Proceedings of the East Asian School
of Knots, Links, and Related Topics
February 16–20, 2004 • Seoul, Korea

DIAGRAMS COLOURINGS AND APPLICATIONS

PATRICK DEHORNOY

Abstract. This paper reviews some results involving arc colourings in a braid or a link diagram. The left self-distributivity idendity then appears as an algebraic counterpart to Reidemeister move of type III. Using classical and less classical self-distributive operations leads to a number of different results, as well as to many open questions.

It has been observed for many years that there exist a connection between braids and links on the one hand, and left self-distributive systems (LD-systems for short) on the other hand, the latter consisting of a set equipped with a binary operation $*$ that satisfies the left self-distributivity identity

$$(LD) \qquad x * (y * z) = (x * y) * (x * z).$$

In this text, we review some of the results about links and, mainly, braids, that can be obtained using this approach. Some results are connected with classical LD-systems, such as the racks of [30] or the quandles of [37]: here, we use "classical" for those LD-systems whose operation is close to conjugacy in a group, the most common example. But the main emphasis will be put on non-classical LD-systems. The latter are examples of a completely different flavour which have been considered from the beginning of the 1990's in connection with work in Set Theory—but do not depend on this approach, which is involved as a motivation only. We shall in particular show how considering non-classical LD-systems leads to ordering properties, and how self-distributive operations can be defined on braids themselves. The unifying principle behind all the developments described here is the Hurwitz action of braids on the power of an LD-system, as identified for instance by Brieskorn in [6].

1. Colouring the strands of a diagram

1.1. **The basic principle.** Let us consider a standard braid or link diagram such as those of Figure 1.

Figure 1. A braid diagram (left) and a link diagram (right)

Received by the editors on March 2, 2004.
2000 *Mathematics Subject Classification.* 20F05, 20F36, 20B07.

Colouring the strands of such a diagram, say D, means choosing an auxiliary set S (the colours) and attaching with each arc in D an element of S, *i.e.*, use the elements of S to label the arcs of the diagram. The basic idea is to use such colourings to extract information about D, or, rather, about the braid or the link represented by D.

It is natural to assume that the colours remain unchanged while propagated along the arcs, and the question is of what happens at crossings. If we decide that both strands keep their color, then only n different colours may occur in an n strand braid diagram or an n component link diagram and, as can be expected, not much about the braid or the link represented by the diagram can be extracted.

Things become more interesting when we allow colours to change at crossings. Several rules can be considered, but here we shall concentrate on the most natural one, namely when the front strand (the one that is not interrupted) keeps its colour, while the back strand may change its colour so that the new colour only depends on the colours of the two strands involved in the crossing. We shall always consider oriented diagrams, so that there are two cases, according to whether the front strand comes from the left or from the right. This amounts to saying that there exists a binary operation on the set of colours so that the new colour is the product of the two initial colours. As crossings may have two distinct orientations, we are led to assume that the set of colours S is equipped with two binary operations $*, \overline{*}$, and the rules of Figure 2 are obeyed at each crossing.

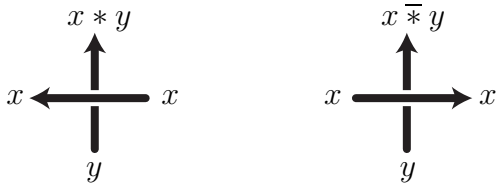


FIGURE 2. Rules for changing colours: y becomes $x * y$ when it is overcrossed by x coming from its right, and $x \,\overline{*}\, y$ when it is overcrossed by x coming from its left

1.2. **Invariance under isotopy.** We are interested in using colourings to extract information about the braid or the link represented by a diagram, so we wish that the colourings are, in some sense, invariant under isotopy. As is well-known—see for instance [3, 8, 40] or [50]—two link diagrams represent the same link if and only if they can be connected by a finite sequence of Reidemeister moves, and two braid diagrams represent the same braid if and only if they can be connected by a finite sequence of braid equivalences, which are special cases of Reidemeister moves of type II and III. Thus we are led to study whether the colourings defined as in Figure 2 are invariant under the previous transformations. We shall successively consider three cases, namely the case of positive braid diagrams (those in which all crossings have the same orientation), then the case of arbitrary braid diagrams, and, finally, the case of link diagrams.

We implicitly assume that some index n is fixed and consider n strand braid diagrams. We allow $n = \infty$, but, as usual, only consider diagrams with finitely many crossings. As is standard, we use σ_i for the elementary diagram consisting of

a single crossing between the strands at position i and $i+1$ (Figure 3). The braid diagrams are supposed to be oriented from the top to the bottom.

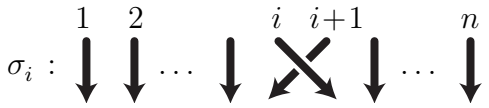


FIGURE 3. The elementary n strand braid diagram σ_i

We shall say that a colouring is *compatible* with a family of diagram transformations if, for any choice of the input colours, the output colours are not changed when the considered transformations are applied.

Lemma 1.1. *In the case of positive braid diagrams, the colourings defined in Figure 2 are compatible with isotopy if and only if the operation $*$ satisfies the identity*

$$x * (y * z) = (x * y) * (x * z). \tag{1.1}$$

Proof. As is well-known, two positive braid diagrams, *i.e.*, two diagrams obtained by stacking several diagrams σ_i one over the other, are isotopic if and only if they can be connected by applying finitely many times the so-called braid relations

$$\sigma_i\,\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geqslant 2, \quad \sigma_i\,\sigma_j\,\sigma_i = \sigma_j\sigma_i\,\sigma_j \text{ for } |i-j| = 1. \tag{1.2}$$

Thus the question is to check whether, for each choice of the input colours, the output colours of a positive braid diagram are not changed when braid relations are applied. The compatibility with $\sigma_i\,\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geqslant 2$ is automatic. As for the length 3 relation $\sigma_i\,\sigma_j\,\sigma_i = \sigma_j\sigma_i\,\sigma_j$ with $|i-j| = 1$—a Reidemeister move of type III—the argument is illustrated in Figure 4. □

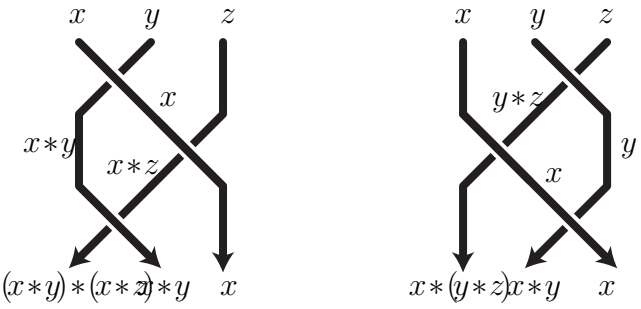


FIGURE 4. Compatibility of colouring with the braid relations

Let us consider now arbitrary braid diagrams, which contain, in addition to the elementary diagrams σ_i, their mirror images σ_i^{-1}.

Lemma 1.2. *In the case of arbitrary braid diagrams, the colourings defined in Figure 2 are compatible with isotopy if and only if the operation $*$ satisfies* (1.1) *and, in addition, we have*

$$x * (x \mathbin{\overline{*}} y) = x \mathbin{\overline{*}} (x * y) = y. \tag{1.3}$$

Proof. For arbitrary braid diagrams, isotopy corresponds to applying the braid relations of (1.2), plus the free group relations

$$\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = 1 \tag{1.4}$$

—which correspond to Reidemeister moves of type II. Then (1.3) arises as a translation of (1.4), as shown in Figure 5. □

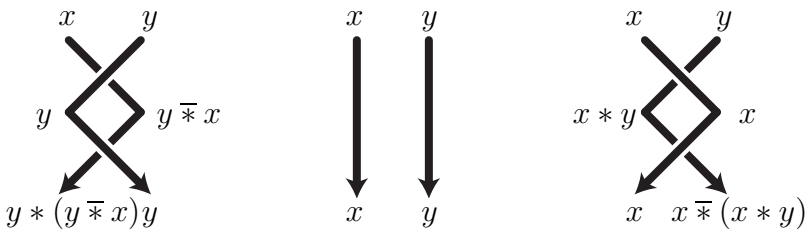


FIGURE 5. Compatibility of colouring with the free group relations

Relations (1.3) express that the operation $\overline{*}$ is a sort of left inverse for the operation $*$, and *vice versa*. In particular, (1.3) implies that all left translations relative to $*$ and $\overline{*}$ are bijections, hence in particular that left cancellation with respect to $*$ and $\overline{*}$ is allowed. Let us observe that the conjunction of (1.1) and (1.3) implies several other distributivity relations, namely

$$x \,\overline{*}\, (y \,\overline{*}\, z) = (x \,\overline{*}\, y) \,\overline{*}\, (x \,\overline{*}\, z), \tag{1.5}$$

$$x \,\overline{*}\, (y * z) = (x \,\overline{*}\, y) * (x \,\overline{*}\, z), \tag{1.6}$$

$$x * (y \,\overline{*}\, z) = (x * y) \,\overline{*}\, (x * z). \tag{1.7}$$

For instance, we find

$$x * (x \,\overline{*}\, (y * z)) =_{(1.3)} y * z =_{(1.3)} (x * (x \,\overline{*}\, y)) * (x * (x \,\overline{*}\, z)) =_{(1.1)} x * ((x \,\overline{*}\, y) * (x \,\overline{*}\, z)),$$

and (1.6) follows by cancelling x on the left.

