



**HAL**  
open science

## THE BRAID SHELF

Patrick Dehornoy

► **To cite this version:**

| Patrick Dehornoy. THE BRAID SHELF. 2018. hal-01649705v2

**HAL Id: hal-01649705**

**<https://hal.science/hal-01649705v2>**

Preprint submitted on 7 Feb 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# THE BRAID SHELF

PATRICK DEHORNOY

ABSTRACT. The braids of  $B_\infty$  can be equipped with a selfdistributive operation  $\triangleright$  enjoying a number of deep properties. This text is a survey of known properties and open questions involving this structure, its quotients, and its extensions.

## 1. INTRODUCTION

According to an approach that can be traced back to Joyce [39], Matveev [51], and Brieskorn [4], selfdistributivity (SD) is an algebraic distillation of Reidemeister's move of type III and, therefore, it is not surprising that structures involving SD operations often appear in low-dimensional topology, typically when one wishes to attach isotopy-invariant colourings to the strands of a diagram. In this approach, which, for instance, leads to the fundamental quandle of a knot and to a number of nontrivial invariants [10, 11, 9], SD structures are external tools outside the world of topological objects. However, there also exists a disjoint approach, in which the topological objects themselves are equipped with an SD operation: this happens for the braids of  $B_\infty$ , and for the elements of various related structures. As can be expected, combining the internal and external aspects of SD is what leads to interesting results. Our aim is to explore this a priori strange situation.

Most of the results presented below already appeared in literature (with the exception of some in Section 4), in particular in [27], where the connection between the SD operation on braids and the standard braid ordering is explained. However, a number of side results are disseminated in various papers and not easily accessible. Moreover, SD operations mainly occur as auxiliary tools, and there existed no comprehensive presentation specifically concentrating on the SD operations themselves. These notes aim at filling this gap. A particular orientation toward open questions has been given, appealing for further research.

The text is organized in four sections after this introduction. In Section 2, we recall the existence of a selfdistributive operation  $\triangleright$  on the family  $B_\infty$  of braids involving an unlimited number of strands, and its basic properties. In Section 3, we concentrate on special braids, which are those braids obtained from the unit braid using the SD operation  $\triangleright$ . Special braids form a free left-shelf, and give rise to canonical decompositions for arbitrary braids. Section 4 is devoted to a few observations about SD operations in quotients of braid groups, typically in permutation groups. Finally, we discuss in Section 5 three examples of SD operations living in extensions of the group  $B_\infty$ , and leading to further open questions.

---

1991 *Mathematics Subject Classification.* 20F36, 20N02, 57M25, 57M60.

*Key words and phrases.* selfdistributivity, shelf, braid, special braid, symmetric group, Laver table, charged braid, parenthesized braid.

## 2. A SELFDISTRIBUTIVE OPERATION ON BRAIDS

The central object of interest in these notes is a certain binary operation  $\triangleright$  defined on the braid group  $B_\infty$ . After recalling the standard terminology for selfdistributive structures, we introduce the operation  $\triangleright$  in Subsection 2.1. In Subsection 2.2, we briefly recall its origin as a projection from a certain geometry group of selfdistributivity. Next, we state a few typical algebraic properties of  $\triangleright$  (Subsection 2.3), and we explain how it can be used to color the strands of braid diagrams (Subsection 2.4).

**2.1. A self-distributive operation on  $B_\infty$ .** The selfdistributivity law comes in two versions:

$$\begin{aligned} \text{(LD)} \quad & \textit{left selfdistributivity:} & x \triangleright (y \triangleright z) &= (x \triangleright y) \triangleright (x \triangleright z), \\ \text{(RD)} \quad & \textit{right selfdistributivity:} & (x \triangleleft y) \triangleleft z &= (x \triangleleft z) \triangleleft (y \triangleleft z). \end{aligned}$$

It is often more convenient in topology to use the right version (and, accordingly, the symbol  $\triangleleft$ ), but, here, in order both to be coherent with the existing literature and because of some specific features that are not invariant under symmetry (see Remark 2.11), we shall use the left version, and the symbol  $\triangleright$ . We use the prefix “left” everywhere to avoid ambiguity.

