

TUTORIAL ON THE BRAID GROUPS

Dale Rolfsen

*Department of Mathematics
University of British Columbia
Vancouver, BC, V6T 1Z2, Canada
E-mail: rolfsen@math.ubc.ca*

This is an introduction to the theory of braids, one of the most beautiful examples of algebra and topology working hand-in-hand. The emphasis is on the variety of points of view from which one can view braids, and the information one gains from each aspect. As preparation for further lectures in a summer school and conference on the braid groups, these talks (and therefore this chapter) are intended for students with some basic background in topology and the theory of groups.

1. Introduction

The braid groups B_n were introduced by E. Artin eighty years ago [1], although their significance to mathematics was possibly realized a century earlier by Gauss, as evidenced by sketches of braids in his notebooks, and later in the nineteenth century by Hurwitz. The braid groups provide a very attractive blending of geometry and algebra, and have applications in a wide variety of areas of mathematics, physics, and recently in polymer chemistry and molecular biology.

Despite their ripe old age, and an enormous amount of attention paid to them by mathematicians and physicists, these groups still provide us with big surprises. The subject was given a major boost when V. Jones discovered, in the mid 1980's, new representations of the braid groups, which led to the famous Jones polynomial of knot theory. In this chapter, we will touch on that discovery, and more recent ones, regarding this wonderful family of groups, and raise a few questions about them which are still

open. Along the way, we will also discuss some properties of these groups which deserve to be better known. Among our personal favorites is the orderability of braid groups, which implies that they have some special algebraic properties.

This discussion will not include many interesting aspects of braid theory, such as the conjugacy problem as solved by Garside, dynamics of braids, applications to cryptography and connections with homotopy groups of spheres. Many proofs will be omitted in this presentation. Some proofs will be left as exercises for the students, often with hints or references.

The emphasis here is that there are many ways of looking at braids, and each point of view provides new information about these groups. Though much of the motivation for studying braids comes from knot theory, we will be stressing the algebraic aspects of braid groups.

1.1. Prerequisites

Students will be assumed to have background in basic topology and group theory. No other specialized expertise is necessary.

1.2. Suggested reading

At the time of this writing, an excellent book on braid theory is in press; we predict it will become the “bible” of the theory:

- C. Kassel and V. Turaev, *Braids*, Springer, 2008.
Following are some other useful introductions to the subject.
- Joan Birman and Tara Brendle, Braids, A Survey, in *Handbook of Knot Theory* (eds. W. Menasco and M. Thistlethwaite), Elsevier, 2005.
Available electronically at:
<http://www.math.columbia.edu/~jb/Handbook-21.pdf>.
- Joan Birman, *Braids, Links and Mapping Class Groups*, Annals of Mathematics Studies, Princeton University Press, 1974.
This classic is still a useful reference.
- Gerhard Burde and Heiner Zieschang, *Knots*, De Gruyter Studies in Mathematics 5, second edition, 2003.
This book on knots contains a very readable chapter on braid groups.
- Patrick Dehornoy, Ivan Dynnikov, Dale Rolfsen, and Bert Wiest, *Ordering Braids*, Mathematical Surveys and Monographs, Amer. Math. Soc. (2008).
More than you ever wanted to know about braid ordering appears in this monograph.

- Vaughan F. R. Jones, *Subfactors and Knots*, CBMS Regional Conference series in Mathematics, Amer. Math. Soc., 1991.
This gem focuses on the connection between operator algebras and knot theory, via the braid groups.
- Vassily Manturov, *Knot Theory*, Chapman & Hall, 2004.
- Kunio Murasugi and Bohdan Kurpita, *A Study of Braids*, Mathematics and Its Applications, Springer, 1999.
Also see research papers and other books in the reference section.

2. Braids as Strings, Dances or Symbols

One of the interesting things about the braid groups B_n is they can be defined in so many ways, each providing a unique insight. We will briefly describe some of these definitions, punctuated by facts about B_n which are revealed from the various points of view. You can check the excellent references [1, 2, 5, 7, 11, 17] for more information.

2.1. Definition 1: Braids as strings in 3-D

This is the usual and visually appealing picture. An n -braid is a collection of n strings in (x, y, t) -space, which are disjoint and monotone in (say) the t direction.

We require that the endpoints of the strings are at fixed points, say the points $(k, 0, 0)$ and $(k, 0, 1)$, $k = 1, \dots, n$. We also regard two braids to be equivalent (informally, we will say they are equal) if one can be deformed to the other through the family of braids, with endpoints fixed throughout the deformation.

Although most draw braids vertically, we prefer to view them horizontally with the t -axis running from left to right. The reason is that we do algebra (as in writing) from left to right, and the multiplication of braids is accomplished by concatenation (which is made more explicit in the second definition below), which we take to be in the same order as the product. In the vertical point of view, some view the product $\alpha\beta$ of two braids α and β with α above β , while others would put β on top of α . The horizontal convention eliminates this ambiguity.

There is, of course, a strong connection between braids and knots. A braid β defines a knot or link $\hat{\beta}$, its closure, by connecting the endpoints in a standard way, without introducing further interaction between the strings.

Equivalent braids give rise to equivalent links, but different braids may give rise to the same knot or link. We will discuss how to deal with this

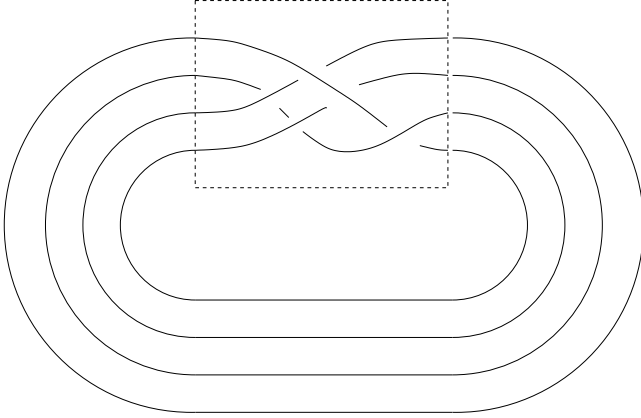


Fig. 1. The closure of a braid.

ambiguity later. B_n will denote the group formed by n -braids with concatenation as the product, which we will soon verify has the properties of a group, namely, an associative multiplication, with identity element and inverses.

2.2. Definition 2: Braids as particle dances

If we take t as a time variable, then a braid can be considered to be the time history of particles moving in the (x, y) plane, or if you prefer, the complex plane, with the usual notation $x + y\sqrt{-1}$.

This gives the view of a braid as a dance of noncolliding particles in \mathbb{C} , beginning and ending at the integer points $\{1, \dots, n\}$. We think of the particles moving in trajectories

$$\beta(t) = (\beta_1(t), \dots, \beta_n(t)), \quad \beta_i(t) \in \mathbb{C},$$

where t runs from 0 to 1, and $\beta_j(t) \neq \beta_k(t)$ when $j \neq k$. A *braid* is then such a time history, or dance, of noncolliding particles in the plane which end at the spots they began, but possibly permuted. Equivalence of braids roughly reflects the fact that choreography does not specify precise positions of the dancers, but rather their relative positions. However, notice that if particle j and $j + 1$ interchange places, rotating clockwise, and then do the same move, but counterclockwise, then their dance is equivalent to just standing still!

The product of braids can be regarded as one dance following the other, both at double speed. Formally, if α and β are braids, we define their

product $\alpha\beta$ (in the notation of this definition) to be the braid which is $\alpha(2t)$ for $0 \leq t \leq 1/2$ and $\beta(2t - 1)$ for $1/2 \leq t \leq 1$.

Exercise 2.1. Verify that the product is associative, up to equivalence. The identity braid is to stand still, and each dance has an inverse; doing the dance in reverse. More formally, if β is a braid, as defined in this section, define $\bar{\beta}(t) = \beta(1 - t)$. Write a formula for the product $\gamma = \beta\bar{\beta}$ and verify that there is a continuous deformation from γ to the identity braid. [Hint: Let s be the deformation parameter, and consider the dance which is to perform β up till time $s/2$, then stand still until time $1 - s/2$, then do the dance $\bar{\beta}$ in the remaining time.]

