ in $\mathscr{B}$.

Observation 1. Suppose there exists an $m \in \{1, \ldots, p-1\}$ so that $s_i^m \in \Gamma$, then $s_i^m \in \ker \psi$.

By definition of Γ, s_i^m acts on $\mathscr{O}_\phi$ by conjugation, fixing $\mathscr{O}_\phi$ setwise. By the relations of the braid group, s_i^m commutes with every element of $\mathscr{O}_\phi$ except for $s_{i\pm1}$. Since $\mathscr{O}_\phi$ is fixed setwise, then either

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

conjugation by s_i^m swaps the elements s_{i+1} and s_{i-1}, or fixes the elements pointwise. Suppose first that conjugation by s_i^m swaps the elements s_{i+1} and s_{i-1}, meaning $s_i^m s_{i-1} s_i^{-m} = s_{i+1}$. Then,

$$s_{i+2}(s_{i+1})s_{i+2}^{-1} = s_{i+2}\left(s_i^m s_{i-1} s_i^{-m}\right) s_{i+2}^{-1} = s_i^m s_{i-1} s_i^{-m} = s_{i+1},$$

which shows that s_{i+2} and s_{i+1} commute. By Lemma 3.2, ϕ must be cyclic. If i is large enough so that either $i+1 > n-1$ or $i+2 > n-1$, an analogous argument shows that s_{i-2} and s_{i-1} commute and that ϕ is cyclic. In both cases, we have contradicted our assumption that ϕ is non-cyclic. Thus, conjugation by s_i^m does not swap the elements s_{i+1} and s_{i-1} but rather fixes these elements pointwise. Therefore, for all i, conjugation by s_i^m fixes every element of S pointwise. This implies that if $s_i^m \in \Gamma$, then $s_i^m \in \ker \psi$.

Observation 2**.** $s_i \notin \Gamma$ for i even.

Suppose that $s_i \in \Gamma$. Observation 1 implies that $s_i \in \ker \psi$ and s_i commutes with every other s_j. Lemma 3.2 implies that ϕ is a cyclic map, a contradiction. Therefore, $s_i \notin \Gamma$.

Observation 3**.** $s_i^m \notin \Gamma$ for i even and m relatively prime to p.

Suppose that $s_i^m \in \Gamma$ for some $m \geq 2$ and i even. By Observation 1, $s_i^m \in \ker \psi$ and commutes with every element of $\mathscr{O}_\phi$ and $\mathscr{E}_\phi$. Since s_i^m commutes with every s_j, this implies that s_i^m is central in the image of ϕ. If there exists an integer r so that $(s_i^m)^r = s_i$, then this implies s_i is also central in the image of ϕ, which by Lemma 3.2, implies that ϕ is cyclic, a contradiction. Thus, for integers m that are relatively prime to $p = ord(s_i)$, the elements s_i^m cannot be elements of $\ker \psi$ and hence are not elements in Γ. For the powers m that are not relatively prime to p, there is no contradiction, and it is possible for s_i^m to be in $\ker \psi$.

Observation 4**.** $s_i^{m_1}\Gamma \neq s_j^{m_2}\Gamma$ when i and j are even, m_1 and m_2 are relatively prime to p, and $m_1 - m_2$ is relatively prime to p.

From Observation 3, $s_i^{m_1}, s_j^{m_2} \notin \Gamma$ for every i, j even and m_1, m_2 relatively prime to p. Suppose that $s_i^{m_1}\Gamma = s_j^{m_2}\Gamma$. This implies that $s_i^{-m_1} s_j^{m_2} \in \Gamma$.

If $i = j$, then $s_i^{-m_1} s_j^{m_2} \in \Gamma$ implies that $s_i^{m_2 - m_1} \in \Gamma$. Then, $m_2 - m_1$ is not relatively prime to p, a contradiction.

If $i < j$, then s_j commutes with s_{i-1}. Consider the action of $s_i^{-m_1} s_j^{m_2}$ on s_{i-1} by conjugation:

$$s_j^{-m_2} s_i^{m_1} s_{i-1} s_i^{-m_1} s_j^{m_2} = s_i^{m_1} s_{i-1} s_i^{-m_1}.$$

Since we supposed that $s_i^{-m_1} s_j^{m_2} \in \Gamma$, then conjugation by $s_i^{-m_1} s_j^{m_2}$ fixes the set $\mathscr{O}_\phi$ setwise. Therefore, the above equation shows that $s_i^{m_1} s_{i-1} s_i^{-m_1} \in \mathscr{O}_\phi$. The exponent m_1 was chosen so that $s_i^{m_1} \notin \Gamma$, which means that $\mathscr{O}_\phi$ is not closed under conjugation by $s_i^{m_1}$. As described in Observation 1, $s_i^{m_1} s_{i-1} s_i^{-m_1}$ is not an element of $\mathscr{O}_\phi$ when ϕ is non-cyclic, a contradiction. Hence, $s_i^{-m_1} s_j^{m_2} \notin \Gamma$.

Observation 5**.** Counting the cosets of Γ.