**Definition 2.1 (selfdistributive structures).** (i) A *left-shelf* is a structure  $(S, \triangleright)$ , where  $\triangleright$  is a binary operation on  $S$  that obeys the law LD.

(ii) A *left-spindle* is a left-shelf  $(S, \triangleright)$ , in which  $x \triangleright x = x$  always holds.

(iii) A *left-rack* is a left-shelf  $(S, \triangleright)$ , in which left translations are bijective, that is, for every  $a$  in  $S$ , the map  $L_a : y \mapsto a \triangleright y$  is a bijection from  $S$  to itself.

(iv) A *left-quandle* is a left-rack that is also a left-spindle.

Lots of examples are known. We refer to [26] for a general picture of the structures known so far, and, in particular, for a survey of results about (left) shelves that are not racks or spindles.

In a non-associative context, paying attention to brackets is necessary, and, for  $a$  in a set equipped with a binary operation  $\triangleright$ , we write  $a^{[m]}$  and  $a_{[m]}$  for the  $m$ th *right* and *left* powers of  $a$  inductively defined by

$$(2.1) \quad a^{[1]} := a_{[1]} := a, \quad a^{[m+1]} := a \triangleright a^{[m]}, \quad a_{[m+1]} := a_{[m]} \triangleright a.$$

Let us now turn to the braid operation. The braid group  $B_n$  is the group of isotopy classes of  $n$ -strand braid diagrams, as well as the mapping class group of an  $n$ -punctured disk—see for instance [2] or [27]. It admits the presentation

$$(2.2) \quad \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{for } |i - j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{for } |i - j| = 1 \end{array} \right\rangle.$$

For every  $n$ , the inclusion of  $\{\sigma_1, \dots, \sigma_{n-1}\}$  into  $\{\sigma_1, \dots, \sigma_n\}$  extends into an embedding  $i_{n,n+1}$  of  $B_n$  into  $B_{n+1}$ . The group  $B_\infty$  is the limit of the inductive system so obtained, hence simply the union of all  $B_n$ s when  $i_{n,n+1}$  is identified with identity. The group  $B_\infty$  admits the presentation analogous to (2.2) with an infinite sequence of generators  $\sigma_1, \sigma_2, \dots$

From the presentation, it is clear that mapping  $\sigma_i$  to  $\sigma_{i+1}$  for every  $i$  defines an endomorphism  $\text{sh}$  of  $B_\infty$ , hereafter called the *shift* endomorphism. Note that  $\text{sh}$  is not surjective:  $\sigma_1$  does not lie in  $\text{Im}(\text{sh})$ .

**Definition 2.2 (shifted conjugation).** For  $\beta_1, \beta_2$  in  $B_\infty$ , we put

$$(2.3) \quad \beta_1 \triangleright \beta_2 := \beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}.$$

The braid  $\beta_1 \triangleright \beta_2$  is a sort of conjugate of  $\beta_2$  under  $\beta_1$ , but with shifts and an additional factor  $\sigma_1$  added, see Fig. 1. The reader can check the values

$$1 \triangleright 1 = \sigma_1, \quad 1 \triangleright \sigma_1 = \sigma_2 \sigma_1, \quad \sigma_1 \triangleright 1 = \sigma_1^2 \sigma_2^{-1}, \quad \dots$$

and, more generally,  $1^{[m]} = \sigma_{m-1} \cdots \sigma_2 \sigma_1$  for every  $m \geq 1$ . The above equalities show that  $\triangleright$  is neither commutative nor idempotent. Note that, because of the shift operator in (2.3), the operation  $\triangleright$  is defined on  $B_\infty$  only, and it induces no well-defined operation on  $B_n$  for any finite  $n$ .