A braid β defines a permutation $i \rightarrow \beta_i(1)$ which is a well-defined element of the permutation group Σ_n . This is a homomorphism $B_n \rightarrow \Sigma_n$ with kernel, by definition, the subgroup $P_n < B_n$ of *pure* braids. P_n is sometimes called the *colored* braid group, as the particles can be regarded as having identities, or colors. P_n is of course normal in B_n , of index $n!$, and there is an exact sequence

$$1 \rightarrow P_n \rightarrow B_n \rightarrow \Sigma_n \rightarrow 1.$$

Exercise 2.2. Show that any braid is equivalent to a piecewise-linear braid. Moreover, one may assume that under the projection $p : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ given by $p(x, y, t) = (y, t)$, there are only a finite number of singularities of p restricted to the (image of the) given braid. One may assume these are all double points, where a pair of strings intersect transversely, and at different t -values.

Exercise 2.3. Viewing the projection in the (y, t) -plane, with the t -axis as horizontal, for any fixed value of t at which a crossing does not occur, label the strings $1, 2, \dots, n$ counting from the bottom to the top in the y direction. Let σ_i for $i = 1, \dots, n-1$ denote the braid with all strings horizontal, except that the string $i + 1$ crosses over the i string, resulting in the permutation $i \leftrightarrow i + 1$ in the labels of the strings. (Think of it as a right-hand screw motion of these two strings. Argue that any braid is equivalent to a product of these “generators” of the braid group.) [In Fig. 1, for example, the braid could be written either as $\sigma_2^{-1}\sigma_1^{-1}\sigma_3\sigma_2\sigma_1^{-1}$ or $\sigma_2^{-1}\sigma_3\sigma_1^{-1}\sigma_2\sigma_1^{-1}$ (or indeed many other ways).]

Finally, note that the inverse of σ_i is the braid with all strings horizontal, except that the string i crosses over the $i + 1$ string. The first sketch in Fig. 2 shows that these are indeed inverse to each other.

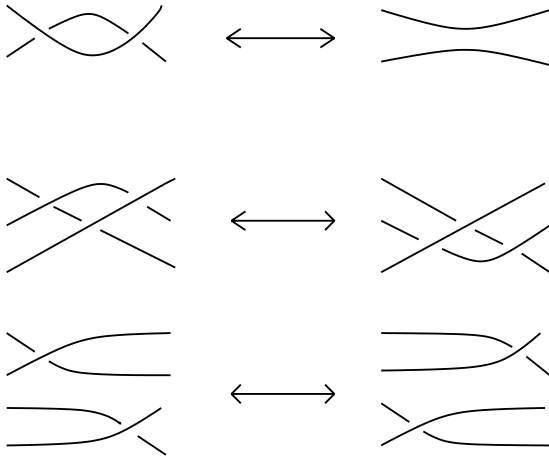


Fig. 2. Equivalent braids.

2.3. Definition 3: The algebraic braid group

B_n can be regarded algebraically as the group presented with generators $\sigma_1, \dots, \sigma_{n-1}$, where σ_i is the braid described in the previous exercise. These generators are subject to the relations (as suggested in Fig. 2):

$$\sigma_i \sigma_j = \sigma_j \sigma_i, \quad |i - j| > 1,$$

$$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j, \quad |i - j| = 1.$$

It was proved by Artin that these are a complete set of relations to abstractly define B_n . This means that any relation among the σ_j can be deduced from the above relations.

Exercise 2.4. Verify that, in B_n , all the generators σ_j are conjugate to each other. Show the total degree $deg(\beta)$ which is the sum of the exponents which appear in an expression of β in the σ_j , is well-defined, i.e. independent of the expression. Verify that the abelianization of B_n , for $n \geq 2$, is the infinite cyclic group \mathbb{Z} , and $deg : B_n \rightarrow \mathbb{Z}$ is equivalent to the abelianization homomorphism. Thus the commutator subgroup of B_n consists of all words of total degree zero.

Exercise 2.5. In B_3 , consider the special element $\Delta = \Delta_3 = \sigma_1 \sigma_2 \sigma_1$, which consists of a clockwise “half-twist” of the three strings. Verify that $\Delta \sigma_1 = \sigma_2 \Delta$ and $\Delta \sigma_2 = \sigma_1 \Delta$. Conclude that Δ^2 commutes with both

generators of B_3 and therefore is in the center of B_3 . (It actually generates the center, but we will not prove this.)

Show that in B_3 there are two braids α and β such that $\alpha \neq \beta$ but $\alpha^3 = \beta^3$. What about squares?

Exercise 2.6. For $n \geq 3$, define $\gamma = \gamma_n = (\sigma_1\sigma_2 \cdots \sigma_{n-1})^n$. Draw this braid and convince yourself that it is a “full-twist” and that γ is central in B_n .

In fact γ_n generates the (infinite cyclic) center of B_n .

We can take a whole countable set of generators $\sigma_1, \sigma_2, \dots$ subject to the above relations, which defines the infinite braid group B_∞ . If we consider the (non-normal) subgroup generated by $\sigma_1, \dots, \sigma_{n-1}$, these algebraically define B_n . Notice that this convention gives “natural” inclusions $B_n \subset B_{n+1}$ and $P_n \subset P_{n+1}$.

Exercise 2.7. Does B_∞ have a nontrivial center?

Going the other way, if one forgets the last string of an $(n+1)$ -braid the result is an n -braid. But strictly speaking, this is only a well-defined homomorphism for pure braids, (or at best for the subgroup of braids in which the string beginning at the point $n+1$ also ends there). Later, we will have a use for this forgetful map

$$f : P_{n+1} \rightarrow P_n.$$

It is easy to see that f is a left inverse of the inclusion, or in other words a retraction in the category of groups.

2.4. Artin combing

We now have the ingredients for the combing technique, which gives a solution to the word problem for pure braid groups, and therefore for the full braid groups.

Solving the word problem in B_n reduces to P_n : Given a word in the σ_j , first work out its corresponding permutation. If the permutation is non-trivial, so is the group element it represents. If trivial, the braid is a pure braid, and we have reduced the problem to the word problem for P_n .

Let β be a pure n -braid and $f(\beta)$ the pure $n-1$ braid obtained by forgetting the last string, but then by inclusion, regard $f(\beta)$ in P_n . Then β and $f(\beta)$ can be visualized as the same braid, except the last string has been changed in $f(\beta)$ so as to have no interaction with the other strings.

Let K be the kernel of f . Then it is easy to verify that $f(\beta)^{-1}\beta \in K$ and the map

$$\beta \rightarrow (f(\beta), f(\beta)^{-1}\beta)$$

maps P_n bijectively onto the cartesian product $P_{n-1} \times K$. However, the multiplicative structure is that of a *semidirect* product, as happens whenever we have a split exact sequence of groups, in this case

$$1 \rightarrow K \rightarrow P_n \rightarrow P_{n-1} \rightarrow 1.$$

Also notice that every element of K can be represented by a braid in which the first $n - 1$ strands go straight across. In this way we identify K with the fundamental group of the complement of the points $\{1, \dots, n - 1\}$ in the plane, which is a free group: $K \cong F_{n-1}$.

Exercise 2.8. Draw the braid $\alpha_i = \sigma_{n-1}\sigma_{n-2} \cdots \sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1} \cdots \sigma_{n-2}^{-1}\sigma_{n-1}^{-1}$ and verify that $\alpha_1, \dots, \alpha_{n-1}$ represent a free basis for the group K above.

To solve the word problem in P_n : let $\beta \in P_n$ be a braid expressed in the standard generators σ_i ; the goal is to decide whether β is really the identity. Consider its image $f(\beta)$, which lies in P_{n-1} . We may assume inductively that the word problem is solved in P_{n-1} . If $f(\beta) \neq 1$ we are done, knowing that $\beta \neq 1$.

On the other hand, if $f(\beta) = 1$, that means that β lies in the kernel K , which is a free group. Express β as a product of the generators α_i in K , and then we can decide if β is the identity, as K is freely generated by the α_i .

The semidirect product decomposition process can be iterated on P_{n-1} to obtain the Artin normal form: P_n is an iterated semidirect product of free groups F_1, F_2, \dots, F_{n-1} . Thus every $\beta \in P_n$ has a unique expression

$$\beta = \beta_1\beta_2 \cdots \beta_{n-1}$$

with $\beta_i \in F_i$.

For later reference, we will call the vector

$$(\beta_1, \beta_2, \dots, \beta_{n-1})$$

the ‘‘Artin coordinates’’ of β .