Let $\mathrm{lpf}(p)$ be the least integer greater than 1 that divides p. Notice that the set $\{2, \ldots, \mathrm{lpf}(p) - 1, \mathrm{lpf}(p) + 1\}$ is a set of $\mathrm{lpf}(p) - 1$ integers which are each relatively prime to p, and pairwise their differences are relatively prime to p. Together with Observation 4, this shows that there are $\mathrm{lpf}(p) - 1$ distinct non-intersecting cosets of Γ for each s_i with i even. Since there are $|\mathscr{E}_\phi|$ distinct elements s_i with i even, we get $(\mathrm{lpf}(p) - 1)|\mathscr{E}_\phi|$ distinct cosets of Γ.

By counting the distinct cosets of Γ, we obtain a lower bound for the complement of Γ in the image of ϕ:

$$|\phi(B_n) - \Gamma| \geq (\mathrm{lpf}(p) - 1)|\mathscr{E}_\phi| \cdot |\Gamma|$$

Combining all of these observations, we arrive at the following lower bound for $|\phi(B_n)|$:

$$\begin{aligned} |\phi(B_n)| \geq |\Gamma| + ((\mathrm{lpf}(p) - 1)|\mathscr{E}_\phi|)|\Gamma| &= ((\mathrm{lpf}(p) - 1)|\mathscr{E}_\phi| + 1) \cdot |\Gamma| \\ &\geq ((\mathrm{lpf}(p) - 1)|\mathscr{E}_\phi| + 1)(|\langle \mathscr{O}_\phi \rangle|)k!. \end{aligned}$$

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

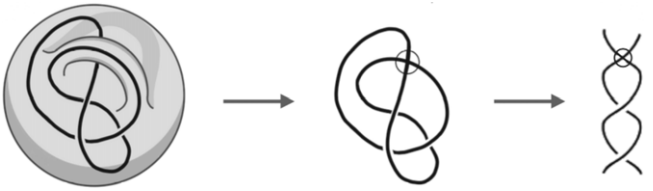

Figure 1. *A virtual knot in a thickened torus, a projection of this virtual knot, and a virtual braid whose closure is the knot*

By substituting the values of k, $|\langle \mathscr{O}_\phi \rangle|$, and $|\mathscr{E}_\phi|$, we arrive at our final result:

$$|\phi(B_n)| \geq \left((\mathrm{lpf}(p) - 1) \left\lfloor \frac{n-1}{2} \right\rfloor + 1 \right) \left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right) \left\lfloor \frac{n}{2} \right\rfloor !.$$

For all even values of p, we have that $\mathrm{lpf}(p) - 1 = 1$, which gives the minimal bound:

$$|\phi(B_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1 \right) \left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right) \left\lfloor \frac{n}{2} \right\rfloor !.$$

4. Totally symmetric sets in the virtual and welded braid groups

In this section, we motivate and introduce two generalizations of the braid group, namely, the virtual braid group and the welded braid group. For each group, we give examples of totally symmetric sets as well as provide the important lemmas required to prove the main results, Theorems 1.2 and 1.3.

Classical knot theory is the study of embedded circles in S^3 up to ambient isotopy and planar projections of these knots up to classical Reidemeister moves. Virtual knot theory is a natural generalization of classical knot theory by instead studying embedded circles in thickened surfaces of higher genus, which are called virtual knots.

Due to the higher genus, projections of these virtual knots have two types of crossings: classical crossings coming from arcs crossing in the thickness of the surface, and virtual crossings arising from an arc in a handle that pass over another arc of the knot, as shown in Figure 1. Virtual crossings are denoted as a circled crossing, and a virtual knot diagram can have both classical and virtual crossings. Like the classical setting, virtual knot diagrams are considered up to *virtual Reidemeister moves*, as described by Kauffman [17, 18]. There are virtual analogs of Alexander's theorem, first proved by Kamada [15], and Markov's theorem, proved by Kauffman–Lambropolou [16]. These theorems give rise to a rich study of virtual braid groups, which we describe below.

4.1. The virtual braid group

Let vB_n denote the *virtual braid group* on n strands. This group has generators $\sigma_1, \ldots, \sigma_{n-1}$ and $\tau_1, \ldots, \tau_{n-1}$. The generators $\sigma_1, \ldots, \sigma_{n-1}$ satisfy the classical braid group relations, and the generators $\tau_1, \ldots, \tau_{n-1}$ generate the symmetric group. There are also some mixing relations. We list all relations in the virtual braid group, below:

(1) $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| > 1$ (Far Commutativity)
(2) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $1 \leq i \leq n-2$ (Braid Relation)
(3) $\tau_i^2 = 1$ for $1 \leq i \leq n-1$ (τ is a Transposition)
(4) $\tau_i\tau_j = \tau_j\tau_i$ for $|i-j| > 1$ (τ Far Commutativity)
(5) $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ for $1 \leq i \leq n-2$ (τ Braid Relation)
(6) $\sigma_i\tau_j = \tau_j\sigma_i$ for $|i-j| > 1$ (Mixed Far Commutativity)
(7) $\tau_{i+1}\sigma_i\tau_{i+1} = \tau_i\sigma_{i+1}\tau_i$ for $1 \leq i \leq n-2$ (Mixed Braid Relation)