Finally, let us consider link diagrams. The results takes the following form:

Lemma 1.3. *In the case of link diagrams, the colourings defined in Figure 2 are compatible with isotopy if and only if the operation $*$ satisfies Identities* (1.1) *and* (1.3)*, and, in addition,*

$$x * x = x. \tag{1.8}$$

Proof. Relation (1.8) arises when we translate the compatibility with Reidemeister moves of type I, as shown in Figure 6. As for other types, we observed that the free group relations are particular Reidemeister moves of type II, and that the braid relations are particular Reidemeister moves of type III. So Lemma 1.2 shows that (1.1) and (1.3) are necessary conditions. That they are sufficient requires a few additional verifications, because, in the general case, the orientations of the arcs need not be those of Figures 5 and 4. Checking all possible combinations is easy. For type III, in addition to (1.1) and (1.3), the requirements about $*$ and $\overline{*}$ turn out to be the identities (1.5), (1.6), and (1.7), which we have seen are consequences of the previous ones. Two case are displayed in Figures 7 and 8. □

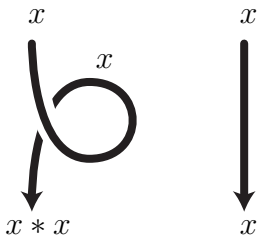


FIGURE 6. Compatibility of colouring with Reidemeister move of type I

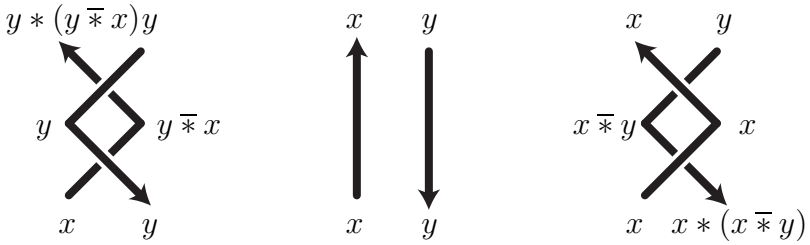


FIGURE 7. Compatibility of colouring with another Reidemeister move of type II (observe that, here, this is twice the same transformation)

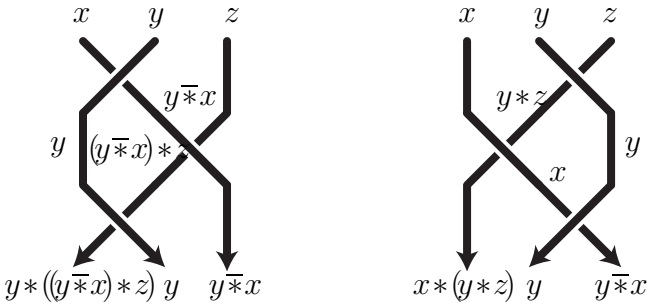


FIGURE 8. Compatibility of colouring with another Reidemeister move of type III: by (1.1) and (1.3), we have $y*((y\,\overline{*}\,x)*z) = (y*(y\,\overline{*}\,x))*(y*z) = x*(y*z)$

Relation (1.1) is called the *(left) self-distributivity* law for the operation $*$, as it expresses that $*$ is distributive with respect to itself; it will be denoted LD in the sequel, while (1.8) is the *idempotency* law. Observe that, when (1.1) and (1.3) are satisfied, $*$ satisfying the idempotency law is equivalent to $\overline{*}$ doing, as we have $x*(x\,\overline{*}\,x) =_{(1.3)} x =_{(1.8)} x*x$, hence $x\,\overline{*}\,x = x$ by cancelling x on the left. We are thus led to consider algebraic systems consisting on a set equipped with one or two self-distributive operations. We fix the following vocabulary.

Definition. (i) An algebraic system consisting of a set S equipped with a binary operation $*$ satisfying (1.1) is called an *LD-system*.

(ii) An algebraic system consisting of a set R equipped with two binary operations $*, \overline{*}$ satisfying (1.1) and (1.3) is called a *rack*—or an *LD-quasigroup* in the terminology of [19], or an *automorphic set* in that of [6].

(iii) An algebraic system consisting of a set Q equipped with two binary operations $*, \overline{*}$ satisfying (1.1), (1.3) and (1.8) is called a *quandle*—or, equivalently, an *LDI-quasigroup* in [19].

In the sequel, we choose "rack" and "quandle" because these are the most common names in the context of topology. As it stands, a rack involves two binary operations. Actually, each operation determines the other. Indeed, if $(R, *, \overline{*})$ is a rack, then, for all x, y in R, we have

$$x \,\overline{*}\, y = \text{ the unique } z \text{ satisfying } x * z = y, \tag{1.9}$$

and all left translations in the LD-system $(R, *)$ are bijective—hence they are automorphisms of $(R, *)$. Conversely, if $(R, *)$ is an LD-system where all left translations are bijective, then using (1.9) to define a second operation $\overline{*}$ gives R the structure of a rack. Such an LD-system can therefore be called a rack—or a quandle if its operation happens to be idempotent—without ambiguity.

Many examples of LD-systems will appear in the sequel. For the moment, let us just observe that, if S is any set, then S equipped with the operation $x * y = y$ is a quandle (the "trivial" quandle on S), and that, if G is a group, then G equipped with the conjugacy operation $x * y = xyx^{-1}$ is also a quandle (the "conjugacy" quandle on G).

1.3. **Two ways of using colourings.** Building on the previous common approach, we can use diagram colourings to study braids or links. It turns out that, up to now, colourings and self-distributive systems have been used in rather different ways according to whether either braids or links are considered. The point is that braids are *open* objects, while knots and links are *closed*.

In the case of braids, the strands have open initial and final ends, and the general principle is to fix a rack $(R, *, \overline{*})$ and then to use R to colour every braid diagram. In this way, every n strand braid b defines a mapping ρ_b of R^n into itself (Figure 9), hence a sort of R-valued representation of dimension n. We use ρ_b to extract information about b.

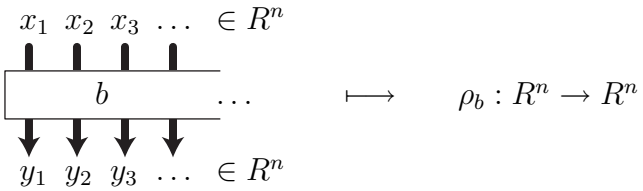


FIGURE 9. Using braid colourings: extracting information about the braid b from its action on sequences of colours

More formally, n strand braids (*resp.* positive braids) make a group B_n (*resp.* a monoid B_n^+), and considering the correspondence in R^n induced by colouring n strand diagrams amounts to defining an action of braid words on sequences of colours:

Definition. Assume that $(R, *, \overline{*})$ is an algebraic system consisting of a set equipped with two binary operations. For $2 \leqslant n \leqslant \infty$, we inductively define a right action of n strand braid words on R^n by $\boldsymbol{x} \bullet \varepsilon = \boldsymbol{x}$ (where ε denotes the empty word), and

$$\boldsymbol{x} \bullet (\sigma_i\, w) = (x_1, \dots, x_{i-1}, x_i * x_{i+1}, x_i, x_{i+2} \dots) \bullet w, \tag{1.10}$$

$$\boldsymbol{x} \bullet (\sigma_i^{-1} w) = (x_1, \dots, x_{i-1}, x_{i+1}, x_i \,\overline{*}\, x_{i+1}, x_{i+2} \dots) \bullet w. \tag{1.11}$$

Throughout the paper, we use the convention that, when $\boldsymbol{x}$ denotes a (finite or infinite) sequence, the successive elements of $\boldsymbol{x}$ are denoted $x_1, x_2, \dots$ Then Lemmas 1.1 and 1.2 yield the following result, which can be traced back at least to Brieskorn:

Proposition 1.4 ([6]). *(i) For each LD-system $(S, *)$,* (1.10) *defines an action of B_n^+ on S^n.*

(ii) For each rack $(R, *, \overline{*})$, (1.10) *and* (1.11) *define an action of B_n on R^n.*

The previous action will be called the *Hurwitz action* of braids on the powers of S or R. In this case, for $\boldsymbol{x}$ a sequence of elements of S or R, and b a braid, we denote $\boldsymbol{x} \bullet b$ for the result of applying b to $\boldsymbol{x}$, *i.e.*, for the sequence $\boldsymbol{x} \bullet w$ where w is an arbitrary expression of b.

The case of a knots or a link L is different. Again we can start with a fixed algebraic system, typically a quandle Q, and try to use Q to colour the arcs of a diagram representing L. Now the problem is that L is a closed diagram, and pushing the colours along the arcs is likely to result in obstructions. As is well-known, every link can be represented as the closure of a braid, so we can concentrate on this case. If L is the closure of the braid b and we choose arbitrary colours $x_1, x_2, \dots$ for the top strands of b, then the colours $y_1, y_2, \dots$ of the bottom strands of b are in general different from $x_1, x_2, \dots$. A natural solution to the problem is to go from Q to the quotient-quandle S_b of S obtained by identifying y_i with x_i for each i. Thus, the idea is no longer to use the same fixed algebraic system for each topological object, but rather to associate with every topological object a specific algebraic system, which, in good cases, we can hope to be an invariant of the considered knot or link (Figure 10).

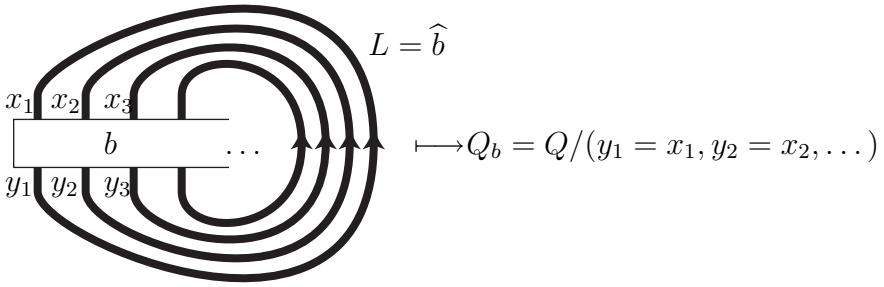


FIGURE 10. Using link colourings: extracting information about the link L from the associated quotient-structure

In this approach, the more general the initial quandle is, the most powerful the associated invariant is likely to be. In particular, for the closure L of an n strand braid, we can start with the free quandle on n generators. Then the associated quotient Q_L is called the *fundamental* quandle of L, and we have the following optimal result:

Proposition 1.5 (Joyce [37], Matveev [49]). *The fundamental quandle is a complete invariant of the isotopy type up to a mirror symmetry.*

Example 1.6. The trefoil knot of Figure 1 is the closure of the braid σ_1^3, and the reader will easily check that its fundamental quandle is the finitely generated

quandle that (as a quandle) admits the presentation $\langle x, y\,;\, ((x*y)*x)*(x*y) = x, (x*y)*x = y\rangle$, hence also

$$\langle x, y, z\,;\, x*y = z, y*z = x, z*x = y\rangle.$$

Proposition 1.5 shows that the fundamental quandle of a link captures almost completely the topological structure of that link, which is not surprising as the quandle identities are the exact algebraic counterpart of the Reidemeister transformations. The problem is that there is no known solution to the general isomorphism problem for finitely presented quandles, *i.e.*, there is no algorithm to decide whether two finitely presented quandles are isomorphic or not—and therefore Proposition 1.5 cannot be converted into an algorithm deciding whether two link diagrams are isotopic. Even recognizing free quandles, *i.e.*, recognizing unknottedness, remains problematic.

More partial information about the link can be extracted by considering quotients of the fundamental quandle. In terms of colourings, this amounts to starting with more particular quandles instead of free quandles. For instance, one can restrict to involutory quandles, which are those quandles in which the two operations coincide, *i.e.*, that satisfy $x*(x*y) = y$ for all x, y. General references in this direction are [31, 32].