In the above discussion, the subgroup F_j of P_{j+1} (with $j < n$) consists of the pure braids in the subgroup P_{j+1} of P_n , which become trivial if the strand labeled $j + 1$ is removed. A set of generators for F_j is given by the

braids α_{ij} , $i < j$, which link the i and j strands over the others:

$$\alpha_{ij} = \sigma_{j-1}\sigma_{j-2}\cdots\sigma_{i+1}\sigma_i^2\sigma_{i+1}^{-1}\cdots\sigma_{j-2}^{-1}\sigma_{j-1}^{-1}.$$

Note that α_{in} is just the braid we called α_i above.

The semidirect product decomposition permits us to write a finite presentation for P_n . An example is the following:

Generators are α_{ij} with $1 \leq i < j \leq n$.

Relations are:

$$\alpha_{ij}\alpha_{ik}\alpha_{jk} = \alpha_{ik}\alpha_{jk}\alpha_{ij} = \alpha_{jk}\alpha_{ij}\alpha_{ik} \text{ whenever } 1 \leq i < j < k \leq n.$$

$$\alpha_{ij}\alpha_{kl} = \alpha_{kl}\alpha_{ij} \text{ and } \alpha_{il}\alpha_{jk} = \alpha_{jk}\alpha_{il} \text{ whenever } 1 \leq i < j < k < l \leq n.$$

$$\alpha_{ik}\alpha_{jk}\alpha_{jl}\alpha_{jk}^{-1} = \alpha_{jk}\alpha_{jl}\alpha_{jk}^{-1}\alpha_{ik} \text{ whenever } 1 \leq i < j < k < l \leq n.$$

Exercise 2.9. Verify these relations for specific values of i, j, k and l and convince yourself that they are “obvious”.

Exercise 2.10. Show that the abelianization of P_n is free abelian of rank $\binom{n}{2}$. Conclude that the set of generators for P_n given above is minimal: no smaller set of generators is possible.

Exercise 2.11. By contrast, show that the full braid group B_n can be generated by just two generators. Hint: Recall that the generators σ_i are all conjugates in B_n .

It may seem strange that even though P_n is a subgroup of B_n , its abelianization is, in general, considerably larger. An even more striking example of this phenomenon can be obtained from the free group on two generators, together with its commutator subgroup, which is an infinitely generated free group. After abelianization they become, respectively, \mathbb{Z}^2 and \mathbb{Z}^∞ .

We mention an important theorem of W. Thurston. An infinite group is called *automatic* if it is well-modeled (in a well-defined technical sense which we will not elaborate here) by a finite-state automaton. The standard reference is [10].

Theorem 2.12 (Thurston). B_n is automatic.

This implies, for example, that the word problem can be solved by an algorithm which is quadratic in the length of the input.

Exercise 2.13. What is the complexity of the Artin combing algorithm?

Exercise 2.14. Show that K is not normal in B_n , but is normalized by the subgroup B_{n-1} . Moreover, the action of B_{n-1} on K by conjugation is essentially the same as the Artin presentation, given in the next section.

3. Mapping Class Groups and Braids

3.1. Definition 4: B_n as a mapping class group

Going back to the second definition, imagine the particles are in a sort of planar jello and pull their surroundings with them as they dance about. Topologically speaking, the motion of the particles extends to a continuous family of homeomorphisms of the plane (or of a disk, fixed on the boundary). This describes an equivalence between B_n and the mapping class of D_n , the disk D with n punctures (marked points). That is, B_n can be considered as the group of homeomorphisms of D_n fixing ∂D and permuting the punctures, modulo isotopy fixing $\partial D \cup \{1, \dots, n\}$.

3.2. Definition 5: B_n as a group of automorphisms

A mapping class $[h]$, where $h : D_n \rightarrow D_n$, gives rise to an automorphism $h_* : F_n \rightarrow F_n$, where F_n is the fundamental group of the punctured disk, a free group of rank n . Using the interpretation of braids as mapping classes, this defines a homomorphism

$$B_n \rightarrow \text{Aut}(F_n),$$

which Artin showed to be faithful, i.e. injective.

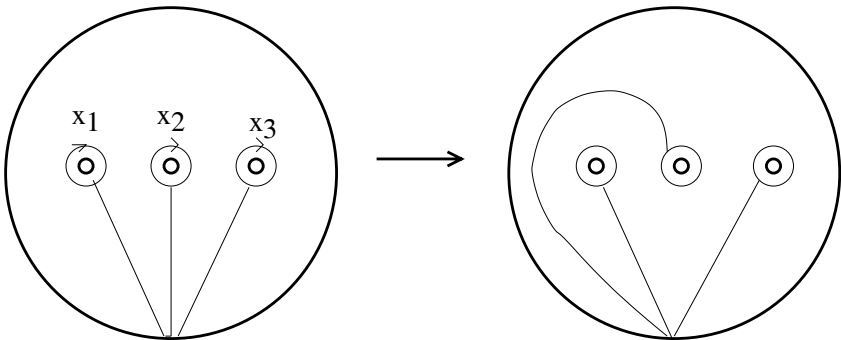


Fig. 3. The action of σ_1 on D_3 .

The generator σ_i acts as

$$\begin{aligned} x_i &\rightarrow x_i x_{i+1} x_i^{-1} \\ x_{i+1} &\rightarrow x_i \\ x_j &\rightarrow x_j, j \neq i, i+1. \end{aligned} \tag{3.1}$$

This is shown in the figure above, for the case $n = 3$, and the action of σ_1 .

Theorem 3.1 (Artin). *Under the identification described above, B_n is the set of automorphisms $h \in \text{Aut}(F_n)$ of the form*

$$h(x_i) = w_j^{-1} x_j w_j,$$

where w_j are words in F_n , and satisfying $h(x_1 \cdots x_n) = x_1 \cdots x_n$.

The last equation of Artin's theorem reflects the fact that h comes from a map that is fixed on the boundary.

This point of view gives further insight into the group-theoretic properties of braid groups. A group G is *residually finite* if for every nonidentity element $g \in G$ there is a homomorphism $h : G \rightarrow F$ onto a finite group F such that $h(g)$ is not the identity. In other words, any element other than the identity can be proved nontrivial by looking at some homomorphism of G to a finite group.

Exercise 3.2. Show that subgroups of residually finite groups are residually finite.

Exercise 3.3. Show that the automorphism group of any finitely generated residually finite group is itself residually finite. [This is a result of Baumslag. You may want to consult [21] for a proof, and further discussion on the subject.]

Exercise 3.4. Show that finitely-generated abelian groups are residually finite. The matrices $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ generate a free group in the group $SL(2, \mathbb{Z})$, two-by-two integral matrices with determinant 1, which is a group of automorphisms of \mathbb{Z}^2 . Thus $SL(2, \mathbb{Z})$ is residually finite and so is the rank 2 free group. Conclude that a free group of any finite or countable rank is residually finite.

From these observations, we see that $\text{Aut}(F_n)$ is residually finite and conclude the following.

Theorem 3.5. B_n is residually finite.

A group G is said to be Hopfian if it is not isomorphic with any nontrivial quotient group. In other words, if $G \rightarrow H$ is any surjective homomorphism with nontrivial kernel, then $H \cong G$.

Exercise 3.6. A finitely-generated residually finite group is Hopfian.

It follows immediately that

Theorem 3.7. B_n is Hopfian.

3.3. The word problem

If a group G is given by generators, say $\{g_i\}$, and relations, it may be difficult to determine whether two words in the generators actually represent the same element of G . This is called the *word problem*. It easily reduces to the question: given a word in the g_i , does it represent the identity element of G ?

If G is residually finite, then in principle a given word which does *not* represent the identity, can be proven so by finding a homomorphism of G onto a finite group in which the word is sent to a nontrivial element, where verifying this is a finite problem. Of course, finding such a homomorphism may well be terribly difficult. But for particular groups there may be more algorithmic methods for solving the word problem. Giving such an algorithm, for a particular group, or class of groups, is what is meant by a *solution* to the word problem.

Such solutions exist for free groups and for the braid groups. First, consider a free group, with free generators $\{x_i\}$. If w is a given word in these generators, simply perform all free cancellations which are possible: that is, remove any two consecutive letters which happen to be $x_i x_i^{-1}$ or $x_i^{-1} x_i$. Continue doing this until no such cancellations are possible. If the result is the empty word, w represents the identity; otherwise it does not.