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

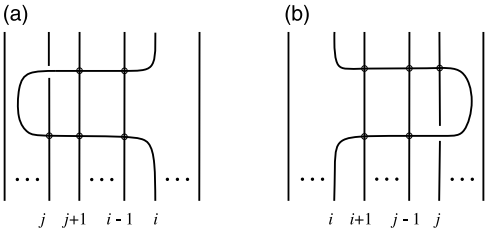

Figure 2. *(a) The element $\sigma_{i,j}$ when $j < i$. (b) The element $\sigma_{i,j}$ when $i < j$*

We note that these relations encode the *virtual (or extended) Reidemeister moves*. From this point of view, vB_n is the free product of the braid group and the symmetric group modulo relations (6) and (7), $vB_n = B_n * \Sigma_{n\ (6),(7)}$. This presentation is nice in the sense that you can "see" the braid group as a subgroup of the virtual braid group. B_n embeds into vB_n, as was first proven by Kamada [14]; see also Gaudreau [12] and Bellingeri–Paris [4]. The canonical embeddings of B_n and Σ_n in vB_n are $B_n = \langle \sigma_1, \cdots, \sigma_{n-1} \rangle$ and $\Sigma_n = \langle \tau_1, \cdots, \tau_{n-1} \rangle$.

Another presentation of vB_n highlights a key difference between the virtual braids and the classical braids. The pure virtual braid group, PvB_n, is a subgroup of vB_n which is the kernel of the projection $vB_n \to \Sigma_n$ by sending $\sigma_i \mapsto \tau_i$ and $\tau_i \mapsto \tau_i$. Unlike the classical braid group, vB_n splits as a semidirect product, $vB_n \cong PvB_n \rtimes \Sigma_n$ [3].

The subgroup PvB_n is generated by elements denoted $\sigma_{i,j}$ of the form:

$$\sigma_{i,j} = \tau_i \tau_{i+1} \dots \tau_{j-2} \tau_{j-1} \sigma_{j-1} \tau_{j-2} \dots \tau_{i+1} \tau_i \qquad \text{when } i < j, \text{ and}$$
$$\sigma_{i,j} = \tau_{i-1} \tau_{i-2} \dots \tau_{j-2} \tau_{j-1} \sigma_j \tau_j \tau_{j-1} \dots \tau_{i-1} \qquad \text{when } j < i.$$

These generators are depicted in Figure 2. A presentation for PvB_n is generated by the $\sigma_{i,j}$, for $i \neq j$ elements and the following two relations [3]:

Commutativity Relation: $\sigma_{i,j}\sigma_{k,l} = \sigma_{k,l}\sigma_{i,j}$ where $|\{i, j, k, l\}| = 4$

Braid Relation: $\sigma_{i,j}\sigma_{i,k}\sigma_{j,k} = \sigma_{j,k}\sigma_{i,k}\sigma_{i,j}$ where $|\{i, j, k\}| = 3$

4.1.1. Totally symmetric sets in the virtual braid group

Since B_n is a subgroup of vB_n, the sets $S_{odd} = \{\sigma_{2i-1}\}_{i=1}^{\lceil n/2 \rceil}$ and $S_{even} = \{\sigma_{2i}\}_{i=1}^{\lfloor n/2 \rfloor}$ are also totally symmetric subsets of vB_n. Additionally, the sets $T_{odd} = \{\tau_{2i-1}\}_{i=1}^{\lceil n/2 \rceil}$ and $T_{even} = \{\tau_{2i}\}_{i=1}^{\lfloor n/2 \rfloor}$ are totally symmetric subsets of vB_n. A fun way to see why T_{odd} and T_{even} are totally symmetric is that they are the homomorphic image of S_{even} and S_{odd} under the canonical projection map from $B_n \to \Sigma_n$.

The sets $\{\tau_i\sigma_i\}_{even}$ and $\{\tau_i\sigma_i\}_{odd}$ are totally symmetric sets in vB_n. The sets are commutative by a combination of relations (1), (5), and (7). The conjugation condition holds since you can swap $\tau_i\sigma_i$ with $\tau_{i+2}\sigma_{i+2}$ by conjugation under $\tau_{i+1}\tau_{i+2}\tau_i\tau_{i+1}$, which leaves all other elements of the set fixed.

4.2. The welded braid group

The welded braid group, wB_n, is a quotient of vB_n by the *Over Crossings Commute* relation, or "OC" relation, defined as $\tau_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\tau_{i+1}$ [5]. The welded braid group has also been called the *braid-permutation group* by Fenn–Rimányi–Rourke [10], a finite-index subgroup of the *ring group* by Brendle–Hatcher [6], and the *loop braid group* by Baez–Crans–Wise [2].