Remark 1.7. Constructing an algebraic structure that is specific to the considered knot or link is not the only approach developed so far for using diagram colourings. In particular, counting the possible colourings associated with some fixed quandle is another possibility. With the help of some (co)-homological methods, it leads to link invariants of state-sum type [10, 11, 25].

Remark 1.8. Instead of calling $x*y$ the colour obtained when y is overcrossed by x, we could call it $y*x$ as well: both conventions equally appear in literature, our current one "$x*y$" seems to be more common in the case of braids, while the other one "$y*x$"—often denoted $x \triangleright y$—is more common in the case of knots and links. Of course, when the alternative convention is used, the identities are to be replaced with their symmetrized counterpart, in particular, left self-distributivity is to be replaced with right self-distributivity $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$.

2. Classical examples of racks and quandles

In this section, we review the classical examples of racks, and describe the properties of braids or links one captures by using the corresponding colourings. All results here are well-known, but, at the least, this review shows that the approach is useful, and it is a sort of warm-up before more sophisticated developments are mentioned.

2.1. **The trivial rack.** As already mentioned, any (nonempty) set S equipped with $x*y = x \mathbin{\overline{*}} y = y$ is a rack, and even a quandle. We shall refer to this structure as the *trivial rack* on S. Using a trivial rack to colour the arcs of a diagram amounts to deciding that the colours do not change at crossings.

In the case of braids and their action on sequences of colours, the output colours make a permutation of the input colours, so the action of a braid b on a trivial

rack S factors through the permutation of b. Formally, for each braid b in B_n, and every sequence $\boldsymbol{x}$ in S^n, we have

$$\boldsymbol{x} \bullet b = \mathrm{perm}(b)(\boldsymbol{x}), \tag{2.1}$$

where $\mathrm{perm}(b)$ denotes the permutation that specifies the initial positions of the strands in terms of their final positions. Thus, the Hurwitz action associated with this particular rack leads to the surjective homomorphism

$$\mathrm{perm} : B_n \to \mathfrak{S}_n.$$

In the case of a link, using the most general trivial rack means starting with a cardinality n set S when we are considering a link diagram that is the closure of an n strand braid diagram. Then identifying the sequence of output colours with the sequence of input colours yields a quotient S_L of S that has k elements if the represented link has k components. Thus the piece of information we can extract using trivial racks is the number of components.

2.2. **The shift rack.** Let $\mathbf{Z}$ denote the set of all integers. Then the operations

$$x * y = y + 1, \qquad x \mathbin{\overline{*}} y = y - 1 \tag{2.2}$$

turn $\mathbf{Z}$ into a rack. For every braid b in B_n, and every sequence $\boldsymbol{x}$ in $\mathbf{Z}^n$, we find

$$\sum(\boldsymbol{x} \bullet b) = \sum \boldsymbol{x} + \mathrm{sum}(b), \tag{2.3}$$

where $\sum \boldsymbol{x}$ denotes $x_1 + \cdots + x_n$, and $\mathrm{sum}(b)$ denotes the exponent sum of b, defined to be the difference between the number of positive and legative letters in any expression of b. Thus,the Hurwitz action leads here to the augmentation homomorphism

$$\mathrm{sum} : B_n \to (\mathbf{Z}, +)$$

that maps every generator σ_i to 1.

The current rack is not a quandle, as, for instance, we have $0 * 0 = 1 \neq 0$, so there is no direct way to use it to obtain a link invariant. Observe that the current rack as well as the trivial ones belong to the more general type $x * y = f(y)$, $x \mathbin{\overline{*}} y = f^{-1}(y)$, where f is a bijection of the underlying domain.

2.3. **The Alexander rack.** Assume that E be a $\mathbf{Z}[t, t^{-1}]$-module. The binary operations

$$x * y = (1 - t)x + ty, \qquad x \mathbin{\overline{*}} y = (1 - t^{-1})x + t^{-1}y \tag{2.4}$$

turn E into a rack, actually a quandle. For every n-strand braid b, and every sequence $\boldsymbol{x}$ in E^n, the output colours $\boldsymbol{x} \bullet b$ are linear combinations of the input colours $\boldsymbol{x}$. Therefore, there exists an $n \times n$-matrix $r_B(b)$ satisfying

$$\boldsymbol{x} \bullet b = \boldsymbol{x} \times r_B(b). \tag{2.5}$$

Thus we obtain a linear representation

$$r_B : B_n \to \mathrm{GL}_n(\mathbf{Z}[t, t^{-1}]).$$

It turns out that this representation is the (unreduced) Burau representation.

Considering the case of links amounts to quotienting under the relations $\boldsymbol{x} \bullet b = \boldsymbol{x}$: these relations generate the Alexander ideal of the link $\widehat{b}$, and, in particular, the Alexander polynomial can be recovered from this ideal.

2.4. **The conjugacy rack.** Let G be a group. Then the binary operations defined by

$$x * y = xyx^{-1}, \qquad x \mathbin{\overline{*}} y = x^{-1}yx \tag{2.6}$$

turn G into a rack, and even a quandle. In particular, let F_n be the free group based on $\{x_1, \dots, x_n\}$. Then define elements $y_1, \dots, y_n$ of F_n by

$$(x_1, \dots, x_n) \bullet b = (y_1, \dots, y_n), \tag{2.7}$$

and let $\varphi(b)$ be the endomorphism of F_n that maps x_i to y_i for every i. Then φ is an endomorphism of B_n into $\mathrm{End}(F_n)$, and, as $\varphi(b^{-1}) = \varphi(b)^{-1}$ holds by construction, the image of φ is actually included in $\mathrm{Aut}(F_n)$. Thus, the Hurwitz action associated with the conjugacy rack leads to Artin's representation

$$\varphi : B_n \to \mathrm{Aut}(F_n),$$

which is known to be faithful—a proof will be mentioned below.

According to our general scheme, going to links means attaching to the closure $\widehat{b}$ of the braid b the quotient of the free group F_n under the relations $y_i = x_i$: the resulting group is the fundamental group of the complement of $\widehat{b}$, and the obtained presentation is known as the Wirtinger presentation.

Using Fox' free differential calculus, it is standard to derive the Alexander rack from the conjugacy rack of a free group—hence the Alexander polynomial of a link from the Wirtinger presentation of its group.

2.5. **Free racks.** The previous examples show that a number of classical results about braids or links can be obtained using diagram colourings and self-distributive systems. We are thus led to the natural question: Can we get more by considering further examples of racks or quandles?

We do not claim that the answer is negative, but we shall see now that, in some sense, we are close to the optimum when considering the conjugacy rack of a free group. Indeed, we can expect that using the most general racks will lead to the most powerful results, and, in this respect, using *free* racks is the best we can do. Now free racks are very close to conjugacy racks.

Assume that G is a group, and X is a subset of G. We define binary operations on $G \times X$ by

$$(a, x) * (b, y) = (axa^{-1}b, y), \qquad (a, x) \mathbin{\overline{*}} (b, y) = (ax^{-1}a^{-1}b, y). \tag{2.8}$$

The operations of (2.8) can valuably be called *half-conjugacy* as, when G is a free group, they amounts to selecting the first half of the conjugacy words; in any case, mapping (a, x) to axa^{-1} yields a morphism of $G \times X$ equipped with the half-conjugacy operations into G equipped with the conjugacy operations.

Proposition 2.1 ([24]). *For G a group and $X \subseteq G$, the set $G \times X$ equipped with half-conjugacy is a rack. Moreover, if G is the free group based on X, then the half-conjugacy rack $X \subseteq G$ is a free rack based on X—more exactly on $\{1\} \times X$.*

The verifications are easy. In $X \times G$, we have $(a, x) * (a, x) = (ax, x)$. Thus, a free rack is not a quandle. But we see that the difference between the half-conjugacy rack and the conjugacy rack on a free group only lies in the repetition of the central letter, making the half-conjugacy rack appear as a sort of product of the conjugacy rack and the shift rack of Subsection 2.2.

A consequence of this is that free racks, and therefore, arbitrary racks, satisfy some extra identities that, we shall see in the sequel, have no direct connection with self-distributivity. Excepted the shift rack and the free racks, all above mentioned examples are idempotent, *i.e.*, they satisfy the identity $x * x = x$. We observed that this is not the case of the free racks, but the latter are so close to conjugacy racks implies that they inherit a weak form of idempotence:

Lemma 2.2. *Every rack satisfies the identity*

$$(x * x) * y = x * y. \tag{2.9}$$

The verification is trivial using the explicit formulas in (2.8):

$$((a, x) * (a, x)) * (b, y) = (ax, x) * (b, y) = (axa^{-1}b, y) = (a, x) * (b, y).$$

Alternatively, we may observe that Identity (2.9) follows from the rack identities:

$$(x * x) * y = (x * x) * (x * (x \mathbin{\overline{*}} y)) = x * (x * (x \mathbin{\overline{*}} y)) = x * y.$$

Important from our point of view is the fact that Identity (2.9) prevents racks from being orderable in any reasonable sense. Indeed, on the shape of natural numbers and, more generally, of free semigroups, it is natural to consider possible orderings that extend the left divisibility relation, *i.e.*, orderings in which $y = x * z$ implies $x < y$. A necessary condition for such an ordering to possibly exist is that no element is a left divisor of itself. Now, Lemma 2.2 shows that, if $(R, *)$ is a rack, then every element of the form $x * x$ is a left divisor of itself, since we have $x * x = (x * x) * x$. So, at this point, we are led to the following double question:

Question 2.3. *Does there exist some LD-system (necessarily not an rack) where left division admits no cycle? If so, can we use such an LD-system to colour braids?*

We shall see in the sequel that the answer to both questions is positive. For the moment, let us conclude with a last example, which provides a (very) partial answer to Question 2.3. We denote by I_∞ the monoid of all injective, non-bijective mappings of $\mathbf{N}$ into itself equipped with composition. For f, g in I_∞, let us define the injection $f * g$ by

$$f * g(n) = \begin{cases} fgf^{-1}(n) & \text{if } n \text{ belongs to the image of } f, \\ n & \text{otherwise.} \end{cases} \tag{2.10}$$

It is easy to verify that this operation is left self-distributive, and that the coimage of $f * g$ is the image under f of the coimage of g—the coimage being the complement of the image in $\mathbf{N}$. Hence no equality of the form $f * g = f$ is possible in I_∞, for the coimage of $f * g$ is included in the image of f, hence disjoint from the coimage of f. It follows that left division in $(I_\infty, *)$ admits no cycle of length 1—but it can be seen that it admits cycles of length 2.