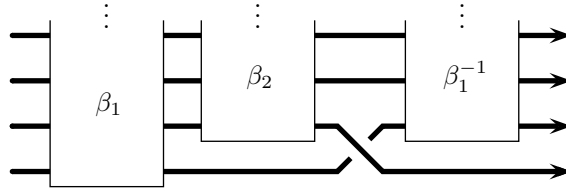


FIGURE 1. Braid diagram for  $\beta_1 \triangleright \beta_2$ : a sort of conjugation of  $\beta_2$  under  $\beta_1$ , with shifts and one  $\sigma_1$  added.

Our interest in the operation  $\triangleright$  on  $B_\infty$  stems from

**Proposition 2.3 (braid shelf).** *The operation of (2.3) obeys the law LD, that is,  $(B_\infty, \triangleright)$  is a left-shelf. It is neither a left-spindle, nor a left-rack.*

*Proof.* A simple verification. Expanding the definition, we find for all  $\beta_1, \beta_2, \beta_3$

$$\begin{aligned} \beta_1 \triangleright (\beta_2 \triangleright \beta_3) &= \beta_1 \cdot \text{sh}(\beta_2) \cdot \text{sh}^2(\beta_3) \cdot \sigma_2 \cdot \text{sh}^2(\beta_2)^{-1} \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}, \\ (\beta_1 \triangleright \beta_2) \triangleright (\beta_1 \triangleright \beta_3) &= (\beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}) \triangleright (\beta_1 \cdot \text{sh}(\beta_3) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}) \\ &= (\beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}) \cdot \text{sh}(\beta_1 \cdot \text{sh}(\beta_3) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1}) \\ &\quad \cdot \sigma_1 \cdot \text{sh}(\beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1})^{-1} \\ &= \beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1} \cdot \text{sh}(\beta_1) \cdot \text{sh}^2(\beta_3) \cdot \sigma_2 \cdot \text{sh}^2(\beta_1)^{-1} \\ &\quad \cdot \sigma_1 \cdot \text{sh}^2(\beta_1) \cdot \sigma_2^{-1} \cdot \text{sh}^2(\beta_2)^{-1} \cdot \text{sh}(\beta_1)^{-1} \\ &= \beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}^2(\beta_3) \cdot \sigma_2 \cdot \text{sh}^2(\beta_1)^{-1} \\ &\quad \cdot \sigma_1 \cdot \text{sh}^2(\beta_1) \cdot \sigma_2^{-1} \cdot \text{sh}^2(\beta_2)^{-1} \cdot \text{sh}(\beta_1)^{-1}. \end{aligned}$$

As  $\sigma_1$  commutes with every braid in  $\text{Im}(\text{sh}^2)$  and  $\sigma_1 \sigma_2 \sigma_1 \sigma_2^{-1} = \sigma_2 \sigma_1$  holds, we find  $\beta_1 \triangleright (\beta_2 \triangleright \beta_3) = (\beta_1 \triangleright \beta_2) \triangleright (\beta_1 \triangleright \beta_3) = \beta_1 \cdot \text{sh}(\beta_2) \cdot \text{sh}^2(\beta_3) \cdot \sigma_2 \sigma_1 \cdot \text{sh}^2(\beta_2)^{-1} \cdot \text{sh}(\beta_1)^{-1}$ , and the law LD is satisfied.

We already noted the equality  $1 \triangleright 1 = \sigma_1$ , which shows that  $(B_\infty, \triangleright)$  is not a left spindle. Observe that, more generally, we *always* have

$$(2.4) \quad \beta \neq \beta \triangleright \beta,$$

as an equality would expand into  $1 = \text{sh}(\beta) \sigma_1 \text{sh}(\beta)^{-1}$ , clearly impossible.