Recall from Section 4.1.1, a presentation for PvB_n is generated by the elements denoted $\sigma_{i,j}$. These elements also generate the pure welded braid group, PwB_n. Analogous to the virtual braid group, wB_n is a semidirect product of the pure welded braid group and the symmetric group, $wB_n = PwB_n \rtimes \Sigma_n$. Through communication with Dror Bar-Natan, we learned the folklore result that the OC relation implies

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

that $\sigma_{i,k}\sigma_{i,j} = \sigma_{i,j}\sigma_{i,k}$, and a proof of this fact can be found in [22]. It follows that PwB_n is a quotient of PvB_n by the OC relation, and PwB_n has the following presentation:

Generators: $\{\sigma_{i,j}\}$ for $1 \leq i, j \leq n$ with $i \neq j$

Commutativity Relation: $\sigma_{i,j}\sigma_{k,l} = \sigma_{k,l}\sigma_{i,j}$ where $|\{i, j, k, l\}| = 4$

Braid Relation: $\sigma_{i,j}\sigma_{i,k}\sigma_{j,k} = \sigma_{j,k}\sigma_{i,k}\sigma_{i,j}$ where $|\{i, j, k\}| = 3$

OC Relation: $\sigma_{i,k}\sigma_{i,j} = \sigma_{i,j}\sigma_{i,k}$

4.2.1. Totally symmetric sets in wB_n

All of the totally symmetric sets in vB_n are also totally symmetric in wB_n. Due to the OC relation, wB_n has additional totally symmetric sets coming from subsets of the $\sigma_{i,j}$ elements.

If $i < j$, we call $\sigma_{i,j}$ a *right generator* and is shown in Figure 2(b). We denote the set of right generators with fixed i as $R_i = \{\sigma_{i,j}\}_{j>i}^{n}$. If $i < j$, we call $\sigma_{i,j}$ a *left generator* and is shown in Figure 2(a). For a fixed i, the set of left generators is denoted by $L_i = \{\sigma_{i,j}\}_{i>j}^{n}$. Let $A_i = L_i \cup R_i$ be the set of all elements of the form $\sigma_{i,j}$ which have the same first index. The sets A_i, R_i, and L_i are totally symmetric sets in wB_n.

Lemma 4.1. *For each integer $1 \leq i \leq n$,*

(1) A_i is a totally symmetric set in wB_n of size $n - 1$.
(2) R_i is a totally symmetric set in wB_n of size $n - i$.
(3) L_i is a totally symmetric set in wB_n of size $i - 1$.

Proof. Fix i. By definition, $|R_i| = n - i$, $|L_i| = i - 1$, and $|A_i| = |R_i| + |L_i| = n - 1$. Since R_i and L_i are subsets of A_i, it suffices to show that A_i is a totally symmetric set in wB_n. The elements in A_i all have the same first index i and commute by the OC relation.

From the semidirect product decomposition $wB_n = PwB_n \rtimes \Sigma_n$, Σ_n acts on PwB_n by conjugation which results in permutation of the indices. That is, for $s \in \Sigma_n$, $s\sigma_{i,j}s^{-1} = \sigma_{s(i),s(j)}$. □

The OC relation is required for the sets R_i, L_i, and A_i to satisfy the commutation condition. These sets are *not* totally symmetric in vB_n but do satisfy the conjugation condition in vB_n.

4.2.2. Important lemmas

The classical braid group B_n and the symmetric group Σ_n are subgroups of vB_n, and also wB_n, under the canonical embeddings $B_n = \langle \sigma_i \rangle_{i=1}^{n-1} \subseteq vB_n$ and $\Sigma_n = \langle \tau_i \rangle_{i=1}^{n-1} \subseteq vB_n$. This was proven by Kamada [15] for the virtual case and Fenn–Rimányi–Rourke [10] for the welded case. The pure subgroup has the canonical presentation $PvB_n = \langle \sigma_{i,j} \rangle_{i \neq j} \subseteq vB_n$, similarly for PwB_n. From here on, the restriction of a map on vB_n (resp. wB_n) to B_n, Σ_n or PvB_n (resp. PwB_n) refers to the canonical embeddings of these groups. Recall from the introduction that a map ϕ is called cyclic (resp. abelian), if its image is cyclic (resp. abelian).

Lemma 4.2. *If $\phi : vB_n \to G$ is a group homomorphism so that ϕ restricted to either Σ_n or B_n is abelian, then ϕ abelian.*

Proof. Suppose that ϕ restricted to Σ_n is abelian. The τ braid relation gives that $\phi(\tau_i) = \phi(\tau_{i+1})$ for all i, and so ϕ is cyclic on Σ_n. Denote $\phi(\tau_i) = g$. Applying ϕ to the mixed braid relation yields

$$\begin{aligned} \phi(\tau_{i+1}\sigma_i\tau_{i+1}) &= \phi(\tau_i\sigma_{i+1}\tau_i) \\ g\phi(\sigma_i)g &= g\phi(\sigma_{i+t})g \\ \phi(\sigma_i) &= \phi(\sigma_{i+1}) \end{aligned}$$

This shows that ϕ restricted to B_n is also cyclic, and therefore ϕ is abelian.