3. Colouring with more general LD-systems

A few more examples of LD-systems still exist, but most of them are connected with the conjugacy operation of a group, and, in particular, they are racks (or even quandles)—here we think in particular of the LD-systems one can build using root systems and their reflections [6], or alternating bilinear forms [54]. The situation radically changed when new LD-systems of a completely different flavour appeared at the end of the 1980's in connection with set theoretical objects called elementary embeddings [16, 19]. There is no need that we describe these examples here, but we shall just say that these examples did seem strange and promising enough to give a strong motivation for investigating Question 2.3, and, in particular, proving that the Hurwitz action of braids can be extended to arbitrary left cancellative LD-systems, at the expense of becoming a partial action.

This extension is what we shall explain in this section.

3.1. **Braid word reversing.** We have to begin with a detour. Lemma 1.1 tells us that we can use $(S, *)$ to colour the strands of a positive braid whenever $(S, *)$ is an LD-system, *i.e.*, whenever $*$ is a left self-distributive operation on S. On the other hand, Garside's theory [34] guarantees that every braid is the quotient of two positive braids: for each b in B_n, there exist b_1, b_2 in B_n^+ such that b equals $b_1^{-1}b_2$, *i.e.*, equivalently, b can be represented by a word of the form $u^{-1}v$ where u, v are positive braid words (no letter σ_i^{-1}). Using this result to extend the action of positive braids into an action on arbitrary braids is natural.

However, things are not so easy. The problem is that, if b is represented by $u^{-1}v$, then we can use an arbitrary LD-system $(S, *)$ to colour the strands of the diagram encoded by $u^{-1}v$, but, in general, we cannot prove uniqueness and compatibility with respect to the braid and free group relations. Going further requires that we improve on Garside's result and use a decomposition result that is more precise than the mere existence of a fractional expression. This is where the technique called *word reversing* is useful.

In the sequel, we denote by $\boldsymbol{\sigma}$ the alphabet $\{\sigma_1, \sigma_2, \dots\}$. We use $\boldsymbol{\sigma}^*$ for the set of all words on $\boldsymbol{\sigma}$, *i.e.*, for the set of all positive braid words. Braid word equivalence is denoted by $\equiv$: if w, w' are braid words, $w \equiv w'$ means that w and w' represent the same braid.

Now, let us observe that, if f is the mapping of $\boldsymbol{\sigma} \times \boldsymbol{\sigma}$ to $\boldsymbol{\sigma}^*$ defined by

$$f(\sigma_i, \sigma_j) = \begin{cases} \sigma_j & \text{for } |i-j| \geqslant 2, \\ \sigma_j\sigma_i & \text{for } |i-j| = 1, \\ \varepsilon & \text{for } i = j, \end{cases}$$

then the presentation (1.2) of the braid group consists of all relations

$$\sigma_i \ f(\sigma_i, \sigma_j) = \sigma_j \ f(\sigma_j, \sigma_i) \tag{3.1}$$

with $i \neq j$. Now (3.1) also implies

$$\sigma_i^{-1} \ \sigma_j = f(\sigma_i, \sigma_j) \ f(\sigma_j, \sigma_i)^{-1}. \tag{3.2}$$

It follows that, if we replace in a braid word w a subword of the form $\sigma_i^{-1}\sigma_j$ with the corresponding word $f(\sigma_i, \sigma_j)f(\sigma_j, \sigma_i)^{-1}$, then the new word is equivalent to w.

Definition. Assume that w, w' are braid words. We say that w is *right reversible* to w' (in k steps) if one can transform w into w' by successively replacing k subwords of the type $\sigma_i^{-1}\,\sigma_j$ with the corresponding subwords $f(\sigma_i\,,\sigma_j)\;f(\sigma_j,\sigma_i\,)^{-1}$.

Example 3.1. Consider $w = \sigma_1^{-1}\sigma_3^{-1}\sigma_2\sigma_4$. Then w contains the subword $\sigma_3^{-1}\sigma_2$, and this is the only subword of the type $\sigma_i^{-1}\sigma_j$ in w: so the only way of applying right reversing to w is to go to $w_1 = \sigma_1^{-1}\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_4$. Now, in w_1, there are two subwords of the type $\sigma_i^{-1}\sigma_j$, namely the initial subword $\sigma_1^{-1}\sigma_2$, and the final subword $\sigma_3^{-1}\sigma_4$. Hence two words can be obtained from w by two steps of word reversing, namely $\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_4$ and $\sigma_1^{-1}\sigma_2\sigma_3\sigma_2^{-1}\sigma_4\sigma_3\sigma_4^{-1}\sigma_3^{-1}$. The reader can continue, and check that all sequences of word reversing from w end in 16 steps with the word $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_4^{-1}\sigma_3^{-1}$. The latter word can no longer be reversed, for it contains no more factor of the form $\sigma_i^{-1}\sigma_j$.

By construction, w being right reversible to w' implies that w and w' are equivalent. Of course, the converse implication need not be true. However, in good cases [20], typically in the case of the standard braid presentation, as well as in the case of the alternative band generator presentation of [4] (after some technical adaptation), there is a sort of converse implication:

Lemma 3.2 ([15])**.** *Assume that u, v are positive braid words. Then u and v are equivalent, i.e., they represent the same (positive) braid if and only if the word $u^{-1}v$ is right reversible to the empty word.*

This technical result is instrumental in the following property, which will be crucial here:

Proposition 3.3. *For every braid word w, there exist unique positive words $N_R(w)$, $D_R(w)$ such that w is right reversible to $N_R(w)D_R(w)^{-1}$. Then, $w \equiv w'$ holds if and only if there exist positive words v, v' satisfying*

$$N_R(w)\;v \equiv N_R(w')\;v' \quad \textit{and} \quad D_R(w)\;v \equiv D_R(w')\;v'. \tag{3.3}$$

In the above result, N_R and D_R stand for "right numerator" and "right denominator". For instance, in the case of the word w of Example 3.1, the words $N_R(w)$ and $D_R(w)$ are $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1$ and $\sigma_3\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4$, respectively.

(The easy part of) Lemma 3.2 guarantees that w is equivalent to $N_R(w)\;D_R(w)^{-1}$, and, therefore, a consequence of Proposition 3.3 is that every braid can be expressed as a right fraction ab^{-1} with a, b in B_∞^+—as asserted by Garside's theory. However, Proposition 3.3 gives us more than the mere equivalence of the words w and $N_R(w)D_R(w)^{-1}$: it gives a distinguished way for transforming w into $N_R(w)D_R(w)^{-1}$, one that avoids introducing any subword of the type $\sigma_i^{-1}\sigma_i$ or $\sigma_i\,\sigma_i^{-1}$.

As braid relations are symmetric, everything we said so far about right reversing can be transposed into similar statements about a symmetric *left* reversing, in which the basic step consists in replacing $\sigma_i\,\sigma_j^{-1}$ with $g(\sigma_j\,,\sigma_i\,)^{-1}\;g(\sigma_i\,,\sigma_j)$, where g is a mapping of $\boldsymbol{\sigma}\times\boldsymbol{\sigma}$ into $\boldsymbol{\sigma}^*$ that the reader will easily find by himself. The counterpart of Proposition 3.3 is:

Proposition 3.4. *For every braid word w, there exist unique positive words $N_L(w)$, $D_L(w)$ such that w is left reversible to $D_L(w)^{-1}N_L(w)$. Then, $w \equiv w'$ holds if and*

only if there exist positive words u, u' satisfying

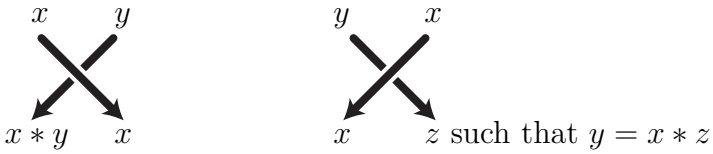
$$u\ N_{\scriptscriptstyle L}(w) \equiv u'\ N_{\scriptscriptstyle L}(w') \quad \textit{and} \quad u\ D_{\scriptscriptstyle L}(w) \equiv u'\ D_{\scriptscriptstyle L}(w'). \tag{3.4}$$

Remark 3.5. Braid word reversing is defined at the level of braid words only, and not at the level of braids. Indeed, the functions $N_{\scriptscriptstyle R}$ and $D_{\scriptscriptstyle R}$ do not induce well-defined mapping of B_∞ into B_∞^+. For instance, let $w = \sigma_1\sigma_1^{-1}$ and $w' = \varepsilon$. Then w and w' are equivalent, as both represent the unit braid. Now, by definition, each of w, w' is terminal with respect to right reversing, as it contains no subword $\sigma_i\,\sigma_j^{-1}$, and we find $N_{\scriptscriptstyle R}(\sigma_1\sigma_1^{-1}) = D_{\scriptscriptstyle R}(\sigma_1\sigma_1^{-1}) = \sigma_1$ and $N_{\scriptscriptstyle R}(\varepsilon) = D_{\scriptscriptstyle R}(\varepsilon) = \varepsilon$ (the empty word). This shows that $w \equiv w'$ does *not* imply $N_{\scriptscriptstyle R}(w) \equiv N_{\scriptscriptstyle R}(w')$ or $D_{\scriptscriptstyle R}(w) \equiv D_{\scriptscriptstyle R}(w')$, and (3.3) is optimal in some sense.

Of course, the functions $N_{\scriptscriptstyle L}$ and $D_{\scriptscriptstyle L}$ do not induce well-defined mappings on braids either. However, let us mention that using a double, left and right, word reversing results in mappings that are invariant under braid equivalence: if we define $N_{\scriptscriptstyle RL}(w) = N_{\scriptscriptstyle L}(N_{\scriptscriptstyle R}(w)D_{\scriptscriptstyle R}(w)^{-1})$ and $D_{\scriptscriptstyle RL}(w) = D_{\scriptscriptstyle L}(N_{\scriptscriptstyle R}(w)D_{\scriptscriptstyle R}(w)^{-1})$, then the mappings $N_{\scriptscriptstyle RL}$ and $D_{\scriptscriptstyle RL}$ induce well-defined mappings on braids, *i.e.*, $w \equiv w'$ implies $N_{\scriptscriptstyle RL}(w) \equiv N_{\scriptscriptstyle RL}(w')$ and $D_{\scriptscriptstyle RL}(w) \equiv D_{\scriptscriptstyle RL}(w')$. It follows in particular that $w \equiv \varepsilon$ holds if and only if the words $N_{\scriptscriptstyle RL}(w)$ and $D_{\scriptscriptstyle RL}(w)$ are empty, *i.e.*, if, starting from w, the double reversing process consisting in right reversing w and then left reversing the result ends up with an empty word.

3.2. **The Hurwitz partial action of braids on left cancellative LD-systems.** Using braid word reversing, we shall now be able to extend the action of B_n^+ on S^n into a partial action of B_n on S^n when $(S, *)$ is a left cancellative LD-system, *i.e.*, one in which left translations are injective, but not necessarily surjective. However, the price to pay for such an extension is that, in general, we shall obtain a *partial* action only, *i.e.*, one that need not be defined everywhere.