Artin's theorem provides a means for solving the word problem algorithmically in B_n by reducing it to several word problems in a free group. Suppose a word w in the Artin generators σ_i is given. Then we may consider w to be an automorphism of the free group F_n . Using equations (3.1), we can explicitly calculate the values $w(x_1), \dots, w(x_n)$ as words in the x_i . We can then solve the word problem n times in F_n to decide whether $w(x_i) = x_i$ for each $i = 1, \dots, n$. If this is the case, w represents the identity of B_n ; otherwise, it does not.

Another solution to the word problem in braid groups, again reducing it to free groups, will be discussed later, using the technique called "Artin

combing”. Yet another, due to Garside, also solves the so-called *conjugacy* problem, which is to decide whether two given words in the generators are conjugates in the group. We will not discuss Garside’s method here, as it is covered quite thoroughly in the notes on cryptography in this workshop.

3.4. The modular group

There is an interesting connection between the braid group B_3 and two-by-two integral matrices.

Consider the matrices

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad T = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

One can easily check that $S^2 = -I = T^3$. These matrices generate cyclic subgroups of $SL(2, \mathbb{Z})$, \mathbb{Z}_4 and \mathbb{Z}_6 , respectively (we use the abbreviation $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$). It is well-known that, using the generators S and T , there is an amalgamated free product structure

$$SL(2, \mathbb{Z}) \cong \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6.$$

The *modular group* $PSL(2, \mathbb{Z})$ is the quotient of $SL(2, \mathbb{Z})$ by its center $\{\pm I\}$. One can also regard $PSL(2, \mathbb{Z})$ as the group of Möbius transformations of the complex plane

$$z \mapsto \frac{az + b}{cz + d} \quad \text{corresponding to} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL(2, \mathbb{Z}).$$

The modular group has the structure of a free product $\mathbb{Z}_2 * \mathbb{Z}_3$, with (the cosets of) S and T generating the respective factors.

Exercise 3.8. Show that the braid group $B_3 \cong \langle \sigma_1, \sigma_2 | \sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2 \rangle$ also has the presentation $\langle x, y | x^2 = y^3 \rangle$, by finding appropriate expressions of x, y in terms of σ_1, σ_2 , and vice versa, so that the transformations respect the relations and are mutual inverses.

Verify that the element $x^2 (= y^3)$ is central in B_3 and in fact generates the center of B_3 .

Show that B_3 modulo its center is isomorphic with $PSL(2, \mathbb{Z})$.

3.5. Definition 6: B_n as a fundamental group

In complex n -space \mathbb{C}^n consider the big diagonal

$$\Delta = \{(z_1, \dots, z_n); z_i = z_j, \text{ some } i < j\} \subset \mathbb{C}^n.$$

Using the basepoint $(1, 2, \dots, n)$, we see that

$$P_n = \pi_1(\mathbb{C}^n \setminus \Delta).$$

In other words, pure braid groups are fundamental groups of complements of a special sort of complex *hyperplane arrangement*, itself a deep and beautiful subject.

To get the full braid group we need to take the fundamental group of the *configuration space*, of orbits of the obvious action of Σ_n upon $\mathbb{C}^n \setminus \Delta$. Thus

$$B_n = \pi_1((\mathbb{C}^n \setminus \Delta)/\Sigma_n).$$

Notice that since the singularities have been removed, the projection

$$\mathbb{C}^n \setminus \Delta \longrightarrow (\mathbb{C}^n \setminus \Delta)/\Sigma_n$$

is actually a covering map. As is well-known, covering maps induce injective homomorphisms at the π_1 level, so this is another way to think of the inclusion $P_n \subset B_n$.

It was observed in [13] that $\mathbb{C}^n \setminus \Delta$ has trivial homotopy groups in dimension greater than one. That is, it is an Eilenberg-MacLane space, also known as a $K(P_n, 1)$. Therefore its cohomology groups coincide with the group cohomology of P_n . By covering theory, the quotient space $(\mathbb{C}^n \setminus \Delta)/\Sigma_n$ also has trivial higher homotopy, so it is a $K(B_n, 1)$. Since these spaces have real dimension $2n$, this view of braid groups gives us the following observation.

Theorem 3.9. *The groups B_n and P_n have finite cohomological dimension.*

If a group contains an element of finite order, standard homological algebra implies that the cohomological dimension of the group must be infinite. Thus there are no braids of finite order.

Corollary 3.10. *The braid groups are torsion-free.*

Finally, we note that the space $(\mathbb{C}^n \setminus \Delta)/\Sigma_n$ can be identified with the space of all complex polynomials of degree n which are monic and have n distinct roots

$$p(z) = (z - r_1) \cdots (z - r_n).$$

This is one way in which the braid groups play a role in classical algebraic geometry, as fundamental groups of such spaces of polynomials.

3.6. Definition 7: The fundamental group of a space of polynomials

B_n is the fundamental group of the space of all monic polynomials of degree n with complex coefficients and only simple roots.

3.7. Surface braids

Let Σ denote a surface, with or without boundary. One can define a braid on Σ in exactly the same way as on a disk — namely, a collection of disjoint paths $\beta_1(t), \dots, \beta_n(t)$ in $\Sigma \times I$, with each $\beta_i(t) \in \Sigma \times \{t\}$ so that they begin and end at the same points of Σ , possibly permuted. They form a group, which is usually denoted $B_n(\Sigma)$.

The subgroup of braids for which the permutation of the points is the identity is the *pure* surface braid group $P_n(\Sigma)$. Thus $B_n(D^2)$ and $P_n(D^2)$ are the classical Artin braid groups which we have discussed before. Much of the above discussion holds for surface braid groups; for example, they may be interpreted as fundamental groups of configuration spaces.

On the other hand, there are differences. For example the braid groups of the sphere S^2 and the projective plane $\mathbb{R}P^2$ have elements of finite order. Van Buskirk showed that these are the only closed surfaces to have torsion in their braid groups, however. There are finite presentations for surface braid groups in the literature, and these groups are currently an active area of research. One reason for their interest is that they play an important part in certain topological quantum field theories (TQFT's).

4. Knot Theory, Braids and the Jones Polynomial

4.1. Knots and Reidemeister moves

One often pictures a knot or link by drawing a projection onto the plane, with only double points, and indicating which string goes under by putting a small gap in it, as in Fig. 1. If one deforms the plane by a planar isotopy, an equivalent projection results. One can also make local changes to a knot diagram. The first two vignettes in Fig. 2 are sometimes called Reidemeister moves of types 2 and 3 (respectively). One can remember the numbering, as type 2 involves two strands and type 3 involves three. There is also a type 1 Reidemeister move.

Theorem 4.1 (Reidemeister). *Two knot diagrams present equivalent knots if and only if one can be transformed to the other by a finite sequence of Reidemeister moves (plus an isotopy of the plane).*

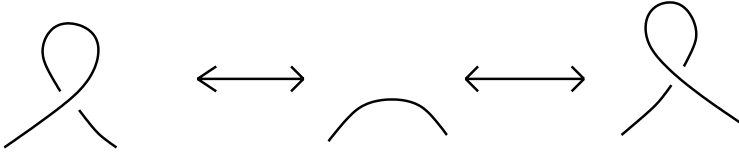


Fig. 4. Reidemeister move of type 1.

4.2. Markov moves

It has already been mentioned that different braids can, upon forming the closure, give rise to the same knot or link. You can easily convince yourself that if α and β are n -string braids, then the closure of $\alpha^{-1}\beta\alpha$ is equivalent to the closure of β . Because of the trivial strings added in forming the closure, α and its inverse can annihilate each other! Therefore we see that conjugate braids close to the same link.

Another example of this phenomenon is to consider the n -braid β as an element of B_{n+1} by adding a trivial string at the top, and compare the original closure $\hat{\beta}$ with the closure of $\beta \times \sigma_n$, the latter braid taken in B_{n+1} . If you sketch this, you can easily convince yourself that these result in the same link (up to isotopy). The first move (conjugation) and the second move just described constitute the two Markov moves. They are the key to understanding the connection between braid theory and knot theory. The following theorem is due to J. W. Alexander (first part) and A. A. Markov. A full proof appeared first, to our knowledge, in [5].