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

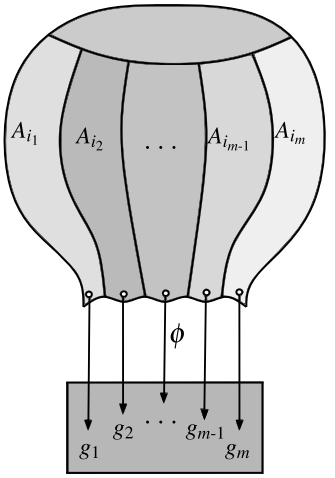

Figure 3. *Schematic diagram for Lemma 4.3*

Suppose that ϕ restricted to B_n is abelian. A similar argument using the braid relations shows that ϕ is cyclic on B_n, and the mixed braid relation shows that ϕ is cyclic on Σ_n. □

Corollary. *If $\phi : wB_n \to G$ is a group homomorphism so that ϕ restricted to either Σ_n or B_n is abelian, then ϕ is abelian.*

Proof. Let $p : vB_n \to wB_n$ be the quotient map which sends a virtual braid to its equivalence class modulo the the OC relation. Apply Lemma 4.2 to the map $\phi \circ p$. □

The following lemma is a key step to proving Theorems 1.2 and 1.3. To use totally symmetric sets to count the cardinality of the image of a homomorphism, the homomorphism needs to split a totally symmetric set. This lemma shows that, under the right conditions, when some subset of the totally symmetric sets $\{A_i\}_{i=1}^n$ do not split under a map $\phi : wB_n \to G$, the images of the A_i's which do not split create a new totally symmetric set in the image. A schematic diagram for Lemma 4.3 is shown in Figure 3.

Lemma 4.3. *Let $\{A_{i_1}, \cdots, A_{i_m}\}$ be a subset of $\{A_1, \cdots, A_n\}$, the totally symmetric sets in wB_n. Let $\phi : wB_n \to G$ be a non-abelian group homomorphism. Suppose ϕ does not split A_{i_j} for all i_j, and each $\phi(A_{i_j})^2$ is a distinct element in the image. Then the set $\{\phi(A_{i_j})^2\}_{j=1}^m$ is a totally symmetric set in $\phi(wB_n)$ of size m.*

Proof. We will prove this lemma for the case where $\{A_{i_1}, \cdots A_{i_m}\} = \{A_1, \cdots, A_m\}$, as all other cases follow from an analogous proof with possible re-indexing.

Let $g_i = \phi(A_i)$. We will show that the set $\{g_i^2\}_{i=1}^m$ is a totally symmetric set in $\phi(wB_n)$ of size m.

By assumption, the g_i^2's are distinct so the set $\{g_i^2\}_{i=1}^m$ has m elements. Notice that every element of A_i is of the form $\sigma_{i,j}$, where the first index, i, remains fixed. Since ϕ does not split any of the totally symmetric sets A_i, $\phi(\sigma_{i,j})$ is determined by its first index i, that is, $\phi(\sigma_{i,j}) = g_i$.

For the commutation condition, applying ϕ to the braid relation in wB_n shows

$$\sigma_{i,j}\sigma_{i,k}\sigma_{j,k} = \sigma_{j,k}\sigma_{i,k}\sigma_{i,j}$$
$$\phi(\sigma_{i,j})\phi(\sigma_{i,k})\phi(\sigma_{j,k}) = \phi(\sigma_{j,k})\phi(\sigma_{i,k})\phi(\sigma_{i,j})$$
$$g_i g_i g_j = g_j g_i g_i,$$

which shows that for each i and j, g_i^2 and g_j commute. In turn, this implies that g_i^2 and g_j^2 commute.

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

To show the conjugation condition holds, notice that if $fg_if^{-1} = g_j$ then $fg_i^2f^{-1} = g_j^2$. Therefore, it suffices to show the conjugation condition holds for the set $\{g_i\}$. The following computations show that conjugation by $\phi(\tau_i)$ swaps g_i and g_{i+1} but fixes all other g_k.

First, we show that conjugation by $\phi(\tau_i)$ swaps g_i and g_{i+1}. There are two cases to consider:

Case 1: Suppose $i \leq n-2$. A similar computation described in Lemma 4.1 shows that conjugation by τ_i swaps $\sigma_{i,i+2}$ with $\sigma_{i+1,i+2}$. Thus,

$$\phi(\tau_i\sigma_{i,i+1}\tau_i) = \phi(\sigma_{i+1,i+2})$$
$$\phi(\tau_i)g_i\phi(\tau_i) = g_{i+1}.$$

Case 2: Suppose $i > n-2$, which implies that $i = n-1$. A similar computation to the one above shows that conjugation by τ_{i-1} swaps $\sigma_{i,i-1}$ and $\sigma_{i+1,i-1}$ and that conjugation by $\phi(\tau_i)$ swaps g_i and g_{i+1}.

Next, we show that g_k is fixed under conjugation by τ_i, when $k \neq i, i+1$. Recall that conjugation by τ_i on $\sigma_{j,k}$ permutes the indices: $\tau_i\sigma_{j,k}\tau_i = \sigma_{\tau_i(j),\tau_i(k)}$. So, when $k \neq i, i+1$, g_k remains fixed under conjugation by $\phi(\tau_i)$ as follows:

$$\phi(\tau_i)g_k\phi(\tau_i) = \phi(\tau_i\sigma_{k,-}\tau_i) = \phi(\sigma_{\tau_i(k),\tau_i(-)}) = \phi(\sigma_{k,-}) = g_k.$$

This proves the conjugation condition in the definition of a totally symmetric set holds, and we have proven our claim. □

Remark. *The Lemma 4.3 is stated for wB_n; however, it is also true for vB_n. In vB_n, the sets A_i are not totally symmetric, but they do satisfy the conjugation condition, which is the only condition needed in the proof.*

5. Finite image homomorphisms of the virtual and welded braid groups

In this section, we prove the classification theorems on the size of finite images of homomorphisms of both wB_n and vB_n.