Assume that $(S, *)$ is a fixed LD-system and w is an n-strand braid word, $n \leqslant \infty$. The rule of Figure 2 left tells us how to use $(S, *)$ to colour positive crossings in w. As for negative crossings, we have so far no way of colouring them, as no second operation $\overline{*}$ is specified. However, we have seen in Lemma 1.2 that the only way that guarantees compatibility with the free group relations $\sigma_i\,\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = \varepsilon$ is to use



If we do not assume the operation $*$ to admit left cancellation, then there can exist more than one element z satisfying $x * z = y$, and our principle of putting input colours at the top of the strands and pushing them to the bottom cannot be applied. But if the operation $*$ admits left cancellation, then we are not sure that every sequence of colours can be propagated but, at the least, we know that each sequence of input colours leads to *at most one* sequence of output colours. This is the approach we will develop now.

From now on, we shall consider LD-systems $(S, *)$ that admit left cancellation, and try to use them to colour braid diagrams—or, possibly, link diagrams. If $(S, *)$ is not a rack, then it is not clear that every braid diagram can be coloured using S,

or that the action leads to a well-defined result, *i.e.*, that equivalent diagrams lead to coherent results. Actually, this is the case, and, to prove it, braid word reversing is the main ingredient.

Lemma 3.6. *Assume that $(S, *)$ is a left cancellation LD-system.*

(i) Let $w_1, \dots, w_p$ be arbitrary n strand braid words. Then there exists at least one sequence $\boldsymbol{x}$ in S^n such that $\boldsymbol{x} \bullet w_i$ is defined for each i.

(ii) Assume that w, w' are equivalent n strand braid words, and $\boldsymbol{x}$ is a sequence in S^n such that both $\boldsymbol{x} \bullet w$ and $\boldsymbol{x} \bullet w'$ are defined. Then the latter sequences are equal.

Proof. We outline the argument, because it is crucial. For (i), let us first consider the case of a single word w. By Proposition 3.4, there exist two positive braid words u, v, namely the left denominators and numerators of w, such that w is left reversible to $u^{-1}v$, and, therefore, uw is left reversible to v. Let $\boldsymbol{z}$ be an arbitrary sequence in S^n. Then we can colour v (which is a positive diagram) starting from colours $\boldsymbol{z}$, and we obtain $\boldsymbol{z} \bullet v$ as output colours. We claim that $\boldsymbol{z}$ is also eligible for colouring uw, *i.e.*, no obstruction can happen with negative crossings. Indeed, we observe that, when w' is left reversible to w'', then $\boldsymbol{x} \bullet w'' = \boldsymbol{y}$ implies $\boldsymbol{x} \bullet w' = \boldsymbol{y}$, this meaning in particular that the considered action is defined. To prove this, it suffices to consider each elementary reversing step. The typical case of $\sigma_1\sigma_2^{-1}$ left reversing to $\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1$ is illustrated in Figure 11. So we conclude that, for every sequence $\boldsymbol{z}$, the sequence $\boldsymbol{z} \bullet u$ is eligible as input colours for colouring w, and the output colours are then $\boldsymbol{z} \bullet v$.

In the case of several words $w_1, \dots, w_p$, we use the fact that the left denominators of $w_1, \dots, w_p$ admit a common right multiple in B_n^+ to find a positive word u such that each word uw_i is left reversible to some positive word. The sequel of the argument is then the same.

For (ii), the argument is analogous, but it now involves right reversing. Here the point is that, if w is right reversible to w', then every sequence of colours that is eligible for colouring w must be eligible for colouring w'—so the deduction goes in the opposite direction as for left reversing. Then one uses the fact that, if w and w' are equivalent, then there exists equivalent positive word u, u' such that wu and $w'u'$ are right reversible to equivalent positive words. □

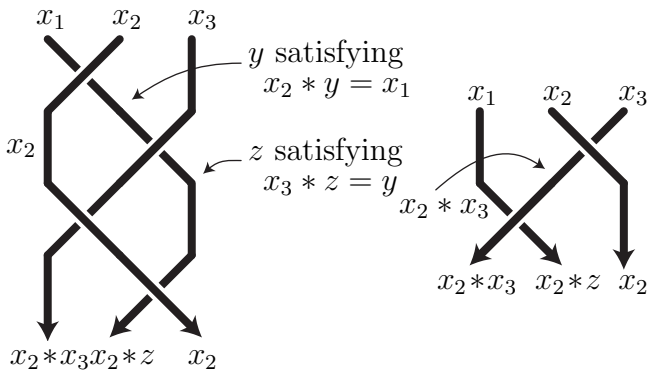


FIGURE 11. The colourability of the left diagram guarantees that of the right diagram: indeed we have $(x_2 * x_3) * (x_2 * z) = x_2 * (x_3 * z) = x_2 * y = x_1$

The previous technical result enable us to define a partial action of braids on the powers of any left cancellative LD-system: the action need not be defined for any initial choice of colours but we know that, for a given braid, there always exists some initial choice of colours for which the action is defined, and that any such choice leads to the same final result. If $\boldsymbol{x}$ is a sequence of colours and b is a braid, we shall denote by $\boldsymbol{x} \bullet b$ the sequence $\boldsymbol{x} \bullet w$ for w any braid word representing b such that the sequence is defined, if there is one.

4. Non-classical LD-systems

The interest of extending the Hurwitz action to left cancellative LD-systems that are not racks is that new systems of a different flavour become eligible. We shall see now how using such non-classical LD-systems naturally leads to new applications, such as ordering the braids. According to our general approach, we shall put the emphasis on the role of braid colourings in the construction. We shall successively appeal to two LD-systems, and, therefore, to two Hurwitz actions, namely free LD-systems firstly, and then another LD-system involving braids themselves.

4.1. **Free LD-systems.** For rather trivial general reasons there exists for every nonempty set X a free LD-system based on X, thus an analog of a free group or a free monoid in the category of LD-systems.

Definition. We define $\mathbf{D}$ to be the free LD-system on one generator. The generators of $\mathbf{D}$ (which turns out to be unique) will be denoted g, and its operation by $*$.

Thus $\mathbf{D}$ consists of all formal expressions g, $g * g$, $g * (g * g)$, etc., two such expressions being identified when one can go from one to the other applying the left self-distributivity identity. One should think of the LD-system $\mathbf{D}$ as a counterpart to the semigroup of positive integers $\mathbf{Z}_+$ (equipped with addition): the latter is the free semigroup with one generator, *i.e.*, the free object of rank 1 in the category (or variety) associated with the identity $x(yz) = (xy)z$, while $\mathbf{D}$ is the free object of rank 1 in the category associated with the identity $x(yz) = (xy)(xz)$. Both algebraic systems share some properties, but the LD-system $\mathbf{D}$ turns out to be much more complicated than its counterpart $\mathbf{Z}_+$—and than free racks and free quandles. We refer to [19] for a thorough study of free LD-systems.

Definition. For $*$ a binary operation on S and x, y in S, we say that x is a *left divisor* of y if $y = x * z$ holds for some z, and denote by $\sqsubset$ the transitive closure of the left divisibility relation.

In the case of the free semigroup $\mathbf{Z}_+$, the left divisibility relation is transitive, and it coincides with the usual ordering of the integers. In a self-distributive framework, the idea remains the same, but transitivity is no longer guaranteed, and that is why we must appeal to the transitive closure explicitly. So, $x \sqsubset y$ is true if and only if there exists a nonempty finite sequence $(z_1, \dots, z_p)$ satisfying

$$y = (\dots((x * z_1) * z_2)\dots) * z_p. \tag{4.1}$$

The similarity with the integers should make the following crucial result natural:

Proposition 4.1 ([14])**.** *The relation $\sqsubset$ is a linear ordering on $\mathbf{D}$, and it is compatible with multiplication on the left.*

As in the case of positive integers (with 1 instead of g), the generator g turns out to be the minimal element of $(\mathbf{D}, \sqsubset)$, and, for each x in $\mathbf{D}$, the element $x * g$ is an immediate successor of x with respect to $\sqsubset$, so that the first elements of $\mathbf{D}$ are g, $g*g$, $(g*g)*g$, etc.—exactly as 1, $1+1$, $(1+1)+1$, etc. are the first elements of $\mathbf{Z}_+$. However, the similarity stops here, as $\mathbf{D}$ contains a number of elements beyond the latter elements: for instance, the element $g * (g * g)$ is larger than all of them.

Although the statement of Proposition 4.1 looks simple, no easy proof is known so far. The only trivial point is the compatibity with left multiplication, which follows from self-distributivity immediately. The remaining part splits into two non-trivial results, namely that any two elements of $\mathbf{D}$ always are comparable with respect to $\sqsubset$, *i.e.*, at least one of $x \sqsubset y$, $x = y$, $y \sqsubset x$ holds for all x, y in $\mathbf{D}$—called *Comparison Property*—and that the relation $\sqsubset$ has no cycle, *i.e.*, $x \sqsubset x$ is impossible for every x in $\mathbf{D}$—called *Acyclicity Property*. It can be mentioned that Proposition 4.1 extends to free LD-systems with more than one generator (using using some lexicographic extension of $\sqsubset$), but we shall not use this result in the sequel. Proposition 4.1 shows that free LD-systems are very different from racks. In particular, the identity $x * y = (x * x) * y$, which we have seen holds in every rack, badly fails in $\mathbf{D}$: for instance, $g*g$ is a left divisor of $(g*g)*g$, so these elements cannot be equal. Actually it can be shown that, in many aspects, racks and free LD-systems are diametrally opposed in the category of all LD-systems.

An easy consequence of Proposition 4.1 is that the LD-system $\mathbf{D}$ admits left cancellation. Indeed, assume $z * x = z * y$ in $\mathbf{D}$. By the Comparison Property, at least one of $x \sqsubset y$, $x = y$, $y \sqsubset x$ holds. Now $x \sqsubset y$ implies $z * x \sqsubset z * y$, hence $z * x \neq z * y$, and so does $y \sqsubset x$. So $x = y$ is the only possibility.