On the other hand, we have  $1 \triangleright \beta = \text{sh}(\beta) \sigma_1$ . As  $\sigma_1$  does not belong to the image of  $\text{sh}$ , it is impossible to have  $1 \triangleright \beta = 1$ , so the left translation associated with 1 is not bijective, and  $(B_\infty, \triangleright)$  is not a left-rack.  $\square$

**Remark 2.4.** Of course, we can obtain a right selfdistributive operation  $\triangleleft$  by considering the opposite operation, namely

$$(2.5) \quad \beta_1 \triangleleft \beta_2 := \text{sh}(\beta_2)^{-1} \cdot \sigma_1 \cdot \text{sh}(\beta_1) \cdot \beta_2.$$

**2.2. Where does the braid shelf come from?** The braid operation  $\triangleright$  was introduced in Def. 2.2 without any explanation, and Formula (2.3) may look odd. We refer to [18] for a complete explanation, but a few words here could be welcome.

One can naturally associate with every algebraic law, or family of algebraic laws, a certain “geometry monoid” that, in some sense, captures the specific properties of the involved laws. When the law is the associativity law  $x(yz) = (xy)z$ , the geometry monoid is essentially Richard Thompson’s group  $F$  [8, 20] and, similarly, when both associativity and commutativity are considered, the geometry monoid is Thompson’s group  $V$ .

In the case of the selfdistributivity law LD, the geometry monoid turns out to be closely connected with a certain group  $G_{\text{LD}}$  generated by an infinite family of elements  $\text{LD}_\alpha$  indexed by finite sequences of 0s and 1s and subject to an explicit list of relations  $\text{Rel}_{\text{LD}}$ . A basic property of LD says that, if a left-shelf  $(S, \triangleright)$  is generated by a single element  $g$ , then, for every  $a$  in  $S$ , the equality

$$(2.6) \quad g^{[n+1]} = a \triangleright g^{[n]}$$

holds for  $n$  large enough: the result is trivial when  $a$  is  $g$  and the inductive argument

$$(2.7) \quad g^{[n+1]} = a \triangleright g^{[n]} = a \triangleright (b \triangleright g^{[n-1]}) = (a \triangleright b) \triangleright (a \triangleright g^{[n-1]}) = (a \triangleright b) \triangleright g^{[n]}$$

gives (2.6) for  $a \triangleright b$  starting from (2.6) for  $a$  and for  $b$ .

By construction, every formal consequence of the law LD is encoded in an element of the group  $G_{\text{LD}}$ . From there, the four equalities in (2.7) are encoded in a product of four elements in  $G_{\text{LD}}$ , and they correspond to defining on  $G_{\text{LD}}$  a binary operation  $*$  by

$$(2.8) \quad f * g := f \cdot \text{sh}_1(g) \cdot \text{LD}_\emptyset \cdot \text{sh}_1(f)^{-1},$$

where  $\text{sh}_1$  is the endomorphism that maps each element  $\text{LD}_\alpha$  to  $\text{LD}_{1\alpha}$  (appending an initial 1 in the finite sequence  $\alpha$ ). The operation  $*$  on  $G_{\text{LD}}$  is not selfdistributive, but, due to the connection of  $*$  with (2.6), the “LD-defect” of  $*$ , namely the quotient

$$(f * (g * h))^{-1} \cdot ((f * g) * (f * h))$$

must lie in the image of the endomorphism  $\text{sh}_0$  that maps  $\text{LD}_\alpha$  to  $\text{LD}_{0\alpha}$  for each  $\alpha$ . As a consequence, when the subgroup  $\text{sh}_0(G_{\text{LD}})$  is collapsed, the operation  $*$  on  $G_{\text{LD}}$  must induce on the quotient an operation with no LD-defect, that is, a selfdistributive operation.