5.1. Proof of Theorem 1.2

First, we prove the classification theorem for the welded braid group, wB_n. This is a first step in classifying non-cyclic homomorphisms $wB_n \to G$, where G is a finite group.

Theorem 1.2. *Let $n \geq 5$, and let $\phi : wB_n \to G$ be a group homomorphism to a finite group, G, so that $\phi(wB_n)$ is not isomorphic to the symmetric group, Σ_n. One of the following must be true:*

(1) ϕ is abelian.
(2) ϕ restricted to PwB_n is cyclic.
(3) $|\phi(wB_n)| \geq 2^{n-2}(n-1)!$
(4) For all i and j, ϕ maps each A_i to a single element with $\phi(A_i)^2 \neq \phi(A_j)^2$, and

$$|\phi(wB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor !.$$

In the statement of Theorem 1.2, the requirement that $n \geq 5$ is only necessary for Part (3) due to the applications of Lemma 3.3 and Theorem 1.1. All other conditions hold for $n \geq 4$.

The proof of Theorem 1.2 is inspired by Figure 4. We consider cases on whether ϕ splits various rows and columns of the diagrams. The rows of the Full diagram, as seen in Figure 4(b), are the totally symmetric sets, A_i, from Lemma 4.1. In the Left diagram, the rows of the outlined triangle are the totally symmetric sets, L_i. The rows above the outlined triangle are the inverses of the columns within

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

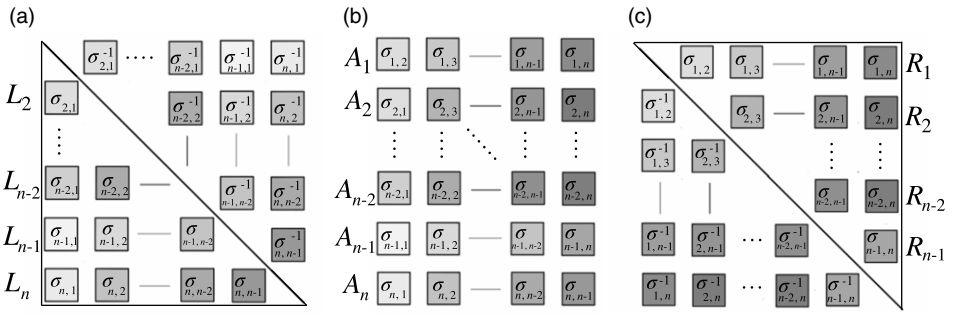

Figure 4. *(a) Left diagram. (b) Full diagram. (c) Right diagram*

the outlined triangle. Both the columns in the outlined triangle and the rows above the outline are not totally symmetric sets but satisfy the conjugation condition. This can be verified by similar computations described in Lemma 4.1. The Right diagram has an analogous form. The rows of the outlined triangle are the totally symmetric sets, R_i. The columns below the outlined triangle are the inverses of the rows within the triangle, and both satisfy the conjugation condition.

Proof of Theorem 1.2. Let us suppose that ϕ is non-abelian and that ϕ restricted to PwB_n is non-cyclic. We consider cases on whether or not ϕ splits the totally symmetric sets A_i.

Case 1: Suppose that there exists an i so that ϕ splits A_i. Since A_i is a totally symmetric set with size $n-1$, applying Proposition 2.5 yields

$$|\phi(wB_n)| \geq 2^{n-2}(n-1)!.$$

Case 2: Suppose ϕ does not split any of the A_i's. Denote $\phi(A_i) = \{g_i\}$. Further suppose that there exists i_0 and j_0 so that $g_{i_0}^2 \neq g_{j_0}^2$. Notice this implies $g_{i_0} \neq g_{j_0}$. Since ϕ is non-abelian, we may assume by Lemma 4.2 that ϕ is non-cyclic on Σ_n and that $\phi(\tau_i) \neq id$. We consider cases on i_0 and j_0 with the goal to apply Lemma 4.3.

Subcase 1: Suppose $i_0, j_0 < n$. We will use the Right diagram in Figure 4 to conclude that $g_1, \cdots, g_{n-1}$ are distinct. By assumption, $g_{i_0} \neq g_{j_0}$ which implies that $\phi\left(\sigma_{i_0,n}\right) \neq \phi\left(\sigma_{j_0,n}\right)$, and therefore $\phi\left(\sigma_{i_0,n}^{-1}\right) \neq \phi\left(\sigma_{j_0,n}^{-1}\right)$. The bottom row of the Right diagram contains both $\sigma_{i_0,n}^{-1}$ and $\sigma_{j_0,n}^{-1}$. Even though the bottom row of the Right diagram is not a totally symmetric set, it does satisfy the conjugation condition. Since $\phi\left(\sigma_{i_0,n}^{-1}\right) \neq \phi\left(\sigma_{i_1,n}^{-1}\right)$, Remark 2.1 implies that ϕ splits the bottom row. Thus, $\phi\left(\sigma_{i,n}^{-1}\right) \neq \phi\left(\sigma_{j,n}^{-1}\right)$ for all $i, j < n$, which shows that $g_i \neq g_j$, for all $i, j < n$. Since $g_{i_0}^2 \neq g_{j_0}^2$ by assumption, Remark 2.2 shows the each of the g_i^2 are unique. Thus, we have shown all of the hypotheses of Lemma 4.3 are satisfied, and $\left\{g_1^2, \cdots, g_{n-1}^2\right\}$ is a totally symmetric set in the image of ϕ of size $n-1$. Proposition 2.5 yields