Theorem 4.2. *Every knot or link is the closure of some braid. Two braids close to equivalent knots or links if and only if they are related by a finite sequence of the two Markov moves.*

Exercise 4.3. If you want to learn a nice, elementary proof of the above theorem, read the paper [24].

Exercise 4.4. Consider the 3-braid $\beta = \sigma_1\sigma_2$ and identify the knot or link, simplifying, if possible by using Reidemeister moves: $\hat{\beta}$, $\hat{\beta}^2$, $\hat{\beta}^3$. For which integers k is the closure of β^k a knot?

4.3. Kauffman's bracket and Jones polynomial

The original construction of the Jones polynomial involved a family of representations

$$B_n \rightarrow \mathcal{A}$$

of the braid groups into an algebra \mathcal{A} involving a parameter t . This algebra has a linear trace function into the ring of (Laurent) polynomials. The composite of the representation and the trace, together with some correction terms to account for the Markov moves, defined the original Jones polynomial.

We will present this in a sort of reverse order, as there is a very simple derivation of the Jones polynomial discovered a few years later by L. Kauffman. From this, we can define an algebra, called the Temperley-Lieb algebra, and reconstruct what is essentially Jones' representation.

Consider a planar diagram D of a link L , which has only simple transverse crossings. Kauffman's bracket $\langle D \rangle$ is (at first) a polynomial in three commuting variables, a, b and d defined by the equations:

$$\langle \text{crossing} \rangle = a \langle \text{smooth} \rangle + b \langle \text{crossing} \rangle \langle \text{loop} \rangle$$

$$\langle \text{D} \cup \text{O} \rangle = d \langle \text{D} \rangle$$

Fig. 5. Equations defining Kauffman's bracket polynomial.

Some explanation is in order. The vignettes in the brackets in the first equation stand for complete link diagrams, which differ only near the crossing in question. Those on the right side represent diagrams with fewer crossings. In the second equation, one can introduce a closed curve which has no intersections with the remainder of the diagram D , resulting in a diagram whose bracket polynomial is d times the bracket of D .

Exercise 4.5. Verify that the bracket polynomial is well-defined, if we decree that the bracket of a single curve with no crossings is equal to 1.

Exercise 4.6. Show that the bracket will be invariant under the type 2 Reidemeister move, if we have the following relations among the variables:

$$a^2 + b^2 + abd = 0 \quad \text{and} \quad ab = 1.$$

Thus we make the substitutions $b = a^{-1}$ and $d = -a^2 - a^{-2}$ and now consider the bracket to be a Laurent polynomial in the single variable a .

Exercise 4.7. Show that the invariance under the type 2 Reidemeister moves implies the bracket is invariant under the type 3 move, too.

Exercise 4.8. Calculate the bracket of the two trefoil knot diagrams with 3 crossings. Show that they are the same, except for reversal of the sign of the exponents.

Exercise 4.9. Investigate the effect of Reidemeister move 1 on the bracket of a diagram, and show that it changes the bracket by a factor of $-a^{\pm 3}$, the sign of the exponent depending on the sense of the curl removed.

Because of this, one can define a polynomial invariant under all three Reidemeister moves, by counting the number of positive minus the number of negative crossings, and modifying the bracket polynomial by an appropriate factor. A positive crossing corresponds to a (positive) braid generator, if both strings are oriented from left to right. This gives, up to change of variable, the Jones polynomial of the knot. Specifically, we define the writhe of an *oriented* diagram \vec{D} for an oriented knot (or link) \vec{K} to be

$$w(D) = \sum_c \epsilon_c$$

where the sum is over all crossings and $\epsilon_c = 1$ if the crossing c is positive, and -1 if negative. Then we define

$$f_{\vec{K}}(a) = (-a^3)^{-w(\vec{D})} \langle D \rangle.$$

This is an invariant of the oriented link \vec{K} . If K happens to be a knot, it is independent of the orientation, as reorienting both strands of a crossing does not change its sign. It is related to the Jones polynomial $V_K(t)$ by a simple change of variables:

$$V_{\vec{K}}(t) = f_{\vec{K}}(t^{-1/4}).$$

Exercise 4.10. Show that all exponents of a in $\langle D \rangle$ are divisible by 4 if D is a diagram of a knot (or link with an odd number of components). In other cases, they are congruent to 2 mod 4. Thus the Jones polynomial is truly a (Laurent) polynomial in t for knots and odd component links, but a polynomial in \sqrt{t} in the other cases.

5. Representations

This is a very big subject, which we will just touch upon. By a representation of a group we will mean a homomorphism of the group into a group of

matrices, or more generally into some other group, or ring or algebra. Often, but not always, we want the target to be finite-dimensional. We've already encountered the Artin representation $B_n \rightarrow \text{Aut}(F_n)$, which is faithful. Here the target group is far from being "finite-dimensional".

5.1. Jones representation and the Temperley-Lieb algebra

Another very important representation is the one defined by Jones [15] which gave rise to his famous knot polynomial, and the subsequent revolution in knot theory. The version we will discuss is more thoroughly described in [17]; it is based on the Kauffman bracket, an elementary combinatorial approach to the Jones polynomial. First we need to describe the Temperley-Lieb Algebras \mathcal{T}_n , in their geometric form. The elements of \mathcal{T}_n are something like braids: we consider strings in a box, visualized as a square in the plane, endpoints being exactly n specified points on each of the left and right sides. The strings are not required to be monotone, or even to run across from one side to the other. There also may be closed components. Really what we are looking at are "tangle" diagrams. Two tangle diagrams are considered equal if there is a planar isotopy, fixed on the boundary of the square, taking one to the other.

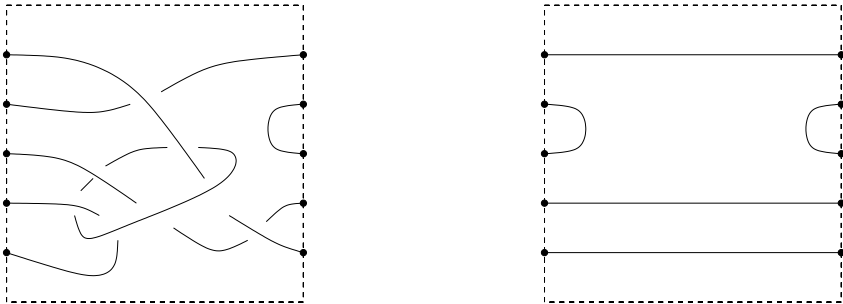


Fig. 6. A typical element in \mathcal{T}_5 and the generator e_3 .

Now we let A be a fixed complex number (regarded as a parameter), and formally define \mathcal{T}_n to be the complex vector space with basis the set of all tangles, as described above, but modulo the following relations, which correspond to similar relations used to define Kauffman's bracket version of the Jones polynomial (we have promoted the variable a to upper case).

$$\begin{aligned}
 \text{X} &= A \text{Y} + A^{-1} \text{Z} \\
 K \cup \bigcirc &= dK, \quad d = -A^2 - A^{-2}
 \end{aligned}$$

Fig. 7. Relations in \mathcal{T}_n .

The first relation means that we can replace a tangle with a crossing by a linear combination of two tangles with that crossing removed in two ways. As usual, the pictures mean that the tangles are identical outside the part pictured. The second relation means that we can remove any closed curve in the diagram, if it does not have any crossings with the rest of the tangle, at the cost of multiplying the tangle by the scalar $-A^2 - A^{-2}$. Using the relations, we see that any element of \mathcal{T}_n can be expressed as a linear combination of tangles which have no crossings and no closed curves — that is, disjoint planar arcs connecting the $2n$ points of the boundary. This gives a finite generating set, which (for generic values of A) can be shown to be a basis for \mathcal{T}_n as a vector space. But there is also a multiplication of \mathcal{T}_n , a concatenation of tangles, in exactly the same way braids are multiplied. This enables us to consider \mathcal{T}_n to be generated *as an algebra* by the elements e_1, \dots, e_{n-1} . In e_i all the strings go straight across, except those at level i and $i + 1$ which are connected by short caps; the generator e_3 of \mathcal{T}_5 is illustrated in Fig. 2. The identity of this algebra is simply the diagram consisting of n horizontal lines (just like the identity braid). \mathcal{T}_n can be described abstractly as the associative algebra with the generators e_1, \dots, e_{n-1} , subject to the relations:

$$e_i e_j = e_j e_i \text{ if } |i - j| > 1 \quad e_i e_{i \pm 1} e_i = e_i \quad e_i^2 = (-A^2 - A^{-2})e_i.$$

