# BRAIDS

Joan S. Birman*

February 14, 2009, DRAFT

## An introduction to Topology and the Theory of Groups

This text is an incomplete draft of a planned book which could be used as either a high school enrichment course, or an introductory college textbook for mathematically talented students. It has been posted for the use of students in Columbia's Saturday AM Science Honors Program, spring semester, 2009. We plan to augment it, as time permits.

# Contents



*[1] Supported in part by NSF grant DMS-0405586. The author wishes to thank the Mathematics Department at the Technion. Its congenial atmosphere was important during the crucial days, 3 weeks in January 2009, when this project first began to develop from a vague idea to a book.

# 1 Getting started

## 1.1 Braids in the natural world

Braids are familiar objects in the natural world. We illustrate with a few examples:

1. Archeologists studying human remains from the dawn of civilization have uncovered skeletons with braided hair. The idea of combing and braiding human hair seems to us to be a message from our earliest ancestors that we share uniquely human traits.

2. Remains from an ancient fishing expedition in Antrea, on the border between Finland and Estonia, show that the discovery of a way to braid reeds, between 6,500 and 4,000 BC, was put to use to catch fish for dinner.

3. Taking a very big leap forward in time, astronomers studying the rings of the planet Saturn have seen what appear to be braiding in the 'strands' of the F-ring. What does it mean? See http://pds.jpl.nasa.gov/planets/captions/saturn/fring.htm

4. The closed orbits in the solutions to Lorenz's differential equations are a model for chaos. Their underlying pattern is based upon braids.

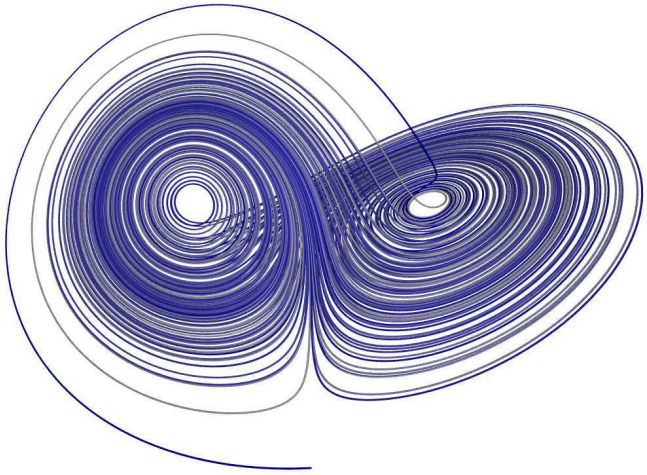

Figure 1: Numerical integration of Lorenz's equations suggests that the orbits are closed braids

5. A famous unsolved problem in that part of Computer Science which is known as *Complexity Theory* is known as the "P = NP" problem. It has been shown to be equivalent to an easily understood problem about braids [2]. We will discuss it in §2.4.

There is much more to say about these examples, however (except for the last example) our primary interest in this book will not be on applications. Rather, we are interested in the way in which braids point us toward new mathematics. To be sure, mathematics has been put to good use in all of the sciences, and in many different ways, yet mathematics is a scientific discipline in its own right, which is motivated less by the wish for ever-new applications than by the wish to discover new mathematical structure. Our goal is to give the reader a small glimpse of that, with braids (and their close relatives, knots and links on the topological side of the family and groups on the algebraic side) as the motivating and unifying theme.

Our choice of this unifying theme, and our approach to it, has its origins in work first done by the mathematician Emil Artin in [1]. His seminal work revealed the basic mathematical framework which underlies the concept of a *group of braids*. As we proceed, we will also be guided by our own tastes and preferences, which have evolved out of the experience gathered during 30 years as a research mathematician whose work has centered about braids. We will require very little in the way of background; most of what will be needed is available to every student who has successfully completed 11th grade (no need for either trigonometry or Calculus!) and mastered the rules of clear thinking. Those rules are basic, not just in mathematics but in essentially all human endeavors. The rewards will be seen to be significant, but we emphasize that the reader will need patience, and may have to read slowly, putting the text aside frequently until new ideas are absorbed. This is perhaps the biggest stumbling block that students encounter in mathematics. Our hope is that the reader who puts the needed effort into the project will come away with a glimpse at both solved and unsolved problems, some of which challenge mathematicians to this day, and with a new understanding of the structure that can be uncovered by the simple use of mathematical reasoning.

## 1.2 Braids in mathematics

### 1.2.1 Braid patterns

We begin our work by trying to capture the very intuitive and familiar notion of a braid on $n$ strands. Examples are given in Figure 2. Braids strands are always oriented top to bottom, as in $W$. The simplest

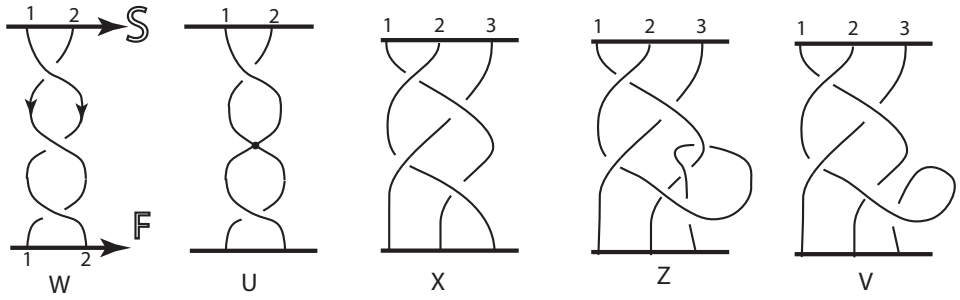


Figure 2: Some examples of braid patterns, and of inadmissible candidates

braid pattern is one on two strands, with the braid $W$ in Figure 2 as an example. One could also continue the twisting arbitrarily many times, or twist in the reverse direction, but that is all. The braid $X$ illustrates the case of 3-strands, and shows two repeats of the pattern for the braid in a person's hair. If one keeps

repeating this pattern one can make a very long braid. The first, second and third braid strands begin at the points that are labeled 1,2,3.