$$|\phi(wB_n)| \geq 2^{n-2}(n-1)!.$$

Subcase 2: Suppose $i_0, j_0 > 1$. An analogous argument to Subcase 1 using the Left diagram from Figure 4 concludes that $\left\{g_2^2, \cdots, g_n^2\right\}$ is a totally symmetric set in the image of ϕ of size $n-1$. Proposition 2.5 yields

$$|\phi(wB_n)| \geq 2^{n-2}(n-1)!.$$

Subcase 3: Suppose $i_0 = 1$ and $j_0 = n$, which implies that $g_1 \neq g_n$, and further that $\phi(\sigma_{1,-}) \neq \phi(\sigma_{n,-})$. Looking at the Full diagram in Figure 4(b), Subcase 3 analyzes when the top and bottom rows of the Full diagram are mapped to different elements.

We now analyze where ϕ can send the second row.

Suppose first that ϕ maps A_2, or all the elements of the second row, to g_1. Then in Figure 4(a), the Left diagram, we notice that L_2 and L_n map to different elements. Therefore, two elements in the top

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

row of Figure 4(a) map to different elements. Since the top row satisfies the conjugation condition, we have that the top row must split. Since $g_{i_0}^2 \neq g_{j_0}^2$ by assumption, Remark 2.2 shows that each g_i^2 is unique. Therefore, by Lemma 4.3, the set $\left\{g_2^2, g_3^2, \ldots, g_n^2\right\}$ is a totally symmetric set of size $n-1$. Proposition 2.5 yields

$$|\phi(wB_n)| \geq 2^{n-2}(n-1)!.$$

A similar argument follows for when ϕ maps A_2, or all the elements of the second row, to g_n, but this time we consider Figure 4(c), the Right diagram. Since R_1 and R_2 map to different elements, the bottom row of the Right diagram must split as it satisfies the conjugation relation. Since $g_{i_0}^2 \neq g_{j_0}^2$ by assumption, Remark 2.2 shows that each g_i^2 is unique. Therefore, by Lemma 4.3, the set $\left\{g_1^2, g_2^2, \ldots, g_{n-1}^2\right\}$ is a totally symmetric set of size $n-1$. In this case, Proposition 2.5 will again yield

$$|\phi(wB_n)| \geq 2^{n-2}(n-1)!.$$

Finally, suppose that ϕ sends A_2 to an element g_2 where $g_2 \neq g_1, g_n$. Then in Figure 4(a), the Left diagram, we notice that L_2 and L_n map to different elements. Therefore, two elements in the top row of Figure 4(a) map to different elements. Since the top row satisfies the conjugation condition, we have that the top row must split. Similarly, in Figure 4(c), the Right diagram, we notice that R_1 and R_2 map to different elements. Therefore, two elements in the bottom row of Figure 4(c) map to different elements, and since the bottom row satisfies the conjugation condition the bottom row must split. Notice that we must have that ϕ sends each A_i to a unique element. Indeed, suppose that $g_i = g_j$ for some i, j. This implies that either the top row of the Left diagram or the bottom row of the Right diagram cannot split, since these rows have the conjugation relation, which is a contradiction to the above. Since $g_{i_0}^2 \neq g_{j_0}^2$ by assumption, Remark 2.2 shows the each g_i^2 is unique. By Lemma 4.3, the set $\left\{g_1^2, g_2^2, \ldots, g_n^2\right\}$ is a totally symmetric set of size n. In this case, Proposition 2.5 will yield that

$$|\phi(wB_n)| \geq 2^{n-1}(n)!.$$

Case 3: Suppose ϕ does not split any of the A_i's, and $\phi(A_i)^2 = \phi(A_j)^2$ for all i and j. Notice that Lemma 4.3 does not apply, and that none of the A_i's are split by ϕ. In this case, we use the fact that ϕ restricted to B_n is non-cyclic. Applying Theorem 1.1 to ϕ restricted to B_n, we get

$$|\phi(wB_n)| \geq |\phi(B_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor!.$$

5.2. Proof of Theorem 1.3

In this section, we provide a proof for Theorem 1.3 which gives a lower bound on the size of vB_n's smallest non-cyclic finite quotient. By considering whether or not a homomorphism factors through wB_n, we may apply our classification of homomorphisms from $wB_n \to G$, or the necessary condition for the existence of a homomorphism $B_n \to G$, to determine a classification of the size of finite images of homomorphisms from vB_n.