It follows that $\mathbf{D}$ is eligible for colouring braid diagrams and that there exists a well-defined partial Hurwitz action of B_n on $\mathbf{D}^n$ for every n. Proposition 4.1 shows that $\mathbf{D}$ is, in a natural sense, an orderable LD-system, so it is not suprising that using this LD-system leads to ordering braids. To this end, we first order each power $\mathbf{D}^n$ using the lexicographical extension $\sqsubset^{Lex}$ of $\sqsubset$: $\boldsymbol{x} \sqsubset^{Lex} \boldsymbol{y}$ holds if and only if, for some i, we have $x_i \sqsubset y_i$ and $x_j = y_j$ for $j < i$. Now, we have a linear ordering on sequences of colours, and the idea for ordering braids is straightforward: starting with two braids b_1, b_2, we put some initial colours $\boldsymbol{x}$ from $\mathbf{D}$, which we know is possible by Lemma 3.6(i), and we compare the output colours $\boldsymbol{x} \bullet b_1$ and $\boldsymbol{x} \bullet b_2$ using the lexicographic order on sequences of colours. This obvious application of the colouring principle works, and the result is:

Proposition 4.2 ([14]). *For b_1, b_2 in B_n, say that $b_1 < b_2$ is true if there exists a sequence $\boldsymbol{x}$ in $\mathbf{D}^n$ such that $\boldsymbol{x} \bullet b_1 \sqsubset^{Lex} \boldsymbol{x} \bullet b_2$ holds. Then the relation $<$ is a linear ordering on B_n that is compatible with multiplication on the left.*

As one can expect, the main point is to prove that the relation $<$ does not depend on the choice of the initial sequence of colours $\boldsymbol{x}$.

We conclude the section with another application of colourings associated with the free LD-system $\mathbf{D}$.

Definition. We say that a braid b is σ_1-*positive* if, among all possible expressions of b, there is at least one in which σ_1 occurs, but σ_1^{-1} does not. We say that a

braid b is *σ-positive* if b can be expressed as $\partial^k b_0$ for some σ_1-positive braid b_0 and some $k \geqslant 0$.

Thus, for instance, the braid $\sigma_1\sigma_2\sigma_1^{-1}$ is σ_1-positive—hence σ-positive—because, among its (infinitely many) expressions, there is $\sigma_2^{-1}\sigma_1\sigma_2$, in which σ_1 occurs, but σ_1^{-1} does not.

Proposition 4.3 ("Property ***A***"). *A σ-positive braid is not trivial.*

As the shift endomorphism ∂ is injective, it suffices to consider the case of a σ_1-positive braid, and the complete proof is then given in Figure 12: once we know that every braid diagram can be coloured in at least one way using colours from **D**, the result is straightforward.

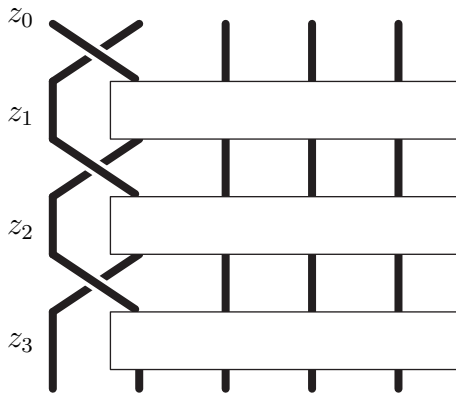


FIGURE 12. Proof of Property ***A***: Consider a diagram in which σ_1 occurs but σ_1^{-1} does not, and put colours from **D**; the left colours make an increasing sequence $z_0 \sqsubset z_1 \sqsubset z_2 \sqsubset \dots$, as, for each i, by construction, $z_{i+1} = z_i * x_i$ holds for some x_i. So we have $z_p \neq z_0$, and the output colour cannot be the input colours

4.2. **Twisted braid conjugation.** We shall now consider a new non-classical left self-distributive operation, namely one that involves braids themselves.

We recall that B_∞ denotes the braid group on infinitely many strands indexed by positive integers: B_∞ is the direct limit of all groups B_n when B_n is embedded into B_{n+1} by adding a new strand at the right. The group B_∞ is equipped with an injective, non-surjective endomorphism, namely the *shift* homomorphism ∂ that maps σ_i to σ_{i+1} for each i.

The following binary operation on B_∞ can be seen as a sort of twisted version of the usual conjugation operation.

Definition. For b_1, b_2 in B_∞, we put

$$b_1 * b_2 = b_1 \cdot \partial b_2 \cdot \sigma_1 \cdot \partial b_1^{-1}. \tag{4.2}$$

We say that a braid b is *special* if it belongs to the closure of $\{1\}$ under operation $*$. The set of all special braids is denoted B_∞^{sp}.

For instance, the reader can check equalities like $1 * 1 = \sigma_1$, $1 * (1 * 1) = \sigma_2\sigma_1$, $(1 * 1) * 1 = \sigma_1^2\sigma_2^{-1}$, etc. Thus the braids σ_1, $\sigma_2\sigma_1$, and $\sigma_1^2\sigma_2^{-1}$ are special. Some motivation for introducing the above operation wil be given below; however, for a complete explanation, we refer to [19] once again.

Lemma 4.4. *The set B_∞ equipped with the operation $*$ of* (4.2) *is a left cancellative LD-system, and so is its subsystem B_∞^{sp}.*

The easy verifications are left to the reader. It follows that we can use the left cancellative LD-system $(B_\infty, *)$ to colour the strands of the braid diagrams. In other words, we have obtained a partial Hurwitz action of B_n on B_∞^n. Technically, the point will be the following easy, but surprising result that connects two *a priori* unrelated things, namely the internal product of braids and the external Hurwitz action of braids on $(B_\infty, *)$—in our approach, this lemma can be taken as the actual motivation for the definition of the operation $*$: it is easy to see that (4.2) is the only possible definition leading to (4.3).

Lemma 4.5. *For $\boldsymbol{x}$ in B_∞^n, define* $\mathrm{eval}(\boldsymbol{x}) = x_1 \cdot \partial x_2 \cdot \partial^2 x_3 \cdot \dots$. *Then, if $\boldsymbol{x}$ is a sequence in B_∞ and $\boldsymbol{x} \bullet b$ is defined, we have*

$$\mathrm{eval}(\boldsymbol{x} \bullet b) = \mathrm{eval}(\boldsymbol{x}) \cdot b. \tag{4.3}$$

Proof. An easy computation just relying on the explicit definition of the operation $*$. Indeed, we have

$$\begin{aligned}
\mathrm{eval}(\boldsymbol{x} \bullet \sigma_i) &= \mathrm{eval}((x_1, \dots, x_i * x_{i+1}, x_i, \dots)) \\
&= x_1 \cdot \partial x_2 \cdot \dots \cdot \partial^{i-1}(x_i * x_{i+1}) \cdot \partial^i x_i \cdot \partial^{i+1} x_{i+2} \dots \\
&= x_1 \cdot \partial x_2 \cdot \dots \cdot \partial^{i-1} x_i \cdot \partial^i x_{i+1} \cdot \sigma_i \cdot \partial^i x_i^{-1} \cdot \partial^i x_i \cdot \partial^{i+1} x_{i+2} \dots \\
&= x_1 \cdot \partial x_2 \cdot \dots \cdot \partial^{i-1} x_i \cdot \partial^i x_{i+1} \cdot \sigma_i \cdot \partial^{i+1} x_{i+2} \dots \\
&= x_1 \cdot \partial x_2 \cdot \dots \cdot \partial^{i-1} x_i \cdot \partial^i x_{i+1} \cdot \partial^{i+1} x_{i+2} \dots \cdot \sigma_i = \mathrm{eval}(\boldsymbol{x}) \cdot \sigma_i,
\end{aligned}$$

which gives the basic case $b = \sigma_i$. □

Lemma 4.5 implies that the Hurwitz action of B_∞ on $(B_\infty, *)$ is strongly faithful in the sense that, if there exists at least *one* sequence of braids $\boldsymbol{x}$ such that $\boldsymbol{x} \bullet b$ and $\boldsymbol{x} \bullet b'$ are defined and equal, then b and b' are equal. Indeed, $\boldsymbol{x} \bullet b = \boldsymbol{x} \bullet b' = \boldsymbol{y}$ implies $b = \mathrm{eval}(\boldsymbol{y}) \cdot \mathrm{eval}(\boldsymbol{x})^{-1} = b'$.

For our purpose, Lemma 4.5 is important because it guarantees that every braid can be expressed in terms of special braids, *i.e.*, in terms of braids constructed from the trivial braid using the operation $*$ exclusively.

Proposition 4.6. *Every braid b in B_n admits a decomposition of the form*

$$b = \partial^{n-1} b_n^{-1} \cdot \dots \cdot \partial b_2^{-1} \cdot b_1^{-1} \cdot b_1' \cdot \partial b_2' \cdot \dots \cdot \partial^{n-1} b_n' \tag{4.4}$$

where $b_1, \dots, b_n, b_1', \dots, b_n'$ are special braids. If b belongs to B_b^+, we may assume $b_1 = \dots = b_n = 1$, and the decomposition is then unique.

Proof. First assume that b lies in B_n^+, and consider the Hurwitz (total) action of B_n^+ on B_∞^n, and put $(b_1', \dots, b_n') = (1, \dots, 1) \bullet b$. By construction, the braids $b_1', \dots, b_n'$ are special. Then we apply (4.3). Uniqueness comes from the fact that special braids

are self-colouring, in the sense that, if b is special, then we have $(1,\dots,1) \bullet b = (b,1,\dots,1)$, as is shown in Figure 13.

For the general case, we write $b = b_0^{-1}b_0'$ with b_0, b_0' in B_n^+. □

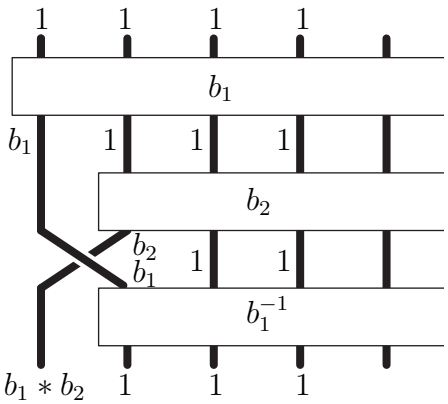


FIGURE 13. Special braids are self-colouring: the property is true for 1, and the diagram above shows that it is true for $b_1 * b_2$ whenever it is for b_1 and b_2.

As an application of diagram colourings appealing to braid twisted conjugacy, we shall come back to the braid ordering of Proposition 4.2, and give a more intrinsic characterization of this ordering not involving the free LD-system **D**. Let us mention that *many* constructions of this ordering are possible, see [23].

Proposition 4.7 ([14])**.** *The relation "$b_1^{-1}b_2$ is σ-positive" is a linear ordering on B_n that is compatible with multiplication on the left and that coincides with the ordering of Proposition 4.2.*

As the shift endomorphism ∂ is injective, it is easy to see that proving Proposition 4.7 reduces to proving the following two results:

- Property ***A***: *A σ_1-positive braid is not trivial;*
- Property ***C***: *Every braid is σ_1-positive, or σ_1-negative, or σ_1-free,*
  where b being σ_1-negative means that b^{-1} is σ_1-positive, and b being σ_1-free means that b belongs to the image of ∂, hence admits an expression where neither σ_1 nor σ_1^{-1} occurs.