We need to define a braid pattern. Since it is usually helpful to think concretely, we shall take $\mathbb{S}$ to be the positive $x$-axis, and $\mathbb{F}$ to be its translation along the $z$ axis to some negative value of $z$, as in the sketches in Figure 2. Choose a positive integer $n$, and mark $n$ distinct points $1, 2, \ldots, n$, in order along $\mathbb{S}$, with corresponding points on $\mathbb{F}$. The points need not be equally spaced, and the spacing on $\mathbb{S}$ and $\mathbb{F}$ need not be the same, however on both $\mathbb{S}$ and $\mathbb{F}$ point $i$ always appears before point $i + 1$. Finally, connect the initial points to the final points by *braid strands*, a set of $n$ distinct arcs which join $\{1, 2, \ldots, n\} \subset \mathbb{S}$ to $\{1, 2, \ldots, n\} \subset \mathbb{F}$. The braid strands are required to obey the following rules:

- The first braid strand begins at point 1 on $\mathbb{S}$ and ends at one of the final points (not necessarily point 1) on $\mathbb{F}$, the second begins at 2 on $\mathbb{S}$ and ends at any unoccupied marked point on $\mathbb{F}$ and so forth. For example, in the braid $W$ in Figure 2 strand 1 starts at point 1 on $\mathbb{S}$ and ends at point 2 on $\mathbb{F}$. Strand 2 starts at point 2 on $\mathbb{S}$ and ends at the only open spot, that is point 1 on $\mathbb{F}$.
- Distinct braid strands never intersect. In Example $X$ strand 1 passes behind strand 2, then in front of strand 3, then behind strand 2. We have shown this by the use of broken lines, in the same way that overpasses and underpasses are distinguished from one-another, to give a suggestion of 3-space, on a 2-dimensional map.
- The collection of braid strands are restricted to lie in the slice of 3-space that lies between the horizontal plane that contains $\mathbb{S}$ and the horizontal plane that contains $\mathbb{F}$. Each braid strand intersects each intermediate plane exactly once, with no backtracking. The union of all $n$ strands intersects each intermediate plane in exactly $n$ points.

Note that Example $U$ is not a braid pattern (because a pair of strands intersects, giving a plane which is intersected once by the braid strands instead of twice. Examples $V$ and $Z$ are also not braid patterns because there are planes that are intersected 4 or 5 times instead of just 3 times by the 3 braid strands.

**Definition 1.1.** A *pattern for an $n$-braid*, or an *$n$-braid pattern* is the union of the initial line $\mathbb{S}$, the final line $\mathbb{F}$ and the $n$ braid strands that join them. Examples are the braid patterns $W$ and $X$ in Figure 2 and $Y_1, Y_2, Y_3$ in Figure 3.

In Figure 2 we are looking at the slice of 3-space that is between the horizontal planes that contain $\mathbb{S}$ and $\mathbb{F}$, and we see the braid strands projected onto a vertical plane that contains $\mathbb{S}$ and $\mathbb{F}$. Example $W$ (respectively $X$) is a 2 (respectively 3)-braid pattern, and examples $Y_1, Y_2, Y_3$ in Figure 3 are 5-braid patterns. In all these examples the braid strands are to be thought of as oriented *from* $\mathbb{S}$ and *to* $\mathbb{F}$. This represents a choice on our part, one that we make purely as a matter of convenience. The reason we have chosen to place $\mathbb{F}$ below $\mathbb{S}$ is to give us room (on a long rectangular page) to draw pictures of very long braids, when we need to do so. Other researchers use different conventions.

An immediate question arises: while the 5-braid patterns $Y_1, Y_2$ and $Y_3$ in the figure are clearly distinct patterns, are they really different 'braids'? Let's try to think like topologists, who seek to catch the essential features about the way that braid strands interweave with one-another, while ignoring non-essential features

such as the lengths of the braid strands, the distance between $\mathbb{S}$ and $\mathbb{F}$, and the spacing between the initial points along $\mathbb{S}$ and final points on $\mathbb{F}$, and even the order in which certain crossings occur. With that in mind, we allow ourselves to subject the pattern to an *admissible deformation* in 3-space, that is a deformation which is subject to the following rule:

- A braid pattern is allowed to be smoothly stretched or tightened through other braid patterns with the same number of strands. At every instant during the deformation distinct strands are disjoint, and intersect each intermediate horizontal plane in exactly $n$ points. In particular, two intersection points never coalesce into one, although they may come arbitrarily close. The $z$-coordinates of $\mathbb{S}$ and $\mathbb{F}$ are allowed to change, stretching or shrinking the braid strands as they do so, in any way, as long as, during the deformation, $\mathbb{S}$ and $\mathbb{F}$ remain parallel, with $\mathbb{F}$ below $\mathbb{S}$.

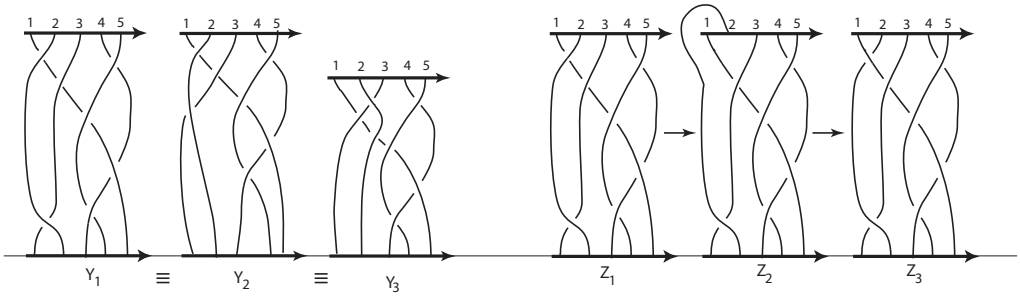


Figure 3: Examples of deformations. $Y_1 \to Y_2 \to Y_3$ is admissible; $Z_1 \to Z_2 \to Z_3$ is not.

Each of the 5-braids $Y_1, Y_2$ and $Y_3$ in Figure 3 is an admissible deformation of the other two. In $Y_2$ the first two strands of $Y_1$ have been deformed so that the projected image of the crossing between these two strands has been 'pushed up'. Note that the two start points and the two finish point (on $\mathbb{S}$ and $\mathbb{F}$) of the strands has not been changed, although we could have changed them as long as we preserved the order 1,2,3,4,5. After the deformation the projected image of the second strand of $Y_2$ crosses strand 1 before it crosses strand 3. Passing from $Y_2$ to $Y_3$ we see that in $Y_3$ the second strand has been stretched to the right, so that now its projected image crosses strand 3 before it crosses strand 1. In all three pictures it should be clear that the 5 strands intersect each intermediate plane in exactly 5 points. If the braid patterns $Y_1, Y_2, Y_3$ are related to one-another by admissible deformations, we say that they are *equivalent*. We write $Y_1 \equiv Y_2 \equiv Y_3$, meaning that $Y_1, Y_2$ and $Y_3$ differ by admissible deformations. Note that $Y_1 \equiv Y_2$ implies $Y_2 \equiv Y_1$. Also, if $Y_1 \equiv Y_2$ and $Y_2 \equiv Y_3$ then $Y_1 \equiv Y_3$. Each deformation of a pattern for an $n$-braid yields a new pattern for an $n$-braid, and there are infinitely many admissible deformations. For example, we could have stretched the entire pattern by moving $\mathbb{S}$ very far up, or moving $\mathbb{F}$ very far down, stretching the strands as we do so but without allowing them to touch one-another in 3-space. It may be helpful to think of admissible deformations in the passage $Y_1 \to Y_2 \to Y_3$ as a 'path $Y_t$ of braids' where $t$ varies over the interval [1,3]. The pattern $Y_1$ is being gradually defomed, in unit time, to $Y_2$, and then to $Y_3$ and at each intermediate $t$ it is a braid. A deformation which is forbidden is one which violates the rules for admissibility. An example of an inadmissible deformation is the passage $Z_1 \to Z_2 \to Z_3$ in Figure 3 because such a deformation creates intermediate configurations which are not braid patterns. The deformation that takes $Z_1$ to $Z_3$ is therefore inadmissible.