Theorem 1.3. *Let $n \geq 5$, and let $\phi : vB_n \to G$ be a group homomorphism to a finite group, G, so that $\phi(vB_n)$ is not isomorphic to the symmetric group, Σ_n. One of the following must be true:*

(1) *ϕ is abelian.*
(2) *ϕ factors through wB_n, and either*

   a. *ϕ restricted to PwB_n is cyclic.*
   b. *$|\phi(vB_n)| \geq 2^{n-2}(n-1)!$*

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

c. *For all i and j, ϕ does not split A_i, $\phi(A_i)^2 \neq \phi(A_j)^2$, and*

$$|\phi(vB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor!.$$

(3) *ϕ does not factor through wB_n and*

$$|\phi(vB_n)| \geq \left(\left\lfloor \frac{n-1}{2} \right\rfloor + 1\right)\left(3^{\lfloor \frac{n}{2} \rfloor - 1}\right)\left\lfloor \frac{n}{2} \right\rfloor!.$$

Proof of Theorem 1.3. Suppose ϕ is not abelian. If ϕ factors through wB_n, then by Theorem 1.2, one of either (2)(a), (2)(b), or (2)(c) must be true. If ϕ does not factor through wB_n and ϕ is non-abelian, Lemma 4.2 gives that ϕ restricted to B_n is non-abelian, and hence non-cyclic. Applying Theorem 1.1 to ϕ restricted to B_n gives that (3) must be true. □

Acknowledgments. The authors thank Dror Bar-Natan and Dan Margalit for helpful conversations and Thomas Ng for helpful conversations which led to the improvement of the bound in Theorem 1.1. The authors also thank the anonymous referee for carefully reading the paper and providing helpful comments.

Funding statement. The first author was partially supported by NSERC grant RGPIN-2018-04350. The second author was supported by the National Science Foundation under Grant No. DMS-1928930 while participating in a program hosted by the Mathematical Sciences Research Institute in Berkeley, California, during the Fall 2020 semester. Both authors would like to thank the Georgia Institute of Technology for their hospitality during the Tech Topology Conference in December of 2019, where this project initially began.

Conflicts of interest. The authors declare none.

Data availability statement. There is no data, code, or other materials required to verify the findings in this paper.

Ethical standards. The research meets all ethical guidelines, including adherence to the legal requirements of the study country.

Author contributions. Both authors contributed equally to this research and manuscript.

References

[1] E. Artin, Braids and permutations, *Ann. Math.* **48**(2) (1947), 643–649.
[2] J. C. Baez, D. K. Wise and A. S. Crans, Exotic statistics for strings in 4D *BF* theory, *Adv. Theor. Math. Phys.* **11**(5) (2007), 707–749.
[3] V. Bardakov, The virtual and universal braids, *Fundamenta Mathematicae* **184**(1) (2004), 1–18.
[4] P. Bellingeri and L. Paris, Virtual braids and permutations, *Ann. l'Institut Fourier* **70**(3) (2020), 1341–1362.
[5] P. Bellingeri and A. Soulié, A note on representations of welded braid groups, *J. Knot Theory Ramif.* **29** (2020), 2050082.
[6] T. E. Brendle and A. Hatcher, Configuration spaces of rings and wickets, *Commentarii Mathematici Helvetici* **88** (2008), 131–162.
[7] N. Caplinger and K. Kordek, Small quotients of braid groups. arXiv:2009.10139 (2020).
[8] A. Chudnovsky, K. Kordek, Q. Li and C. Partin, Finite quotients of braid groups, *Geometriae Dedicata* **207**(48) (2020), 409–416.
[9] B. Farb and D. Margalit, *A primer on mapping class groups* (Princeton University Press, Princeton, New Jersey, 2012).
[10] R. Fenn, R. Rimányi and C. Rourke, The braid-permutation group, *Topology* **36**(1) (1997), 123–135.
[11] M. H. Freedman, A. Kitaev, M. J. Larsen and Z. Wang, Topological quantum computation, *Bull. Am. Math. Soc.* **20**(1) (2002), 31–38.
[12] R. Gaudreau, The braid group injects in the virtual braid group (2020, arXiv preprint arXiv:2008.09631, unpublished).
[13] V. F. R. Jones, Hecke algebra representations of braid groups and link polynomials, *Ann. Math.* **126**(2) (1987), 335–388.
[14] S. Kamada, Invariants of virtual braids and a remark on left stabilizations and virtual exchange moves, *Kobe J. Math.* **21** (2004), 33–49.
[15] S. Kamada, Braid presentation of virtual knots and welded knots, *Osaka J. Math.* **44**(2) (2007), 441–458.
[16] L. Kauffman and S. Lambropoulou, Virtual braids and the L–move, *J. Knot Theory Ramif.* **15**(6) (2005), 773–811.
[17] L. H. Kauffman, Virtual knot theory, *Eur. J. Comb.* **20** (1999), 663–691.

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press

[18] L. H. Kauffman, Detecting virtual knots, *Atti del Seminario Matematico e Fisico dell'Università di Modena* **49** (2001), 241–282.
[19] K. Kordek and D. Margalit, Homomorphisms of commutator subgroups of braid groups, *Bull. London Math. Soc.* **54**(1) (2022), 95–111.
[20] V. Lin, Braids and permutations. arXiv:0404528 (2004).
[21] A. Reid, Profinite rigidity, in *Proceedings of the International Congress of Mathematicians*, Rio de Janeiro, 2018, vol. 1 (2018), 1191–1214.
[22] N. Scherich and Y. Verberne, Proof of the folklore OC relation identity (2020). Available at https://nancyscherich.files.wordpress.com/2020/11/oc-relation.pdf, unpublished.

https://doi.org/10.1017/S0017089523000022 Published online by Cambridge University Press