We already saw how to prove Property ***A*** using **D**-colourings in the previous section, and we shall see now how to establish Property ***C*** using B_∞-colourings. The latter almost directly follows from the decomposition of an arbitrary braid in terms of special braids given in (4.4). Indeed, we have to show that every braid can be expressed without using at least one of σ_1, σ_1^{-1}. Now, in (4.4), the only factors that do not lie in the image of ∂ are the central factors b_1^{-1} and b_1'. So the missing part for deducing property ***C*** is the following result:

Lemma 4.8. *If b, b' are special braids, then the braid $b^{-1}b'$ is either σ_1-positive, or σ_1-negative, or equal to* 1*.*

Proof. In any LD-system S with one generator, any two elements are comparable with respect to $\sqsubset$: indeed S is a projection of the free LD-system **D**, so the result

for **D**, which is what was called the Comparison Property above, implies the result for S. Applying this to the LD-system $(B_\infty^{sp}, *)$, we deduce that, if b, b' are special braids, then at least one of $b \sqsubset b'$, $b = b'$, $b' \sqsubset b$ holds. Now, by definition of the relation $\sqsubset$ and of the specific operation $*$ we consider, $b \sqsubset b'$ implies that $b^{-1}b'$ is σ_1-positive: the basic case is $b' = b * z$, in which case we obtain $b^{-1}b' = \partial z \cdot \sigma_1 \cdot \partial b^{-1}$, an explicitly σ_1-positive expression. □

Using Lemma 4.8, we deduce Property ***C***, which we saw was the only missing piece in a proof of Proposition 4.7.

Let us conclude with an application to braid groups representations. Once we know that every non-trivial braid is either σ-positive or σ-negative, an obvious criterion for proving that a certain representation ρ of B_n is faithful is to prove that the image under ρ of a σ-positive braid is not trivial. Provided ρ is sufficiently compatible with the shift endomorphism ∂, it is even sufficient to prove that the image of a σ_1-positive braid is not trivial. This applies for instance to Artin's representation of B_n in $\mathrm{Aut}(F_n)$: D. Larue observed that the automorphism associated with a σ_1-positive braid must map x_1 to some reduced word ending in x_1^{-1} [47], which gives a quite straightforward proof for the injectivity of this representation—see also [52, 13] for further examples. On the other hand, very little is known about the possible application of the method to linear representations like the Burau, the Jones or the Lawrence–Krammer representations.

5. More non-classical LD-systems and open questions

We saw in the previous section how colouring braid diagrams using non-classical LD-systems leads to non-trivial results about braids. In this last section, we briefly mention some open questions related to the current approach, as well as some further examples of non-classical LD-systems with a potential interest in braid or link theory.

5.1. **The braid ordering.** We have seen how to construct the braid ordering using the Hurwitz action of braids on the power of a free LD-system. Many alternative approaches are now known. Some of them are more combinatorial in spirit, others are completely geometric and appeal to the realization of B_n as the mapping class group of a punctured disk. We refer to [23] for an introduction to these various approaches and a list of open questions.

Here we shall only mention some questions related to our current approach. One of the main and most intriguing property of the braid ordering is the result, proved by R. Laver, that, for each n, the restriction of the order to B_n^+ is a well-ordering, whose ordinal type was subsequently shown by S. Burckel to be $\omega^{\omega^{n-2}}$. This theorem is closely connected with

Proposition 5.1 (Property ***S***). *For every braid b, one has $b\sigma_i > b$ for each i.*

As the braid ordering is *not* compatible with multiplication on the right in general, Property ***S*** is not obvious. Actually, there exist several proofs, based on combinatorial results about free LD-systems (Laver), or on a very tricky analysis of positive braids in terms of finite trees (Burckel), or on an interpretation in hyperbolic geometry (Short and Wiest), but, frustratingly, the following problem remains open:

Question 5.2. *Is there a natural proof of Property **S** based on diagram colourings?*

5.2. **Handle reduction.** One of the main applications of the braid ordering is an efficient algorithm for solving the isotopy problem of braids, *i.e.*, for recognizing whether a braid word w represents the trivial braid. The method is as follows.

Definition. A braid word is defined to be a σ_i *-handle* if it has the form $\sigma_i^e w \sigma_i^{-e}$ where e is ± 1 and w contains no letter $\sigma_j^{\pm 1}$ with $j \leqslant i$ and, in addition, w does not contain both σ_{i+1} and σ_{i+1}^{-1}. Then *reducing* a handle $\sigma_i^e w \sigma_i^{-e}$ is defined to mean deleting the final $\sigma_i^{\pm e}$ and substituting each letter σ_{i+1}^d with $\sigma_{i+1}^{-e}\sigma_i^d\sigma_{i+1}^e$.

Observe that reducing a handle of the form $\sigma_i^e\sigma_i^{-e}$ means just deleting it: handle reduction is an extension of the usual free group word reduction.

Proposition 5.3 ([17])**.** *Let w be an arbitrary braid word. Then starting from w and iteratively reducing handles (in any order) always ends up in a finite number of steps in a word w' containing no handle, and w represents the trivial braid if and only if w' is the empty word.*

The method is extremely efficient in practice: typically, braid words with 10,000 crossings and any number of strands are reduced in 1 sec. on a microcomputer. This efficiency, together with the simplicity of implementation, makes handle reduction relevant for cryptographical applications. However, it should be noted that, contrary to other solutions to the isotopy problem based on Garside's theory, handle reduction is *a priori* connected with no normal form: the final word w' obtained by reducing handles in w depends on the chosen reductions. This fact does not dismiss handle reduction in possible applications, but it requires that the algorithms are designed accordingly [22].

The convergence of handle reduction directly follows from the existence of the braid ordering, but, so far, the only proved upper bound for the number of reduction steps when one starts with a length ℓ braid word is exponential in ℓ, while experiments suggest a quadratic bound in the worst case. A puzzling open problem is:

Question 5.4. *What is the complexity of handle reduction?*

5.3. **The operation $*$ on B_∞.** The colouring approach naturally leads to the notion of a special braid: we have seen that the latter are those braids that produce themselves when one uses $(B_\infty, *)$ to colour the strands of the braid diagrams, *cf.* Figure 13.

As the shift endomorphism ∂ appears in the definition of the operation $*$, the latter is defined in B_∞ only: it makes no sense to restrict $*$ to B_n. Similarly, special braids as defined in B_∞. The decompositions of Proposition 4.6 live in B_∞: when we consider a braid b in B_n^+, its (unique) expression as a shifted product of n special braids involves in general special braids lying in B_N for some very large N (which can be effectively computed), typically exponential in n. However, it would be interesting to precisely control the width of special braids. This leads to the following open problem:

Question 5.5. *How many special braids lie in B_n?*

Experiments suggest that 2^n could be an upper bound.

More generally, many open problems involve the operation $*$ on braids, cf. [18]. Here we would like to draw the attention on the possibility of using $*$ as an alternative to conjugacy in braid groups. Starting with [41]—see also [2, 22, 43, 44, 45, 46]—several cryptosystems based on braid groups have been proposed in the recent years. The supposedly difficult problem on which these systems rely is the conjugacy problem, *i.e.*, the problem of recognizing whether two braids are conjugate, or more exactly in the considered case, the conjugator search problem, which is the variant in which one starts with conjugate braids and the unknown element is a braid witnessing for conjugacy. A potential weakness of these systems is that no lower complexity bound is proved for the braid conjugacy problems. Now, the operation $*$ on braids, *i.e.*, $(x, y) \mapsto x(\partial y)\sigma_1(\partial x)^{-1}$, appears as a sort of twisted version of standard conjugacy operation $(x, y) \mapsto xyx^{-1}$.

Question 5.6. *Can one replace the standard conjugacy operation with its twisted version involving $*$ in the design of braid-based cryptosystems?*

So far no lower complexity bound for any problem involving twisted conjugacy is known, but the very little we know suggest that the latter operation is at least as difficult—and presumably much more difficult—as its standard counterpart. It is not clear how to solve the following basic problem (which is natural although twisted-conjugacy is not an equivalence relation):

Question 5.7. *Is there an algorithm deciding whether two braids b, b' are twisted-conjugate, i.e., there exists x satisfying $b' = x * b$?*

Even the following more particular problem seems to be open: it is easy to check that the function that maps every braid b to $b * 1$, *i.e.*, to $b\sigma_1(\partial b)^{-1}$, is injective.

Question 5.8. *Is there a constructive way to recover b from $b * 1$?*

One point that makes the above questions possibly difficult is that Garside's theory, which proves to be very efficient in many situations, seems to be of very little use here: as far as braid ordering and the operation $*$ are concerned, no connection with positive braids and normal forms seems to exist.

5.4. **The Laver tables.** We mentioned applications of diagram colourings involving two non-standard LD-systems, namely the free LD-system $\mathbf{D}$ and the system $(B_\infty, *)$. This naturally leads to the problem of using further types of LD-systems:

Question 5.9. *Can one use arbitrary LD-systems, in particular those that are not left cancellative, to colour braid (or link) diagrams?*

If an LD-system $(S, *)$ is not left cancellative, then it is not clear how to extend the Hurwitz action itself, but diagram colourings are still well-defined, and we could think of other ways to use them, for instance by counting the number of different colourings of a given diagram as in state-sum invariant.

There exist good candidates for such an approach, namely finite LD-systems. There happens to exist a very interesting family of finite LD-systems called the Laver tables. These are easily constructed as follows. Let us try to construct a left self-distributive operation on the set $\{1, 2, \dots, N\}$ starting with $p * 1 = p + 1$ for $1 \leqslant p < N$ and $N * 1 = 1$. In other words, we try to build a self-distributive table

so that the first column enumerated from top to bottom is $2, 3, \dots, N, 1$. It is easy to see that there exists at most one way to complete the table, by first completing the last raw, then the forelast raw, etc. It is also not very hard to prove that the table so obtained is actually self-distributive if and only if the size N of the table is a power of 2. We shall denote by A_n the table of size 2^n, and call it the nth *Laver table*, after Richard Laver who discovered them at the end of the 1980's in connection with deep work in set theory. The reader might will to check that the first four Laver tables are as indicated in Table 1.

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

TABLE 1. The first Laver tables: the first column is a cyclic shift, and then there is one way only to fill the table so as to force self-distributivity.

The Laver tables are fascinating objects which so far remain rather mysterious. By construction, 1 is a generator of A_n, and the sequence of all A_n's is an inverse system: projecting A_{n+1} mod 2^n yields A_n. The limit of that inverse system is conjectured to be the free LD-system on one generator, but the only known proof of this result involves a so-called large cardinal axiom in set theory, thus an unprovable logical axiom.