Let us record what we have learned, and introduce a term for it:

**Definition 1.2.** Two $n$-braid patterns are *equivalent* if there is an admissible deformation taking one to the other.

Every $n$-braid pattern $Y$ describes a unique $n$-braid $\mathbf{Y}$, but infinitely many different patterns will in general describe the same $n$-braid. This is in fact very similar to the situation encountered when one learns how to multiply and divide numbers. The fractions $\frac{4}{6}$ and $\frac{12}{18}$ describe the same rational number $\mathbf{\frac{2}{3}} \in \mathbb{Q}$, and in fact there are infinitely many other fractions which also do, yet with enough time most elementary-school children understand the need to distinguish the representatives from the underlying rational number. Eventually, they also understand that sometimes it is quite useful to have the flexibility that is afforded by being able to change the representative without changing the underlying fraction, for example by arranging so that two fractions which are to be added have a common denominator. The analogy with braids is so striking that it even seems quite natural to say that $\frac{4}{6}$ and $\frac{12}{18}$ are *equivalent* fractions, i.e. $\frac{4}{6} \equiv \frac{12}{18}$. More generally, all fractions that are equivalent to $\frac{2}{3}$ have the form $\frac{2m}{3m}$, where $m$ is a positive integer. We will call this set, that is $\{\frac{2m}{3m}$, where $m \in \mathbb{Z}\}$ an *equivalence class of fractions*. Similarly,

**Definition 1.3.** The collection of all braid patterns that are deformable to one-another are an *equivalence class of braid patterns*, or more simply a *braid*. For example, the 5-braid pattern $Y_1$ and all 5-braid patterns $Y' \equiv Y_1$ determine a 5-braid $\mathbf{Y}$.

The concept of an "equivalence class" is an important idea in mathematics, and it can be a stumbling block, so one more example may be useful. Let $\mathbb{N} = \{0, +1, -1, +2, -2, \dots\}$ be the set of all integers. Define $n \equiv m$ if 2 divides $n - m$. There are two distinct equivalence classes in $\mathbb{N}$ : the integers that are equivalent to 0 (the even integers) and the integers that are equivalent to 1 (the odd integers), and an arbitrary integer is either even or odd, never both. Thus the condition $n \equiv m$ divides the set of integers into two equivalence classes: the even integers and the odd integers.

In the example of the set of rational numbers $\mathbb{Q}$ there are infinitely many rational numbers, each represented by infinitely many fractions. In the example of braid patterns there are infinitely many distinct braids, each represented by infinitely many distinct braid patterns. In our newest example there are infinitely many even integers and also infinitely many odd integers, but only two equivalence classes, the even and the odd integers.

Returning to fractions and rational numbers, we observe that there is a nice way to decide whether two fractions $\frac{a}{b}$ and $\frac{c}{d}$ describe the same underlying rational number.

- To decide whether fractions $\frac{a}{b}$ and $\frac{c}{d}$ represent the same rational number, we ask whether

$$(\frac{a}{b})(\frac{d}{c}) = \frac{ad}{bc} \equiv 1 \tag{1}$$

For example, if we want to decide whether $\frac{4}{6}$ and $\frac{12}{18}$ represent the same rational number, lets look at the product of $\frac{4}{6}$ and the *inverse* of $\frac{12}{18}$, i.e. $\frac{18}{12}$, that is $\frac{4 \cdot 18}{6 \cdot 12} = \frac{72}{72}$. Clearly this product is 1. On the other hand, the fractions $\frac{4}{6}$ and $\frac{3}{5}$ do not represent the same rational number because $\frac{20}{18} \neq 1$.

This brings us to a fundamental question about braids:

**The first fundamental problem:** Given two $n$-braid patterns $X$ and $X'$, find an algorithm to decide whether $X'$ is deformable through braid patterns to $X$.

Fortunately, we will be able to solve the problem in a very satisfactory way, moreover the solution will turn out to be far from obvious. There is a hint of how to do it in the solution we gave in (1) to the related problem for rational numbers. Let's keep it in mind as we develop the necessary machinery.

### 1.2.2 Multiplying fractions and multiplying braid patterns

The solution that we gave to the fundamental problem for rational numbers was described in (1). Seeking an analogy, we are lead to ask whether there is a way to 'multiply' braids?

Let $X$ and $Y$ be $n$-braid patterns. It is important that we use the same integer $n$ for both. We wish to define

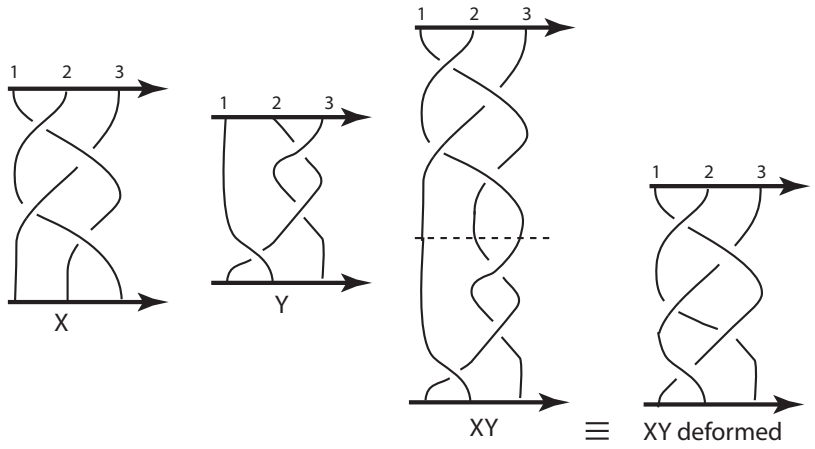


Figure 4: Multiplying braid patterns

a new $n$-braid pattern, which we call $XY$, referring to it as the *product* of $X$ and $Y$, just as the product of the two rational numbers $\frac{4}{6}$ and $\frac{5}{3}$ is $\frac{20}{18}$. To define $XY$ we first use allowable deformations to deform the braid pattern that represents $X$ and the pattern that represents $Y$ until the final line of $X$ coincides in 3-space with the initial line of $Y$, also the marked points on the former and latter coincide. We then erase the final line of $X$ and the initial line of $Y$, as in the example in Figure 4. The result will be a braid pattern which we call $XY$. Its initial line is the initial line of $X$ and its final line is the final line of $Y$. It is an $n$-braid pattern because $X$ and $Y$ were $n$-braid patterns and we took care that the deformations we applied were admissible.