It is an enjoyable exercise to verify these relations from the pictures. Now the Jones representation $J : B_n \rightarrow \mathcal{T}_n$ can be described simply by considering a braid diagram as an element of the algebra. In terms of generators, this is just

$$J(\sigma_i) = A + A^{-1}e_i.$$

5.2. The Burau representation

One of the classical representations of the braid groups is the Burau representation, which can be described as follows. Consider the definition of

B_n as the mapping class group of the punctured disk D_n (Definition 4). As already noted, the fundamental group of D_n is a free group, with generator x_i represented by a loop, based at a point on the boundary of the disk, which goes once around the i^{th} puncture. Consider the subgroup of $\pi_1(D_n)$ consisting of all words in the x_i whose exponent sum is zero. This is a normal subgroup, and so defines a regular covering space

$$p: \bar{D}_n \rightarrow D_n.$$

The group of covering translations is infinite cyclic. Therefore, the homology $H_1(\bar{D}_n)$ can be considered as a module over the polynomial ring $\Lambda := \mathbb{Z}[t, t^{-1}]$, where t represents the generator of the covering translation group. Similarly, if $*$ is a basepoint of D_n , the relative homology group $H_1(\bar{D}_n, p^{-1}(*))$ is a Λ -module.

A braid β can be represented as (an isotopy class of) a homeomorphism $\beta : D_n \rightarrow D_n$ fixing the basepoint. This lifts to a homeomorphism $\bar{\beta} : \bar{D}_n \rightarrow \bar{D}_n$, which is unique if we insist that it fix some particular lift of the basepoint. The induced homomorphism on homology, $\bar{\beta}_* : H_1(\bar{D}_n, p^{-1}(*)) \rightarrow H_1(\bar{D}_n, p^{-1}(*))$ is a linear map of these finite-dimensional modules, and so can be represented by a matrix with entries in $\mathbb{Z}[t, t^{-1}]$. The mapping

$$\beta \rightarrow \bar{\beta}_*$$

is the Burau representation of B_n .

Let us illustrate this for the case $n = 3$. D_3 is replaced by the wedge of three circles, which is homotopy equivalent to it, to simplify visualization. The covering space \bar{D}_n is shown as an infinite graph. Although as an abelian group $H_1(\bar{D}_3, p^{-1}(*))$ is infinitely generated, as a Λ -module it has three generators $g_i = \tilde{x}_i$, the lifts of the generators x_i of D_3 , $i = 1, 2, 3$ beginning at some fixed basepoint in $p^{-1}(*)$. The other elements of $H_1(\bar{D}_3, p^{-1}(*))$ are represented by translates $t^n g_i$.

Now consider the action of σ_1 on D_3 , at the fundamental group level. As we saw in Definition 5, σ_{1*} takes x_1 to $x_1 x_2 x_1^{-1}$. Accordingly $\bar{\sigma}_{1*}$ takes g_1 to the lift of $x_1 x_2 x_1^{-1}$, which is pictured in the lower part of the illustration. In terms of homology, this is $g_1 + t g_2 - t g_1$. Therefore

$$\bar{\sigma}_{1*}(g_1) = (1 - t)g_1 + t g_2.$$

Similarly

$$\bar{\sigma}_{1*}(g_2) = g_1, \quad \bar{\sigma}_{1*}(g_3) = g_3.$$

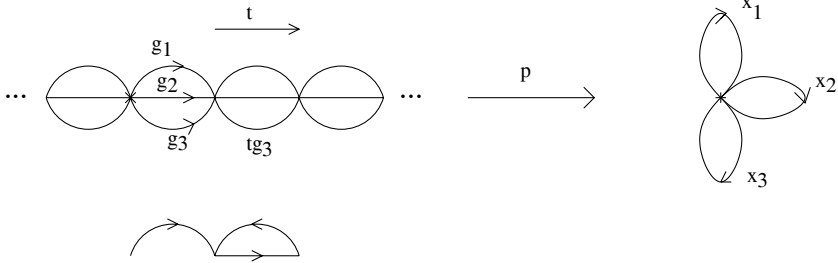


Fig. 8. Illustrating the Burau representation for $n = 3$.

Exercise 5.1. Show that, with appropriate choice of basis, the Burau representation of B_n sends σ_j to the matrix

$$I_{j-1} \oplus \begin{bmatrix} 1-t & t \\ 1 & 0 \end{bmatrix} \oplus I_{n-j-1},$$

where I_k denotes the $k \times k$ identity matrix.

A probabilistic interpretation. Vaughan Jones offered the following interpretation of the Burau representation, which we will modify slightly because we have chosen opposite crossing conventions. Picture a braid as a system of trails which cross only at bridges, where one goes over the other. Wherever one trail crosses under another there is a probability t that a person will jump from the lower trail to the upper trail; the probability of staying on the same trail is $1 - t$. The i, j entry of the Burau matrix corresponding to a braid then represents the probability that, if a person starts on the trail at position i , she will finish on the trail at position j .

It has been known for many years that this representation is faithful for $n \leq 3$, and it is only within the last decade that it was found to be unfaithful for any n at all. John Moody [23] showed in 1993 that it is unfaithful for $n \geq 9$. This has since been improved by Long and Paton [20] and more recently by Bigelow to $n \geq 5$. The case $n = 4$ remains open, at the time of this writing.

5.3. Linearity of the braid groups

It has long been questioned, whether the braid groups are *linear*, meaning that there is a faithful representation $B_n \rightarrow GL(V)$ for some finite-dimensional vector space V . A candidate had been the so-called Burau representation, but as already mentioned it has been known for several years that Burau is unfaithful, in general.

The question was finally settled recently by Daan Krammer and Stephen Bigelow, using equivalent representations, but different methods. They use a representation defined very much like the Burau representation. But instead of a covering of the punctured disk D_n , they use a covering of the *configuration space* of pairs of points of D_n , upon which B_n also acts. This action induces a linear representation in the homology of an appropriate covering, and provides just enough extra information to give a faithful representation!

Theorem 5.2 (Krammer [19], Bigelow [4]). *The braid groups are linear.*

In fact, Bigelow has announced that the BMW representation (Birman, Murakami, Wenzl) [6] is also faithful. Another open question is whether the Jones representation $J : B_n \rightarrow \mathcal{T}_n$, discussed earlier, is faithful.

6. Ordering Braid Groups

This is, to me, one of the most exciting of the recent developments in braid theory. Call a group G *right orderable* if its elements can be given a strict total ordering $<$ which is right-invariant:

$$\forall x, y, z \in G, \quad x < y \Rightarrow xz < yz.$$

Theorem 6.1 (Dehornoy [8]). *B_n is right-orderable.*

Interestingly, we know of three quite different proofs. The first is Dehornoy's, the second is one that was discovered jointly by myself and four other topologists. We were trying to understand difficult technical aspects of Dehornoy's argument, then came up with quite a different way of looking at exactly the same ordering, but using the view of B_n as the mapping class group of the punctured disk D_n . Yet a third way is due to Thurston, using the fact that the universal cover of D_n embeds in the hyperbolic plane. Here are further details.

6.1. Dehornoy's approach

It is routine to verify that a group G is right-orderable if and only if there exists a subset Π (positive cone) of G satisfying:

- (1) $\Pi \cdot \Pi = \Pi$.
- (2) The identity element does not belong to Π , and for every $g \neq 1$ in G exactly one of $g \in \Pi$ or $g^{-1} \in \Pi$ holds.

One defines the ordering by $g < h$ iff $hg^{-1} \in \Pi$.

Exercise 6.2. Verify that the transitivity law holds, and that the ordering is right-invariant. Show that the ordering defined by this rule is also left-invariant if and only if $g\Pi g^{-1} = \Pi$ for every $g \in G$; that is, Π is “normal”.

Dehornoy’s idea is to call a braid i -positive if it is expressible as a word in $\sigma_j, j \geq i$ in such a manner that all the exponents of σ_i are positive. Then define the set $\Pi \subset B_n$ to be all braids which are i -positive for some $i = 1, \dots, n - 1$. To prove (1) above is quite easy, but (2) requires an extremely tricky argument.