It should not be a surprise to hear that the quotient-group  $G_{\text{LD}}/\text{sh}_0(G_{\text{LD}})$  is (isomorphic to) the braid group  $B_\infty$ , and that the operation induced by  $*$  on  $B_\infty$  is the operation  $\triangleright$  of (2.3). More precisely, collapsing  $\text{sh}_0(G_{\text{LD}})$  amounts to collapsing all elements  $\text{LD}_\alpha$  such that  $\alpha$  contains 0. All relations of  $\text{Rel}_{\text{LD}}$  then become trivial, except the following ones:

$$\begin{aligned} \text{LD}_{1^i} \text{LD}_{1^j} \text{LD}_{1^i} &= \text{LD}_{1^j} \text{LD}_{1^i} \text{LD}_{1^j} \text{LD}_{1^i} && \text{for } j = i + 1 \geq 1 \\ \text{LD}_{1^i} \text{LD}_{1^j} &= \text{LD}_{1^j} \text{LD}_{1^i} && \text{for } j \geq i + 2 \geq 2. \end{aligned}$$

Then collapsing  $\text{LD}_{1^i}$  and mapping  $\text{LD}_{1^i}$  to  $\sigma_{i+1}$  defines the expected epimorphism from  $G_{\text{LD}}$  onto  $B_\infty$ . Then (2.8) projects to (2.3), since  $\text{sh}_1$  projects to  $\text{sh}$ , and  $\text{LD}_\emptyset$  is mapped to  $\sigma_1$ . Thus, the braid operation  $\triangleright$  does not come out of the blue.

**2.3. Algebraic properties.** The left-shelf  $(B_\infty, \triangleright)$  is rather different from usual selfdistributive structures such as the various racks and quandles appearing in topology. Here we mention some of its algebraic properties, mainly those involving left translations, which are typical both in their statement and in their proof.

We already noted that  $(B_\infty, \triangleright)$  is not a left-rack, since the left translations  $L_\beta : y \mapsto \beta \triangleright y$  need not be bijections. More is known about such translations [18].

**Proposition 2.5 (left translations).** (i) *For every braid  $\beta$ , the left translation  $L_\beta$  is injective, that is,  $(B_\infty, \triangleright)$  is left cancellative.*

(ii) *A braid  $\gamma$  lies in the image of  $L_\beta$  if, and only if,  $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$  holds.*

*Proof (sketch).* (i) Expanding  $\beta \triangleright \gamma = \beta \triangleright \gamma'$  gives

$$\beta \cdot \text{sh}(\gamma) \cdot \sigma_1 \cdot \text{sh}(\beta)^{-1} = \beta \cdot \text{sh}(\gamma') \cdot \sigma_1 \cdot \text{sh}(\beta)^{-1},$$

whence  $\text{sh}(\gamma) = \text{sh}(\gamma')$  as cancellation is legal in the group  $B_\infty$ . This implies  $\gamma = \gamma'$ , as  $\text{sh}$  is injective. We deduce that  $(B_\infty, \triangleright)$  is left cancellative.

(ii) Assume  $\gamma = \beta \triangleright \beta'$ . The selfdistributivity law implies

$$\beta \triangleright \gamma = \beta \triangleright (\beta \triangleright \beta') = (\beta \triangleright \beta) \triangleright (\beta \triangleright \beta') = \beta^{[2]} \triangleright \gamma,$$

so the condition is necessary. The converse is more tricky. We begin with a general auxiliary result, namely the fact that, for every  $\beta$  in  $B_\infty$ ,

$$(2.9) \quad \beta \text{ belongs to } \text{sh}(B_\infty) \quad \text{if, and only if,} \quad \text{sh}(\beta) \text{ and } \sigma_1 \text{ commute.}$$