In the example in Figure 4, it turns out that when the product $XY$ is formed there is some 'cancellation' at the interface between the the end of $X$ and the beginning of $Y$. The apparent simplification occurs because, in this particular instance, the final crossing in $X$ has a rather special relationship to the initial crossing in $Y$, a matter that will be discussed in §1.2.4.

### 1.2.3 The integer 1 and the identity braid pattern I

Encouraged by the fact that there is a way to multiply braids, we note that the positive rational number 1 plays a very special role in multiplication, in fact it is a trivial role. For every $x \in \mathbb{Q}$ we know that $1 \cdot x = x \cdot 1 = x$. Is there a braid I that behaves, in some way, like the number 1? Indeed there is, and it is shown in Figure 5. The products $X$, I$X$ and $X$I are different braid patterns, but it is immediately and intuitively clear that they represent the same braid $\mathbf{X}$ because there are allowable deformations that shrink the part of the pattern that came from I, whether it is placed before or after the old part $X$.

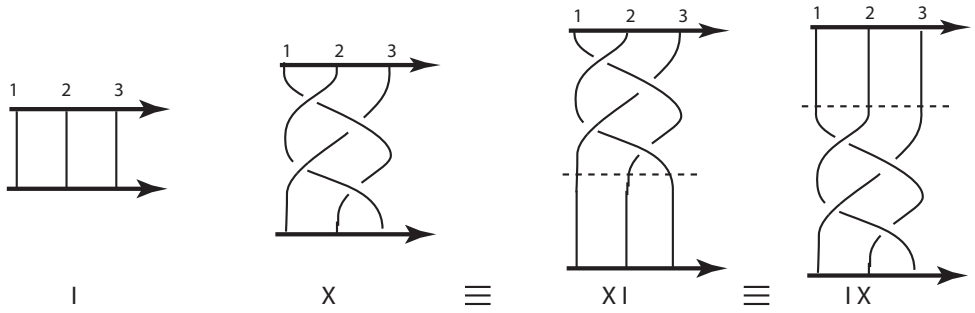


Figure 5: The identity braid pattern

### 1.2.4 Inverses of fractions and inverses of braid patterns

Motivated once again by the example of rational numbers, we note that for every fraction $\frac{a}{b}$ there is another fraction, namely $\frac{b}{a}$ with the property that $(\frac{a}{b})(\frac{b}{a}) = (\frac{b}{a})(\frac{a}{b}) = 1$. We call $\frac{b}{a}$ the *inverse* of $\frac{a}{b}$ because it 'undoes' it. Is there an analogue for braids? In fact there is, and it's illustrated in Figure 6. The left two

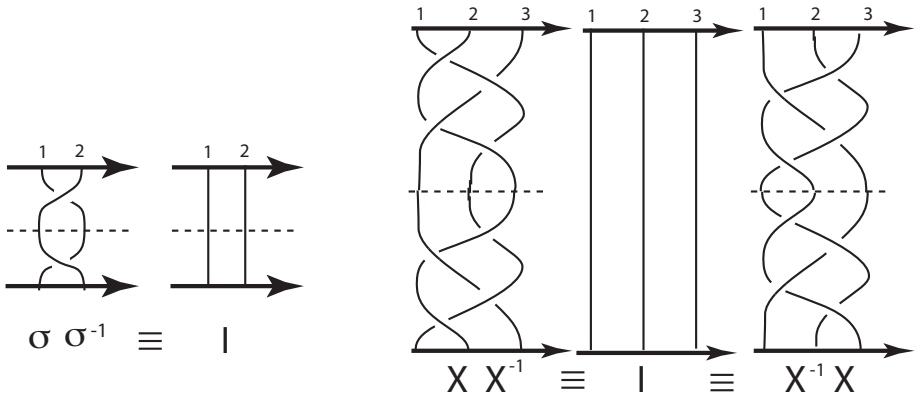


Figure 6: The inverse of a braid pattern

sketches in Figure 6 show the inverse of an *elementary* 2-braid $\sigma$. [1] It's immediately clear that the product of $\sigma$ and its reflection about the finish line is deformable to the identity braid. Choosing any braid pattern $X$, we find $X^{-1}$ by reflecting $X$ about a line parallel to $\mathbb{S}$ and $\mathbb{F}$. The sketches on the right show $XX^{-1}$ and also $X^{-1}X$. It is intuitively clear that $XX^{-1}$ and $X^{-1}X$ are both are deformable to I. More precisely, if we start at the interface between $X$ and $X^{-1}$ then we see crossings that appear to cancel. Tightening the braid strands so as to eliminate the cancelling crossings, new cancelling crossings appear. Continuing, we may repeatedly tighten at the interface, until the entire product is $XX^{-1}$ is reduced to the identity braid. This is why we think of the reflection of $X$ as $X^{-1}$.

**Remark 1.4.** The reader may be wondering whether we have found a solution to the first fundamental problem, the problem of deciding whether two braid patterns $X$ and $Y$ represent the same underlying braid? Recall that when we asked the same question about fractions $x = \frac{4}{6}$ and $y = \frac{12}{18}$ we solved the problem by computing $xy^{-1} = \frac{(4)(18)}{(6)(12} = \frac{72}{72}$ and asking whether it represents the rational number 1? The very same idea works with braid patterns. To decide whether the 3 braid patterns $Y_1, Y_2, Y_3$ in Figure 2 represent the same underlying braid, compute, for example, $Y_1Y_2^{-1}$ and $Y_1Y_3^{-1}$ and ask whether these two braids can be "combed' to the identity braid? The answer is *yes*, and the procedure is indeed a way to solve the first fundamental problem. The only difficulty with it is that we cannot be sure, at this time, that we know how to identify all the patterns that represent the identity braid.

A first thought is that if an $n$-braid pattern represents the identity, then a good hard pull on the finish line should stretch the strands until there its lots of cancellation and $n$ straight lines appear. But is that really so? Our experiences with tangled hair and combs suggest that perhaps yjere are subtleties. Maybe there are patterns for which, for example, we need to increase the number of crossings, inserting some number of little cancelling pairs of elementary braids in strategic places, before the pattern can be simplified. Or maybe it's a simple matter of cancelling crossings very carefully, in the right order. In fact, the problem is fairly subtle. We will solve it, but are not ready to do so yet.