6.2. Ordering braids as mapping classes

Here is the point of view advocated in [12]. Consider B_n as acting on the complex plane, as described above. Our idea is to consider the image of the real axis $\beta(\mathbb{R})$, under a mapping class $\beta \in B_n$. Of course there are choices here, but there is a unique “canonical form” in which (roughly speaking) $\mathbb{R} \cap \beta(\mathbb{R})$ has the fewest number of components. Now declare a braid β to be positive if (going from left to right) the first departure of the canonical curve $\beta(\mathbb{R})$ from \mathbb{R} itself is into the *upper* half of the complex plane. Amazingly, this simple idea works, and gives exactly the same ordering as Dehornoy’s combinatorial definition.

6.3. Braids acting on the real line

Finally, Thurston’s idea for ordering B_n again uses the mapping class point of view, but a different way at looking at ordering a group. This approach, which has the advantage of defining infinitely many right-orderings of B_n is described by H. Short and B. Wiest in [29]. The Dehornoy ordering (which is discrete) occurs as one of these right-orderings – others constructed in this way are order-dense. A group G acts on a set X (on the right) if the mapping $x \rightarrow xg$ satisfies: $x(gh) = (xg)h$ and $x1 = x$. An action is *effective* if the only element of G which acts as the identity is the identity $1 \in G$. The following is a useful criterion for right-orderability:

Lemma 6.3. *If the group G acts effectively on \mathbb{R} by order-preserving homeomorphisms, then G is right-orderable.*

By way of a proof, consider a well-ordering of the rational numbers. Define, for g and $h \in G$,

$$g < h \Leftrightarrow xg < xh \quad \text{at the first } x \in \mathbb{Q} \text{ such that } xg \neq xh.$$

It is routine to verify that this defines a right-invariant strict total ordering of G . (By the way, we could have used any ordered set in place of \mathbb{R} .)

The universal cover \tilde{D}_n of D_n can be embedded in the hyperbolic plane \mathbb{H}^2 in such a way that the covering translations are isometries. This gives a hyperbolic structure on D_n . It also gives a beautiful tiling of \mathbb{H}^2 , illustrated in Fig. 9 for the case $n = 2$.

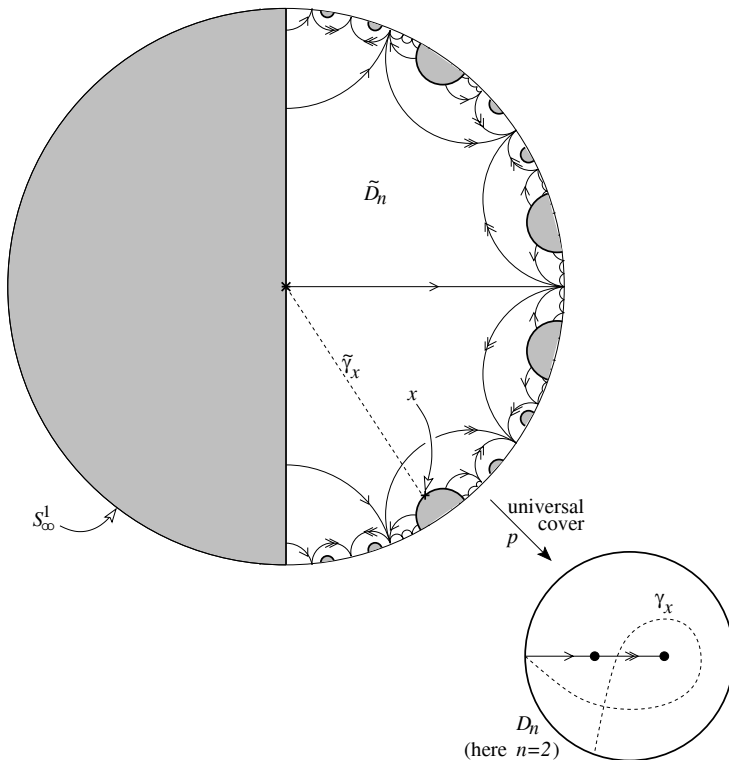


Fig. 9. The universal cover of a twice-punctured disk, with a lifted geodesic. (Courtesy of H. Short and B. Wiest [29].)

Choose a basepoint $* \in \partial D$ and a specific lift $\tilde{*} \in \mathbb{H}^2$. Now a braid is represented by a homeomorphism of D_n , which fixes $*$. This homeomorphism lifts to a homeomorphism of \tilde{D}_n , unique if we specify that it fixes $\tilde{*}$. In turn, this homeomorphism extends to a homeomorphism of the boundary of \tilde{D}_n . But in fact, this homeomorphism fixes the interval of $\partial \tilde{D}_n$ containing

$\tilde{*}$, and if we identify the complement of this interval with the real line \mathbb{R} , a braid defines a homeomorphism of \mathbb{R} . This defines an action of B_n upon \mathbb{R} by order-preserving homeomorphisms, and hence a right-invariant ordering of B_n .

6.4. Two-sided invariance

Any right-invariant ordering of a group can be converted to a left-invariant ordering, by comparing inverses of elements, but that ordering is in general different from the given one. We will say that a group G with strict total ordering $<$ is fully-ordered, or *bi-ordered*, if

$$x < y \Rightarrow xz < yz \quad \text{and} \quad zx < zy, \quad \forall x, y, z \in G.$$

There are groups which are right-orderable but not bi-orderable — in fact the braid groups!

Proposition 6.4 (N. Smythe). *For $n > 2$ the braid group B_n cannot be bi-ordered.*

The reason for this is that there exists a nontrivial element which is conjugate to its inverse: take $x = \sigma_1\sigma_2^{-1}$ and $y = \sigma_1\sigma_2\sigma_1$ and note that $xyx^{-1} = x^{-1}$. In a bi-ordered group, if $1 < x$ then $1 < yxy^{-1} = x^{-1}$, contradicting the other conclusion $x^{-1} < 1$. If $x < 1$ a similar contradiction arises.

Exercise 6.5. Show that in a bi-ordered group $g < h$ and $g' < h'$ imply $gg' < hh'$. Conclude that if $g^n = h^n$ for some $n \neq 0$, then $g = h$. That is, roots are unique. Use this to give an alternative proof that B_n is not bi-orderable if $n \geq 3$.

Theorem 6.6. *The pure braid groups P_n can be bi-ordered.*

This theorem was first noticed by J. Zhu, and the argument appears in [27], based on the result of Falk and Randall [14] that the pure braid groups are “residually torsion-free nilpotent”. Later, in joint work with Djun Kim, we discovered a really natural, and we think beautiful, way to define a bi-invariant ordering of P_n . That ordering has the special property that, restricted to the pure braids which are also positive in the sense of Garside (expressible in the standard braid generators with no negative exponents), it is a well-ordering. We have already done half the work, by discussing Artin combing. Now we need to discuss ordering of free groups.

6.5. Bi-ordering free groups

Lemma 6.7. *For each $n \geq 1$, the free group F_n has a bi-invariant ordering $<$ with the further property that it is invariant under any automorphism $\phi : F_n \rightarrow F_n$ which induces the identity upon abelianization:*

$$\phi_{ab} = id : \mathbb{Z}^n \rightarrow \mathbb{Z}^n .$$

The construction depends on the Magnus expansion of free groups into rings of formal power series. Let F be a free group with free generators x_1, \dots, x_n . Let $Z[[X_1, \dots, X_n]]$ denote the ring of formal power series in the *non-commuting* variables X_1, \dots, X_n .

Each term in a formal power series has a well-defined (total) degree, and we use $O(d)$ to denote terms of degree $\geq d$. The subset $\{1 + O(1)\}$ is actually a multiplicative subgroup of $Z[[X_1, \dots, X_n]]$. Moreover, there is a multiplicative homomorphism

$$\mu : F \rightarrow Z[[X_1, \dots, X_n]]$$

defined by

$$\begin{aligned} \mu(x_i) &= 1 + X_i \\ \mu(x_i^{-1}) &= 1 - X_i + X_i^2 - X_i^3 + \dots . \end{aligned} \tag{6.1}$$

There is a very nice proof that μ is injective in [21], as well as discussion of some of its properties. One such property is that commutators have zero linear terms. For example (dropping the μ)

$$\begin{aligned} [x_1, x_2] &= x_1 x_2 x_1^{-1} x_2^{-1} \\ &= (1 + X_1)(1 + X_2)(1 - X_1 + X_1^2 - \dots)(1 - X_2 + X_2^2 - \dots) \\ &= 1 + X_1 X_2 - X_2 X_1 + O(3). \end{aligned} \tag{6.2}$$

Now there is a fairly obvious ordering of $Z[[X_1, \dots, X_n]]$. Write a power series in ascending degree, and within each degree list the monomials lexicographically according to subscripts. Given two series, order them according to the coefficient of the first term (when written in the standard form just described) at which they differ. Thus, for example, 1 and $[x_1, x_2]$ first differ at the $X_1 X_2$ term, and we see that $1 < [x_1, x_2]$. It is not difficult to verify that this ordering, restricted to the group $\{1 + O(1)\}$ is invariant under both left- and right-multiplication.