Indeed, if  $\beta$  belongs to the image of  $\text{sh}$ , then  $\text{sh}(\beta)$  belongs to the image of  $\text{sh}^2$ , hence it commutes with  $\sigma_1$  in the group  $B_\infty$ . Conversely, for every  $\beta$  in  $B_n$ , the handle trick of Fig. 2 gives

$$\text{sh}(\beta)^{-1} \sigma_1^{-1} \text{sh}(\beta) \sigma_1 = \text{sh}(\beta)^{-1} \sigma_2 \cdots \sigma_n \beta \sigma_n^{-1} \cdots \sigma_2^{-1}.$$

So, if  $\text{sh}(b)$  and  $\sigma_1$  commute, we obtain  $\beta = \sigma_n^{-1} \cdots \sigma_2^{-1} \text{sh}(\beta) \sigma_2 \cdots \sigma_n$ , which belongs to  $\text{sh}(B_\infty)$  explicitly.

Now assume  $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$ . Expanding the expressions gives

$$\beta \text{sh}(\gamma) \sigma_1 \text{sh}(\beta)^{-1} = \beta \text{sh}(\beta) \sigma_1 \text{sh}(\beta)^{-1} \text{sh}(\gamma) \sigma_1 \text{sh}^2(\beta) \sigma_2^{-1} \text{sh}^2(\beta)^{-1} \text{sh}(\beta)^{-1},$$

which can be rewritten as  $\text{sh}(\beta^{-1} \gamma \text{sh}(\beta)) \sigma_1 = \sigma_1 \text{sh}(\beta^{-1} \gamma \text{sh}(\beta)) \sigma_1 \sigma_2^{-1}$ , whence, using the braid relations, into

$$\text{sh}(\beta^{-1} \gamma \text{sh}(\beta) \sigma_1^{-1}) \cdot \sigma_1 = \sigma_1 \cdot \text{sh}(\beta^{-1} \gamma \text{sh}(\beta) \sigma_1^{-1}),$$

which expresses that  $\text{sh}(\beta^{-1} \gamma \text{sh}(\beta) \sigma_1^{-1})$  and  $\sigma_1$  commute. By (2.9), this implies that  $\beta^{-1} \gamma \text{sh}(\beta) \sigma_1^{-1}$  belongs to  $\text{sh}(B_\infty)$ , hence there exists  $\beta'$  satisfying  $\beta^{-1} \gamma \text{sh}(\beta) \sigma_1^{-1} = \text{sh}(\beta')$ . The latter equality is  $\gamma = \beta \triangleright \beta'$ . Hence,  $\gamma$  lies in the image of the left translation  $L_\beta$ .  $\square$

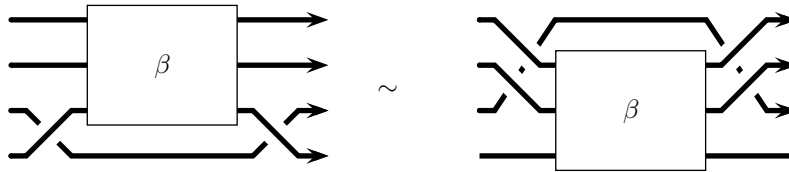


FIGURE 2. The handle trick.

Again about left translations, let us mention another result, which is reminiscent of (2.6), but is quite different in that  $(B_\infty, \triangleright)$  is not monogenerated.

**Proposition 2.6 (absorption).** *A braid  $\beta$  of  $B_\infty$  belongs to  $B_n$  if, and only if, the equality  $\beta \triangleright 1^{[n]} = 1^{[n+1]}$  is satisfied.*

*Proof.* By definition, we find in every case

$$\beta \triangleright 1^{[n]} = \beta \cdot \sigma_n \cdots \sigma_2 \cdot \sigma_1 \cdot \text{sh}(\beta)^{-1} = \beta \cdot 1^{[n+1]} \cdot \text{sh}(\beta)^{-1}.$$

Assume  $\beta \in B_n$ . Then  $\beta$  can be expressed as a product of generators  $\sigma_i^{\pm 1}$  with  $i < n$ . Hence, by the handle trick of Fig. 2,  $\beta \cdot \sigma_n \cdots \sigma_1$  is equal to  $\sigma_n \cdots \sigma_1 \cdot \text{sh}(\beta)$ , implying  $\beta \triangleright 1^{[n]} = 1^{[n+1]}$ .