### 1.2.5 The associative law for fractions and for braid patterns

A final observation is in order about our product rule, that again is suggested by the example of the positive rational numbers $\mathbb{Q}$: The associative law, $(XY)Z = X(YZ)$ holds for braid patterns just as it does when we multiply rational numbers. In the first instance we form the product $XY$, and compose it with $Z$, to obtain $(XY)Z$. In the second instance we begin with the product $YZ$, and then pre-multiply it by $X$, to obtain $X(YZ)$. The reader is encouraged to draw a few pictures to convince himself that the order in which the intermediate lines have been erased makes no difference, and that we can safely drop all the parentheses and refer to the product as $XYZ$. It is worthwhile to mention that our project would be very difficult if the associative law did *not* hold. We would be forced to keep track of multiple parentheses, and the resulting bookeeping would be prohibitive.

**Exercise 1.5.** *Show by example that the product $XY$ and the product $YX$ do not, in general, represent the same braid. This is quite different from multiplication of numbers, where the products $xy$ and $yx$ are*

[1] Mathematicians need to use lots of letters, and the Greek alphabet is particularly handy as an extra set. The lower case Greek letter $\sigma$ has traditionally been used to denote elementary braids, and we follow that tradition. It's called 'sigma', and we will have more to say about it very soon.

*always the same, a matter which is stressed repeatedly even though the children who are learning it have no reason to think it could ever be otherwise.*

**Exercise 1.6.** *Show by example that for certain special braids $X$ and $Y$ the products $XY$ and $YX$ actually do define the same braid.*

**Exercise 1.7.** *Suppose that there is an admissible braid deformation $X_t$ that takes the $n$-braid pattern $XY$ to a new $n$-braid pattern $X_1$ and an admissible deformation $Z_t$ that takes $YZ$ to $Z_1$. The associative law says that $X_1Z$ and $XZ_1$ define the same $n$-braid. Give an explicit way to deform $X_1Z$ to $XZ_1$.*

### 1.2.6 The group $\mathbf{B_n}$ of $n$-braids

We are finally ready to take a big step: to pass from the patterns that describe representatives of braids to the more abstract notion of a braid. Once that that little step has been taken, it will be natural to take the next step, which is to define the concept of a group of braids:

**Definition 1.8.** A *braid* on $n$ strands is an equivalence class of braid patterns, under the equivalence that is defined by admissible deformations.

We have taken care to define products and inverses on braid patterns in such a way that the key laws hold for not just for patterns but also for braids, that is for equivalence classes of patterns. This means that:

1. Let $\mathbf{X}, \mathbf{Y}$ be braids. Choose any patterns $X, Y$ that represent them. The *product* $\mathbf{XY}$ is the braid that is represented by the product of the patterns $X$ and $Y$.
2. Multiplication of braids is associative. In particular, choose any 3 braid patterns $X_1, X_2, X_3$. Then $(X_1X_2)X_3$ and $X_1(X_2X_3)$ represent the same braid $\mathbf{X_1X_2X_3}$.
3. The identity braid $\mathbf{I}$ is well-defined, independently of the choice of its representative . In particular, for any choice of braid patterns $X, I$ representing $\mathbf{X}, \mathbf{I}$ the rule $\mathbf{XI} = \mathbf{IX} = \mathbf{X}$.
4. Inverses of braids are well-defined. In particular, if $X_1, X_2$ that both represent the braid $\mathbf{X}$. Then $X_1^{-1}, X_2^{-1}$ both represent the same braid $\mathbf{X^{-1}}$.

**Definition 1.9.** The collection of $n$-strand braids $\mathbf{B_n}$, with the rule that we have given for forming products, is known as the *group of braids*.

**Remark 1.10.** We may from now on safely work with braid patterns, knowing that anything new that we learn holds more generally for braids, not just for their representating patterns. This is much the same as we do for fractions and the underlying rational numbers that they represent.

Observe that the product rule for multiplying two fractions, and the product rule for multiplying two braids, are very different. In fact they are so different that we seem to need a definition:

**Definition 1.11.** Let $G$ be a set. A *product* on $G$ is a rule which determines, for every ordered pair of elements $x, y \in G$, a unique element $x \cdot y \in G$, which is called the *product* of $g_1$ and $g_2$. The product

is required to be associative, that is $(xy)z = x(yz)$ for every triplet $x, y, z \in G$. Also, there is a unique identity element $1 \in G$ which satisfies $1x = x = x1$ for every $x \in G$. Also, for every $x \in G$ there is a unique element $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = 1$. If all of these are satisfied, then $G$ with this particular product rule is said to be a *group*.

We already know two examples of groups:

1. The group $\mathbb{B}_n$ of braids on $n$ strands.

2. The collection of rational numbers $\mathbb{Q}$ were our first example of a group. The product rule is multiplication of representatives, that is of fractions. The identity element is the rational number 1, represented by the set $\{\frac{n}{n}\}$, where $n$ is any positive integer. The inverse of a rational number is defined by taking any representative $\frac{a}{b}$ and replacing it by $(\frac{a}{b})^{-1} = \frac{b}{a}$. The associative law holds for both fractions and the rational numbers that they represent.

In fact, we also know a third example:

3 The natural numbers $\mathbb{N} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, with *addition of numbers* as the 'product' rule is another example of a group. For every two integers $N, M \in \mathbb{N}$ we know how to determine $N + M$. We also know that if $N, P, M$ are numbers, then $(N + M) + P = N + (M + P)$. The 'identity element' in $\mathbb{N}$ is 0. And we know that for every integer $N$ we can find its *inverse*, that is $-N$, also that $N + (-N) = 0$. Observe that, while $N + (-N) = (-N) + N$, this is not part of the definition of a group, and indeed it is not true for braids.

## 1.3 Looking ahead

Once mathematicians have convinced themselves, via examples, that there is a unifying idea that appears in multiple examples, it is the moment to take a big leap forward, and to ask what can be learned that depends on the unifying theme, and not on the explicit examples. If that can be done, then there are sure to be many applications, because everything that has already been learned can be applied to new examples, without developing all the machinery over again from the start. That is the basic idea that we hope to convey in this little book. But before we take that leap, and consider groups in a more general setting, it would be wise to work out some of the consequences of the existence of a 'group structure' on braids. That will be our goal in Chapter **??**. In particular, we will use the fact that braids form a group to find a solution to the fundamental problem of deciding when two braid patterns define the same underlying braid. We now know that problem is equivalent to the problem of recognizing when a braid pattern is equivalent to the identity, the problem of *combing the identity braid pattern*. See §2.

As a second application, we will explain how a very fundamental and unsolved problem in computer science can be expressed as a question about braids. See §2.4.