Exercise 6.8. Write $x_1, x_2 x_1 x_2^{-1}$ and $x_2^{-1} x_1 x_2$ in increasing order, according to the ordering just described.

6.6. Ordering P_n

If α and β are pure n -braids, compare their Artin coordinates (as described earlier)

$$(\alpha_1, \alpha_2, \dots, \alpha_{n-1}) \quad \text{and} \quad (\beta_1, \beta_2, \dots, \beta_{n-1})$$

lexicographically, using within each F_k the Magnus ordering described above. This all needs choices of conventions, for example, for generators of the free groups, described in detail in [18]. The crucial fact is that the action associated with the semidirect product, by automorphisms φ , has the property mentioned in Lemma 6.7. We recall the definition of a positive braid according to Garside: a braid is Garside-positive if it can be expressed as a word in the standard generators σ_i with only positive exponents.

Theorem 6.9 (Kim-Rolfsen). *P_n has a bi-ordering with the property that Garside-positive pure braids are greater than the identity, and the set of all Garside-positive pure braids is well-ordered by the ordering.*

6.7. Algebraic consequences

The orderability of the braid groups has implications beyond what we already knew — e.g. that they are torsion-free. In the theory of representations of a group G , it is important to understand the group algebra $\mathbb{C}G$ and the group ring $\mathbb{Z}G$. These rings also play a role in the theory of Vassiliev invariants. A basic property of a ring would be whether it has (nontrivial) zero divisors. If a group G has an element g of finite order, say $g^p = 1$, but no smaller power of g is the identity, then we can calculate in $\mathbb{Z}G$

$$(1 - g)(1 + g + g^2 + \dots + g^{p-1}) = 1 - g^p = 0$$

and we see that both terms of the left-hand side of the equation are (nonzero) divisors of zero. A long-standing question of algebra is whether the group ring $\mathbb{Z}G$ can have zero divisors if G is torsion-free. We do know the answer for orderable groups:

Exercise 6.10. If R is a ring without zero divisors, and G is a right-orderable group, then the group ring RG has no zero divisors. Moreover, the only units of RG are the monomials rg , $g \in G, r$ a unit of R .

Proposition 6.11 (Malcev, Neumann). *If G has a bi-invariant ordering, then its group ring $\mathbb{Z}G$ embeds in a division algebra, that is, an extension in which all nonzero elements have inverses.*

These results give us new information about the group rings of the braid groups.

Theorem 6.12. $\mathbb{Z}B_n$ has no zero divisors. Moreover, $\mathbb{Z}P_n$ embeds in a division algebra.

A proof of the theorem of Malcev and Neumann [22] can be found in [25].

Exercise 6.13. Which subgroups of $\text{Aut}(F_n)$ are right-orderable?

Of course, $\text{Aut}(F_n)$ itself is not right-orderable, because it has elements of finite order, e.g. permuting the generators.

6.8. Incompatibility of the orderings

A final note regarding orderings: As we have seen, the methods we have used for ordering B_n and P_n are quite different. One might hope there could be compatible orderings: a bi-ordering of P_n which extends to a right-invariant ordering of B_n . But, in recent work with Akbar Rhemtulla [26], we showed this is hopeless! This result was found independently by Dubrovina and Dubrovin [9].

Theorem 6.14 (Rhemtulla, Rolfsen). For $n \geq 5$, there is no right-invariant ordering of B_n , which, upon restriction to P_n , is also left-invariant.

Acknowledgments

The author wishes to thank the organizers of the summer school and conference at NUS, firstly for the honor of being invited to give the lectures upon which these notes are based, and secondly for their wonderful hospitality and efficiency which made it a memorable scientific event.

References

1. E. Artin, Theorie der Zöpfe, *Abh. Math. Sem. Hamburg. Univ.* 4 (1926), 47–72.
2. E. Artin, Theory of braids, *Annals of Math. (2)* 48 (1947), 101–126.
3. G. Baumslag, Automorphism groups of residually finite groups, *J. London Math. Soc.* 38 (1963), 117–118.
4. S. J. Bigelow, Braid groups are linear, *J. Amer. Math. Soc.* 14 (2001), no. 2, 471–486 (electronic).
5. J. Birman, *Braids, Links and Mapping Class Groups*, Annals of Math. Studies 82, Princeton Univ. Press, 1974.

6. J. Birman and H. Wenzl, Braids, link polynomials and a new algebra, *Trans. Amer. Math. Soc.* 313 (1989), 249–273.
7. G. Burde and H. Zieschang, *Knots*, de Gruyter, 1985.
8. P. Dehornoy, Braid groups and left distributive operations, *Trans Amer. Math. Soc.* 345 (1994), 115–150.
9. T. Dubrovina and N. Dubrovin, On braid groups, *Sbornik Math.* 192 (2001), 693–703.
10. D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson and W. Thurston, *Word Processing in Groups*, Jones and Bartlett, 1992.
11. R. Fenn, An elementary introduction to the theory of braids, notes by B. Gemein, 1999, available at the author’s website.
12. R. Fenn, M. Green, D. Rolfsen, C. Rourke and B. Wiest, Ordering the braid groups, *Pacific J. Math.* 191 (1999), 49–74.
13. E. Fadell and L. Neuwirth, Configuration spaces, *Math. Scand.* 10 (1962), 111–118.
14. M. Falk and R. Randell, Pure braid groups and products of free groups, *Braids (Santa Cruz 1986)*, *Contemp. Math.* 78 (1988) 217–228.
15. V. F. R. Jones, A polynomial invariant for knots via Von Neumann algebras, *Bull. Amer. Math. Soc.* 12 (1985), 103–111.
16. C. Kassell and V. Turaev, *Braids*, Springer, 2008.
17. L. Kauffman, *Knots and Physics*, World Scientific, 1993.
18. D. Kim and D. Rolfsen, An ordering for groups of pure braids and hyperplane arrangements, *Canadian J. Math.* 55 (2002), 822–838.
19. D. Krammer, The braid group B_4 is linear, *Invent. Math.* 142 (2000), no. 3, 451–486.
20. D. Long and M. Paton, The Burau representation is not faithful for $n \geq 6$, *Topology* 32 (1993), 439–447.
21. W. Magnus, A. Karrass, and D. Solitar, *Combinatorial Group Theory*, Wiley, 1966.
22. A. I. Mal’cev, On the embedding of group algebras in division algebras, *Dokl. Akad. Nauk SSSR* 60 (1948), 1944–1501.
23. J. Moody, The faithfulness question for the Burau representation, *Proc. Amer. Math. Soc.* 119 (1993), 439–447.
24. H. R. Morton, Threading knot diagrams. *Math. Proc. Cambridge Philos. Soc.* 99 (1986), no. 2, 247–260.
25. R. Mura and A. Rhemtulla, *Orderable Groups*, Lecture Notes in Pure and Applied Mathematics, vol. 27, Marcel Dekker, New York, 1977.
26. A Rhemtulla and D. Rolfsen, Local indicability in ordered groups: braids and elementary amenable groups, *Proc. Amer. Math. Soc.* 130 (2002), 2569–2577 (electronic).
27. D. Rolfsen and J. Zhu, Braids, orderings and zero divisors, *J. Knot Theory and its Ramifications* 7 (1998), 837–841.
28. D. S. Passman, *The Algebraic Structure of Group Rings*, Pure and Applied Mathematics, Wiley Interscience, 1977.
29. H. Short and B. Wiest, Orderings of mapping class groups after Thurston, *L’enseignement Mathématique* 46 (2000), 279–312.