Conversely, assume  $\beta \notin B_n$ . Let  $m > n$  be minimal such that  $\beta$  belongs to  $B_m$ . By [17], we know that  $\beta$  admits an expression where exactly one of  $\sigma_{m-1}, \sigma_{m-1}^{-1}$  occurs. It follows that  $\text{sh}(\beta)$  has an expression where exactly one of  $\sigma_m, \sigma_m^{-1}$  occurs, and the same holds for  $\beta \cdot 1^{[n+1]} \cdot \text{sh}(\beta)^{-1} \cdot (1^{[n+1]})^{-1}$ , since  $\beta, 1^{[n+1]}$ , and  $(1^{[n+1]})^{-1}$  can be expressed without  $\sigma_m^{\pm 1}$ . Hence, by [13], the latter braid cannot be the unit braid, that is,  $\beta \triangleright 1^{[n]} = 1^{[n+1]}$  fails.  $\square$

The case of right translations  $R_\beta : x \mapsto x \triangleright \beta$  is different, since they need not be injective, but, again, the image can be characterized, this time using conjugacy instead of equality, see [18].

**Remark 2.7.** Because of the similarity with conjugacy, the operation  $\triangleright$  gives rise to potentially difficult algorithmic problems and, therefore, it might be used in cryptographic protocols [23, 40, 49]. This remains marginal so far.

**2.4. The partial action of braids on sequences of braids.** If  $(S, \triangleright)$  is a left-rack and we use  $\bar{\triangleright}$  for the inverse operation so that  $a \triangleright b = c$  is equivalent to  $a \bar{\triangleright} c = b$ , it is well known that the formulas

$$(2.10) \quad (a_1, \dots, a_n) \bullet \sigma_i = (a_1, \dots, a_{i-1}, a_i \triangleright a_{i+1}, a_i, a_{i+2}, \dots, a_n)$$

$$(2.11) \quad (a_1, \dots, a_n) \bullet \sigma_i^{-1} = (a_1, \dots, a_{i-1}, a_{i+1}, a_{i+1} \bar{\triangleright} a_i, a_{i+2}, \dots, a_n)$$

define an action of  $B_n$  on  $S^n$ . This action can be described in terms of strand colorings: for  $\beta$  an  $n$ -strand braid and  $\vec{a}$  a sequence in  $S^n$ , the value of  $\vec{a} \bullet \beta$  is the sequence of output colors obtained when the input colors  $\vec{a}$  are attributed to the initial ends of the strands of  $\beta$  and the colors are propagated according to the rules



When  $(S, \triangleright)$  is only a left-shelf, (2.11) need not make sense. Restricting to positive braids (those that can be expressed without any letter  $\sigma_i^{-1}$ ), and using  $B_n^+$  for the monoid of  $n$ -strand positive braids, we obtain, see Fig. 3:

**Lemma 2.8.** *If  $(S, \triangleright)$  is a left-shelf, (2.10) defines an action of  $B_n^+$  on  $S^n$ .*

However, whenever  $(S, \triangleright)$  is a left cancellative left-shelf, we can extend the action of  $B_n^+$  into a *partial* action of the braid group  $B_n$  on  $S^n$ : using  $\bar{\triangleright}$  for the *partial* operation on  $S$  such that  $a \triangleright b = c$  is equivalent to  $a \bar{\triangleright} c = b$  when such an element  $b$  exists, (2.11) can still be used. The technical result that makes this partial action possibly useful is the following one, whose proof is nontrivial (see [18, Sec. 3.1]):