The subtitle of this book is "An introduction to topology and the theory of groups". Peeking ahead, we will take a little break to show how braids are related to another common object, knots and links. That is the

subject of Chapter3. Knots and links are squarely in the middle of the part of mathematics which is known as topology.

Finally, in Chapter 4 we will learn a little bit more about that part of mathematics that has come to be known as the *Theory of Groups*. We stress that, while the concept of a group is unknown to most educated people, it is just a hairsbreadth away from the manipulations which every grade-school child is forced to learn, sometimes painfully, when he/she learns to add, subtract ,multiply and divide the integers and the rational numbers. Indeed, with the advent of digital computers, most educated people learn (without realizing it) that there is a group of integers mod 2, where the basic elements are just 0 and 1. We will discuss that too in Chapter 4.

A word is in order about proofs. Proofs lie at the heart of mathematics, yet so far we have not had the need to prove anything. Rather, we have taken some trouble to give carefully motivated definitions. Indeed, in an exposition of the same subject to an audience of trained mathematicians, this entire chapter would have been replaced with a single definition: *The braid group $B_n$ is the fundamental group of the space of configurations of $n$ points on a plane*, followed by some number of examples to give meaning to the definition. In this book we will give some proofs. In other places we will suggest how a particular fact can be proved without actually going through all the gory details. In still others we will simply ask the reader to accept a particular fact without proof, either because the proof is too long to be reproduced, or because the anticipated audience will very likely lack the needed tools. We will make every effort not to slide over matters which need proof, an issue which is always present when one tries to leap ahead too quickly.

# 2 Combing the identity braid pattern

Our goals in this chapter are:

1. We will find a way to describe braids symbolically, by 'words' in a set of 'generators', thereby reducing the need for pictures. As will be seen, the words, like words in the Roman alphabet, have a natural notion of letter length. The length is a measure of the 'complexity' of the word, and so of the braid.

2. We will introduce a related tool, 'relations between the generators'. These relations will enable us to gain some control over admissible braid deformations.

3. Armed with the preceding machinery, we will be able to solve the fundamental problem: to decide algorithmically when two braid patterns (described now by words) represent the same braid.

4. The algorithm that we will be able to give is not very efficient. It cries to be improved, and indeed it has been improved. We will not have time to discuss the improvements, however the understanding that is gained by working with specific examples will lead us, naturally, to a discussion of complexity issues. The question of finding a *shortest* word in the generators turns out to be one of a class of problems which is known, in Theoretical Computer Science, as the class of 'NP-complete' problems. We will explain what this means, and in so doing will be able to describe one of the deep open questions which lies at the forefront of current research in complexity theory.

## 2.1 Symbols that describe braid patterns

Pictures motivated the entire concept of a braid, and they are very pleasant to view, but they can be time-consuming. For that reason it is nice to have a way to define patterns for braids symbolically, so that we can reduce our reliance on pictures. The admissible deformations of §1.2.1 are just the tool that we need to do it. To explain what we have in mind, recall that $\mathbb{S}$ and $\mathbb{F}$ are parallel to the $x$ axis in 3-space, with $\mathbb{S}$ above $\mathbb{F}$. The $xz$ plane, call it $P$, then contains $\mathbb{S}$ and $\mathbb{F}$. Project the braid pattern onto $P$. After perhaps an allowable deformation, as shown in the passage from $Y_1$ to $Y_1'$ in Figure 7 we may assume that distinct double points have distinct $z$ coordinates. The projection of the braid pattern then has a finite number, say $m$, of double points, whose $z$-coordinates then have a natural order, according to their distance from $\mathbb{S}$. After each crossing and before the next crossing we choose an intermediate horizontal line that is parallel to $\mathbb{S}$ and $\mathbb{F}$ whose projection intersects the $n$ strands in $n$ distinct points. In this way we have constructed a grid on $P$ which is divided into $m$ strips, and in each strip there will be precisely two elementary braid strands which are adjacent and cross, and $n-2$ additional ones which are essentially vertical arcs. See Figure 7. Finally, observe that there are two kinds of elementary braids, those in which strand $k$ crosses over strand $k+1$, and those in which strand $k+1$ crosses over strand $k$, and they are mutually inverse. Following earlier notation, we call the former $\sigma_k$ and the latter $\sigma_k^{-1}$, noting that if the braid index is $n$ then $1 \leq k \leq n-1$. We can think of $\sigma_1, \ldots, \sigma_{k-1}, \sigma_1^{-1}, \ldots, \sigma_{k-1}^{-1}$ as a set of *letters* in an *alphabet*. Letters can of course, be concatenated to define *words*. For example, the 5-braid $Y_1$ in Figure 7 (it's the same as the braid pattern $Y_1$ in Figure 2) can be described by the word $\sigma_1\sigma_4\sigma_2\sigma_3\sigma_4^{-1}\sigma_3\sigma_1^{-1}$. A different example is

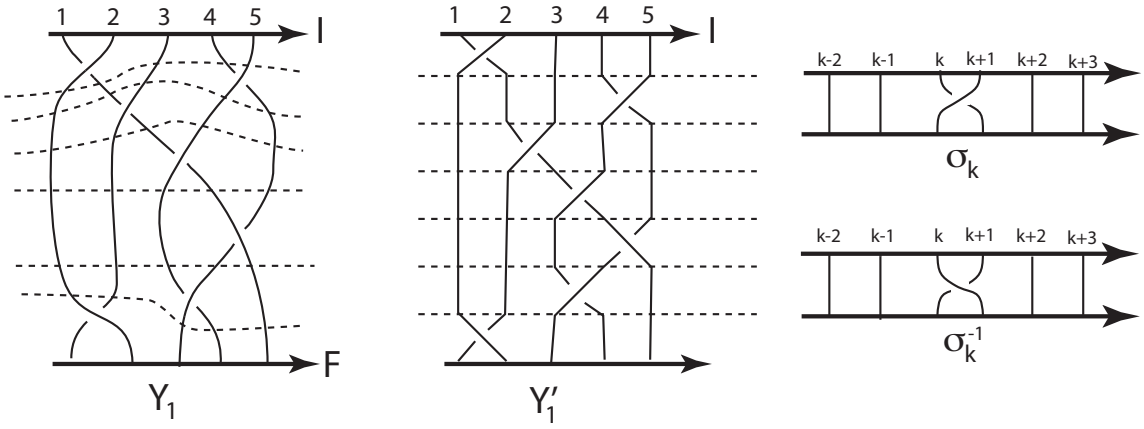


Figure 7: Elementary braids

the 3-braid pattern $X$ in Figure 7, the braid in a person's hair, corresponds to the word $\sigma_1\sigma_2^{-1}\sigma_1\sigma_2^{-1}$. The kind of deformation that was illustrated in Figure 7 can be applied to any braid pattern. This shows that every braid pattern may be described by a word in the alphabet $\sigma_1, \ldots, \sigma_{n-1}, \sigma_1^{-1}, \ldots, \sigma_{n-1}^{-1}$. The word is not unique, because most of the time there are lots of choices that are involved.