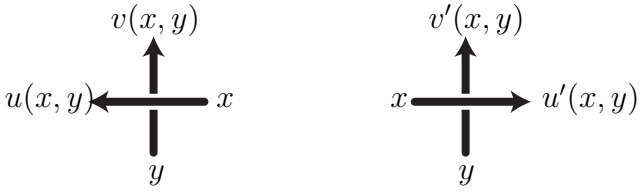
We would like to raise:

Question 5.10. *Can one use the Laver tables to colour braid or link diagrams?*

The Laver tables play a special role among finite LD-systems: a theorem by A. Drápal shows that every finite LD-system with one generator admits a canonical construction from Laver tables [26]. The latter can be thought of as similar to cyclic groups with respect to finite commutative groups—but with a much higher combinatorial complexity. These tables capture in some sense the whole complexity of LD-systems, and one might expect that, if they can be used, then they have the intrinsic power to lead to really deep results.

5.5. **More actions.** Another direction is to use standard sets of colours, for instance free groups, for colouring braid diagrams, but to use more complicated rules for changes of colours than those of Figure 2, in particular allowing both strands to change colours at crossings. Then the constraints are relaxed, and self-distributivity is to be replaced with more general identities involving two binary operations. In

the case of a free group, this means considering crossing rules of the form



where $u(x,y)$, $v(x,y)$, $u'(x,y)$, $v'(x,y)$ are (reduced) words in the variables x, y and their inverses. For instance, the Hurwitz action corresponds to the choice $u(x,y) = u'(x,y) = x$, $v(x,y) = xyx^{-1}$, and $v'(x,y) = x^{-1}yx$.

Question 5.11. *Can one list all possible choices for $u, \dots, v'$ that make the rules compatible with braid relations?*

The question was addressed by Wada in [53]. Several variations of the Hurwitz action are possible, but at least one example of a different type exists, namely $u(x,y) = y^{-1}x^{-1}y$, $v(x,y) = x^2y$, $u'(x,y) = yx^{-1}y^{-1}$, $v'(x,y) = yx^2$. The complete list is unknown, but some results about the existing solutions and the induced representations of B_n into $\mathrm{Aut}(F_n)$ can be found in [13].

5.6. **More diagrams.** Let us conclude with one more possible extension, in a very different direction, namely Richard Thompson's groups. These remarkable groups have received great interest in the recent years [9]. They appear in several different frameworks, from computer science to geometry and topology. In particular, they can be realized as subgroups of mapping class groups—therefore as groups of automorphisms of a free group—and they are not so far from Artin's braid groups. For our current approach, the point is that the elements of Thompson's groups F and V are naturally associated with pairs of diagrams that are finite binary trees, which we can see as cousins of braid diagrams in which the strands merge instead of crossing.

In several recent works [6, 21, 33, 35], braided versions of the Thompson groups are been introduced. These new groups include both Artin's braid group B_∞ and Thompson's group F. Their elements are associated with diagrams of which Figure 14 givs an example. Diagram colouring techniques prove to be relevant for investigating such groups. In particular, it is proved in [21] that both the braid ordering and the braid twisted conjugacy operation $*$ extend to the braided Thompson group BV. To mention one precise open problem in the spirit of the current paper, we ask:

Question 5.12. *Can one realize free LD-systems of arbitrary finite rank inside the group BV?*

It is known that special braids make a realization of the free LD-system $\mathbf{D}$ inside Artin's braid group B_∞. So far, it is unknown whether B_∞ is large enough to similarly include a copy of the free LD-system on two generators, say. We conjecture a negative answer, but we also conjecture that the answer becomes positive when B_∞ is replaced with its natural extension BV.

FIGURE 14. Diagram for a typical element of the braided Thompson group BV: the central part is an n strand braid diagram, the top and the bottom are binary trees with n leaves.

The above question may appear quite technical. Let us insist that the interest of the braided Thompson group seems to go far beyond such a question. In particular, as BV is equipped with a left cancellative self-distributive operation, we may ask:

Question 5.13. *Can one use BV-colourings to establish new results about braids and links?*

As in the case of the Laver tables, the group BV seems to be complicated enough to make non-trivial applications plausible.

REFERENCES

[1] S.I. Adjan, *Fragments of the word Delta in a braid group*, Mat. Zam. Acad. Sci. SSSR **36-1** (1984) 25–34; translated Math. Notes of the Acad. Sci. USSR; 36-1 (1984) 505–510.

[2] I. Anshel, M. Anshel, & D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Research Letters **6** (1999) 287–291.

[3] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies 82, Princeton Univ. Press (1975).

[4] J. Birman, K.H. Ko & S.J. Lee, *A new approach to the word problem in the braid groups*, Advances in Math. **139-2** (1998) 322-353.

[5] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemporary Maths AMS **78** (1988) 45–117.

[6] M. Brin, *The algebraic structure of the braided Thompson group*, Preprint (2003).

[7] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120-1** (1997) 1–17.

[8] G. Burde & H. Zieschang, *Knots*, de Gruyter, Berlin (1985).

[9] J.W. Cannon, W.J. Floyd, & W.R. Parry, *Introductory notes on Richard Thompson's groups*, Ens. Math. **42** (1996) 215–257.

[10] J.S. Carter, D. Jelsovsky, S. Kamada, L. Langford, M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, arXiv: math.GT/9903135 (1999).

[11] J.S. Carter, D. Jelsovsky, S. Kamada, M. Saito, *Computation of quandle cocycle invariants of knotted curves and surfaces*, Adv. Math. **157** (2001) 36–94.

[12] J.S. Carter, S. Kamada, & M. Saito, *Geometric interpretations of quandle homology*, J. Knot Th. Ramific. **10-3** (2001) 345–386.

[13] J. Crisp & L. Paris, *Representations of the braid group by automorphisms of groups, invariants of links, and Garside groups*, Pac. J. Maths, to appear.

[14] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345-1** (1994) 115–151.

[15] P. Dehornoy, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.
[16] P. Dehornoy, *From large cardinals to braids via distributive algebra*, J. Knot Theory & Ramifications **4-1** (1995) 33–79.
[17] P. Dehornoy, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.
[18] P. Dehornoy, *Strange questions about braids*, J. Knot Th. and its Ramifications **8-5** (1999) 589–620.
[19] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser, (2000).
[20] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.
[21] P. Dehornoy, *Geometric presentations of Thompson's groups and related groups*, preprint.
[22] P. Dehornoy, *Braid-based cryptography*, Contemp. Math., to appear.
[23] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses vol. 14, Soc. Math. France (2002).
[24] D. Devine, *Alexander invariants of links and the fundamental rack*, PhD Univ. Sussex (G. B.), 1992.
[25] F.M. Dionísio & P. Lopez, *Quandles at finite temperature II*, J. Knot Th. Ramific. **12-8** (2003) 1041–1092.
[26] A. Drápal, *Finite left distributive groupoids with one generator*, Int. J. for Algebra Computation **7-6** (1997) 723–748.
[27] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.
[28] D. Epstein & *al.*, *Word Processing in Groups*, Jones & Barlett Publ. (1992).
[29] R. Fenn, M.T. Greene, D. Rolfsen, C. Rourke & B. Wiest, *Ordering the braid groups*, Pacific J. of Math., to appear.
[30] R. Fenn & C. P. Rourke, *Racks and links in codimension 2*, J. of Knot Th. Ramific. **1-4** (1992) 343–406;
[31] R. Fenn, C. P. Rourke, & B. Sanderson, *An introduction to species and the rack space*, M.E. Bozhuyu (ed.), Topics in Knot Theory, Kluwer Acad., pp 33–55 (1993).
[32] R. Fenn, C. P. Rourke, & B. Sanderson, *James bundles and applications*, Preprint.
[33] L. Funar & C. Kapoudjian, *On a universal mapping class group in genus zero*, GAFA; to appear.
[34] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.
[35] P. Greenberg & V. Sergiescu, *An acyclic extension of the braid group*, Comment. Mat. Helvetici **66** (1991) 109–138.
[36] A. Inoue, *Homomorphisms of knot quandles to Alexander quandles*, J. Knot Th. Ramific. **10-6** (2001) 813–822.
[37] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. of Pure and Appl. Algebra **23** (1982) 37–65;
[38] C. Kapoudjian & V. Sergiescu, *An extension of the Burau representation to a mapping class group associated to Thompson's group T*, Contemp. Math.; to appear.
[39] C. Kassel, *Quantum groups*, Springer Verlag (1995).
[40] L. Kauffman, *On knots*, Annals of Math. Studies 115, Princeton Univ. Press (1987).
[41] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J.S. Kang, & C. Park, *New public-key cryptosystem using braid groups*, Crypto 2000; Springer Lect. Notes in Comput. Sci., 1880 (2000) 166–184.
[42] D.M. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994) 104–112.
[43] S.J. Lee & E.K. Lee, *Overview of the cryptosystems using braid groups*, ASCOF 2001, pp. 41–50; http://www.kisa.or.kr/technology/sub1/data/ASCoF2001.pdf
[44] S.J. Lee & E.K. Lee, *Potential weakness of the commutator key agreement protocol based on braid groups*, Eurocrypt 2002, Springer Lect. Notes in Comput. Sci. 2332 (2002) 14–28.
[45] E.K. Lee, S.J. Lee, S.G. Hahn, *Pseudorandomness from braid groups*, Crypto 2001; Springer Lect. Notes in Comput. Sci., 2139 (2001) 486–502.
[46] E. Lee & J.H. Park, *Cryptanalysis of the public-key encryption based on braid groups*, Eurocrypt 2003, to appear.

[47] D.M. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994) 104–112.
[48] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.
[49] S.V. Matveev, *Distributive groupoids in knot theory*, Math. Sbornik **119, 1-2** (1982) 73–83.
[50] V.V. Prasolov & A.B. Sossinsky, *Knots, links, braids, and 3-manifolds (in Russian)*, MCCME (1997).
[51] H. Short & B. Wiest, *Orderings of mapping class groups after Thurston*, Ens. Math. **46** (2000) 279–312.
[52] W. Shpilrain, *Representing braids by automorphisms*, Intern. J. of Algebra & Comput; 11-6; 2001; 773–777.
[53] M. Wada, *Groups invariants of links*, Topology **31-2** (1992) 399–406.
[54] D.N. Yetter, *Quandles and monodromy*, J. Knot Th. Ramific. **12-4** (2003) 523–543.

Laboratoire de Mathématiques Nicolas Oresme UMR 6139, Université de Caen, 14032 Caen, France
E-mail address: dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/∼dehornoy