**Definition 2.1.** The elementary braids $\sigma_1, \ldots, \sigma_{n-1}$ are said to *generate* the group $\mathbf{B_n}$ of $n$-braids. This means that every $n$-braid can be described by a word in the elementary braids and their inverses. If $W = s_1 s_2 \cdots s_{k-1} s_k$, where each $s_i$ is a generator $\sigma_i$ or its inverse $\sigma_i^{-1}$, then the *inverse* of $W$ is the word $W^{-1} = s_k^{-1} s_{k-1}^{-1} \cdots s_2^{-1} s_1^{-1}$. The identity element $\mathbb{I}$ of $\mathbf{B_n}$ is represented by the empty word.

**Exercise 2.2.** *Draw some pictures to convince yourself that the 3-braid pattern in Figure 2, which is described by the word $\sigma_1\sigma_2^{-1}\sigma_1\sigma_2^{-1}$, can be deformed to 2 different patterns that are described by the words $\sigma_1^2\sigma_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2^{-1}$ and $\sigma_1\sigma_2^{-1}\sigma_2^{-1}\sigma_2\sigma_1\sigma_2^{-1}$.*

*More generally, show that if $W$ is a word that describes a braid pattern, then an equivalent pattern is obtained by inserting anywhere in the word $W$ the syllable $\sigma_i\sigma_i^{-1}$ or $\sigma_i^{-1}\sigma_i$, for any $i$ between 1 and $n-1$. Explain why the word $W$ and the new word $W'$ define equivalent braid patterns.*

**Exercise 2.3.** *Draw pictures for the 3-braids that are described by the braid words $W = \sigma_1^3\sigma_2^{-2}\sigma_1^5\sigma_2^{-1}$ and $V = \sigma_1^3\sigma_2^{-1}\sigma_1^5\sigma_2^{-2}$*

**Exercise 2.4.** *Let $W = \sigma_{i_1}^{\epsilon_1} \ldots \sigma_{i_r}^{\epsilon_r}$, where each $\imath_q$ is between 1 and $n-1$ and where each $\epsilon_q = \pm 1$ be a word that represents a braid $\mathbf{W}$. Find a word that represents $\mathbf{W}^{-1}$.*

## 2.2 Symbols that describe braid deformations

### 2.2.1 Trivial relations

We already know that braid patterns can be changed by applying admissible deformations. A different aspect of the same phenomenon is that, if a word $W$ describes a braid pattern, then we can always insert or

delete a syllable $\sigma_i^{\pm 1}\sigma_i^{\mp 1}$ somewhere in $W$ to obtain another word that represents an admissible deformation of the pattern, because

$$\sigma_k\sigma_k^{-1} \equiv \sigma_k^{-1}\sigma_k \equiv \mathbb{I} \tag{2}$$

The two 'equations' in (2) are called *trivial relations*. Using them over and over again gives infinitely many different words, all describing equivalent patterns. This suggests the pleasant possibility that a finite set of equivalences between braid words could point the way to capturing the key features of the non-uniqueness of braid patterns. This is encouragement to ask what else might happen?

### 2.2.2 Commutativity relations

There is another fairly basic way that distinct words can be seen to define distinct braid patterns but the same braid. In the sketch of $Y_1$ in Figure 7 we chose the dotted lines so that the first letter is $\sigma_1$ and the second is $\sigma_4$, but we could equally well have chosen a different dotted line, and found that $\sigma_4$ came before $\sigma_1$. Indeed, it is easy to see that whenever two adjacent syllables are $\sigma_j^{\pm 1}\sigma_k^{\pm 1}$, where $j$ and $k$ differ by at least 2, either order is possible. Therefore we have the four 'commutativity relations'. There are four of them because $\sigma_j\sigma_k$ has 2 letters, and each could either be positive or negative, giving $2^2 = 4$ possibilities.

$$\sigma_j\sigma_k \equiv \sigma_k\sigma_j \quad \text{if } |j-k|>1, \text{ for all } 1\le j,k\le n-1 \tag{3}$$

$$\sigma_k^{-1}\sigma_j^{-1} \equiv \sigma_j^{-1}\sigma_k^{-1} \quad \text{if } |j-k|>1, \text{ for all } 1\le j,k\le n-1 \tag{4}$$

$$\sigma_j\sigma_k^{-1} \equiv \sigma_k^{-1}\sigma_j \quad \text{if } |j-k|>1, \text{ for all } 1\le j,k\le n-1 \tag{5}$$

$$\sigma_j^{-1}\sigma_k \equiv \sigma_k\sigma_j^{-1} \quad \text{if } |j-k|>1, \text{ for all } 1\le j,k\le n-1 \tag{6}$$

These four *commutativity relations* between words in the generators capture the analogue, in the setting of words, of admissible deformations of braid patterns.

Let's look at them more carefully. A first observation is that (4) can be obtained from (3) simply by taking inverses of both sides. So (4) seems a little bit repetitious, once we know (3).

Second, observe that once we know that (3) is true, it will certainly continue to be true if we multiply both sides of (3) by $\sigma_k^{-1}$ on both the right and the left. That is, the relation:

$$(\sigma_k^{-1})(\sigma_j\sigma_k)(\sigma_k^{-1}) \equiv (\sigma_k^{-1})(\sigma_k\sigma_j)(\sigma_k^{-1}). \tag{7}$$

is clearly a consequence of (3), because if we replace $\sigma_j\sigma_k$ and $\sigma_k\sigma_j$ in (7) by 1, then it reduces to the identity $\sigma_k^{-2} \equiv \sigma_k^{-2}$. But then let's use the associative law to regroup the terms as:

$$(\sigma_k^{-1}\sigma_j)(\sigma_k\sigma_k^{-1}) \equiv (\sigma_k^{-1}\sigma_k)(\sigma_j\sigma_k^{-1}).$$

Applying the trivial relation (2) to simplify, we have learned that (5) is a consequence of (3) and (2).

We leave it to the reader to show that, in a similar way, (6) is a consequence of (3) and (2). For this reason we say that (3) is the *basic commutativity relation*, and that (4), (5) and (6) are *consequences* of (3).

Sketch (a) in Figure 8 illustrates the basic commutativity relation. It goes without saying that any one of the four could have been chosen as being the basic one, however (for reasons that will be come clear very soon) we will always have a preference for positive words and positive relations between them.

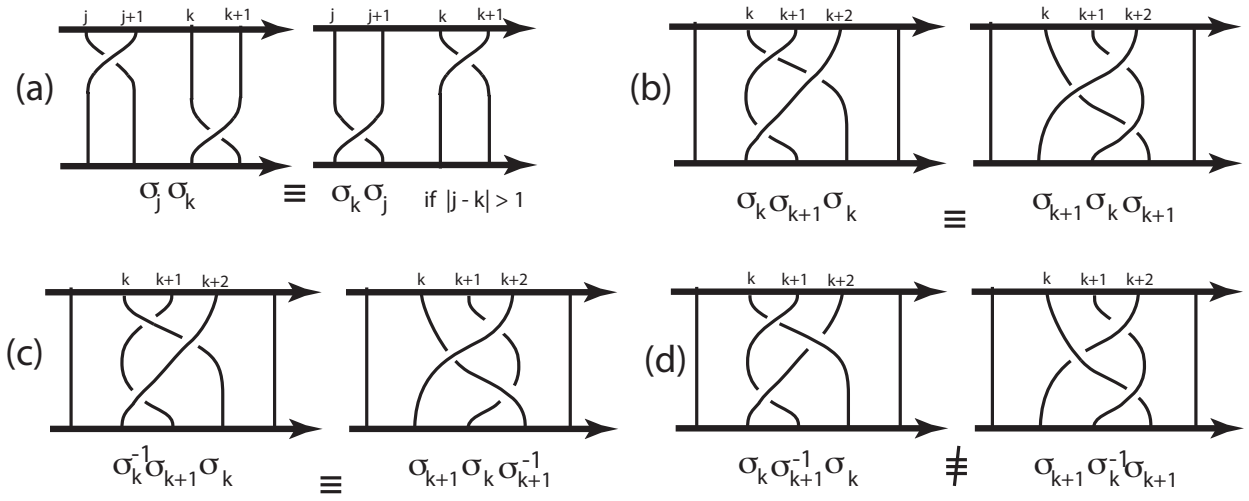


Figure 8: Sketch (a) illustrates the basic commutativity relation. Sketches (b),(c) and (d) illustrate the basic handle move and two others, the one in (c) being valid and that in (d) invalid.

### 2.2.3 Handle relations

Sketch (b) in Figure 8 shows that when $j$ and $k$ differ by 1 there is a different deformation that is possible, namely $\sigma_k\sigma_{k+1}\sigma_k$ can be replaced by $\sigma_{k+1}\sigma_k\sigma_{k+1}$. However, unlike the case of the commutativity relations, when we list all of the possibilities for words $\sigma_k\sigma_{k+1}\sigma_k$ of length 3 when signs are taken into account, we will see that they do not all yield relations. An example can be seen in sketch (c) of Figure 8. In fact, 6 of the 8 possible sign sequences yield a relation which holds in $\mathbf{B_n}$, whereas 2 do not. The reader is invited to check this. The 6 that work are:

$$\sigma_k\sigma_{k+1}\sigma_k \equiv \sigma_{k+1}\sigma_k\sigma_{k+1} \quad \text{for all } k = 1, \ldots, n-2 \tag{8}$$

$$\sigma_k^{-1}\sigma_{k+1}^{-1}\sigma_k^{-1} \equiv \sigma_{k+1}^{-1}\sigma_k^{-1}\sigma_{k+1}^{-1} \quad \text{for all } k = 1, \ldots, n-2 \tag{9}$$

$$\sigma_k^{-1}\sigma_{k+1}\sigma_k \equiv \sigma_{k+1}\sigma_k\sigma_{k+1}^{-1} \quad \text{for all } k = 1, \ldots, n-2 \tag{10}$$

$$\sigma_k\sigma_{k+1}\sigma_k^{-1} \equiv \sigma_{k+1}^{-1}\sigma_k\sigma_{k+1} \quad \text{for all } k = 1, \ldots, n-2 \tag{11}$$

$$\sigma_k^{-1}\sigma_{k+1}^{-1}\sigma_k \equiv \sigma_{k+1}\sigma_k^{-1}\sigma_{k+1}^{-1} \quad \text{for all } k = 1, \ldots, n-2 \tag{12}$$

$$\sigma_k\sigma_{k+1}^{-1}\sigma_k^{-1} \equiv \sigma_{k+1}^{-1}\sigma_k^{-1}\sigma_{k+1} \quad \text{for all } k = 1, \ldots, n-2 \tag{13}$$

**Remark 2.5.** We give a little trick that helps us to remember the valid handle moves, when all the signs are not the same, i.e. (10)-(13). Notice that a handle relation is valid if and only if the exponent of the middle letter is the same as the exponent on both its left and its right. Assume that a handle move is valid, and the exponents are not all the same. Then exactly one of the letters in the 3-letter word on the left has a different sign than the other two. For example, in (10) the letter $\sigma_k^{-1}$ is moved. The handle move then consists of allowing this letter to 'jump across the other two letters, changing its name as it does so'.

**Exercise 2.6.** *Prove (as we did in the case of the commutativity relations) that each of the braid relations* (9),(10),(11),(12) *and* (13) *is a consequence of the basic braid relation* (8).

### 2.2.4 Defining relations

While we have written out the braid relations as if they were equations, for example $R_1 \equiv R_2$, the rule for multiplying braids and taking inverses allow us to replace any such equation by $R_1 R_2^{-1} \equiv 1$. From this point of view, the collection of all braid relations may be thought of as the collection of all words that represent the identity element $\mathbb{I} \in \mathbf{B_n}$.

Now observe that if $R$ is a word in the $n$-braid generators, and if $R \equiv 1$, then for any $n$-braid word $U$ we must also have that $URU^{-1} \equiv 1$ too. TO BE CONTINUED

## 2.3 An application: Garside's solution to the first fundamental problem

Use generators and relations for the braid group to solve the problem of deciding when two patterns define the same braid. Stress the analogy with fractions. To decide whether $\frac{a}{b}$ and $\frac{c}{d}$ define the same rational number, we compute $\frac{ad}{bc}$ and decide whether it is equal to 1. The proof for braids is similar.

## 2.4 Another application: shortest words and the P = NP problem

Discuss complexity of an algorithm. Discuss what it means for an algorithm to be in class P and in class NP. Discuss the P = NP problem. Then describe the shortest word problem and show that if it has a polynomial-time solution, then P = NP.

# 3 Knots and links

Every braid defines a unique knot or link. Every knot or link can be represented by a braid.

The fundamental problem of distinguishing knots and links.

The Jones polynomial.

# 4 The theory of groups

Basic Definitions

Examples: Permutation groups, The dihedral groups

Subgroups. The pure braid group as an example

Every finite group is a subgroup of the group of permutations on $n$ strands for some $n$

Homomorphisms: Braids to permutations as an example.

# References

[1] E. Artin (1925)
[2] Patterson and Razborov