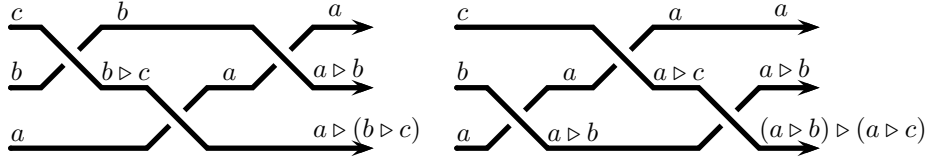


FIGURE 3. Standard translation of Reidemeister III move into the language of selfdistributivity: when colours from a set  $S$  are put on the left ends of the strands and then propagated so that a  $b$ -coloured strand becomes  $a \triangleright b$ -coloured when it overcrosses an  $a$ -coloured arc, then the output colours are invariant under Reidemeister III move if, and only if,  $\triangleright$  obeys the law LD.

**Lemma 2.9 (partial action).** *If  $(S, \triangleright)$  is a left cancellative left-shelf, then (2.10)–(2.11) induce a partial action of braid words such that:*

- (i) *For every finite family of braid words  $w, \dots, w_p$ , there exists a sequence  $\vec{a}$  in  $S^n$  such that  $\vec{a} \cdot w_i$  is defined for every  $i$ ;*
- (ii) *If  $w$  and  $w'$  represent the same braid of  $B_\infty$  and both  $\vec{a} \cdot w$  and  $\vec{a} \cdot w'$  are defined, then they are equal.*

In the above context,  $\vec{a} \cdot \beta$  can be unambiguously defined to be  $\vec{a} \cdot w$  for any word  $w$  such that  $w$  represents  $\beta$  and  $\vec{a} \cdot w$  is defined, if at least one exists.

As  $(B_\infty, \triangleright)$  is a left cancellative left-shelf, it is eligible for the above (total) action of  $B_n^+$ , and partial action of  $B_n$  on  $(B_\infty)^n$ . Such an action is crucial for the developments of Section 3. For the moment, we observe that the external action of  $B_n$  on  $B_\infty^n$  can be connected with an internal multiplication, at the expense of introducing a shifted version of the product.

**Lemma 2.10 (shifted product).** *For  $(\beta_1, \dots, \beta_n)$  in  $B_\infty^n$ , define*

$$(2.12) \quad \prod^{\text{sh}}(\beta_1, \dots, \beta_n) := \beta_1 \cdot \text{sh}(\beta_2) \cdots \text{sh}^{n-1}(\beta_n).$$

*Then, for all  $(\beta_1, \dots, \beta_n)$  in  $B_\infty^n$  and  $\beta$  in  $B_n^+$ , we have*

$$(2.13) \quad \prod^{\text{sh}}((\beta_1, \dots, \beta_n) \bullet \beta) = \prod^{\text{sh}}(\beta_1, \dots, \beta_n) \cdot \beta.$$

*Proof.* For an induction, it suffices to consider the case  $\beta = \sigma_i$ . Next, because the action of  $\sigma_i$  keeps the first  $i - 1$  entries fixed and is a shifting of the action of  $\sigma_1$ , it is even sufficient to consider the case  $\beta = \sigma_1$ . For  $n = 2$ , we find

$$\begin{aligned} \prod^{\text{sh}}((\beta_1, \beta_2) \bullet \sigma_1) &= \prod^{\text{sh}}(\beta_1 \triangleright \beta_2, \beta_1) = (\beta_1 \triangleright \beta_2) \cdot \text{sh}(\beta_1) \\ &= \beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 \cdot \text{sh}(\beta_1)^{-1} \cdot \text{sh}(\beta_1) = \beta_1 \cdot \text{sh}(\beta_2) \cdot \sigma_1 = \prod^{\text{sh}}(\beta_1, \beta_2) \cdot \sigma_1, \end{aligned}$$

Finally, going from  $n = 2$  to  $n \geq 3$  amounts to append some entries  $\text{sh}^{j-1}(\beta_j)$  with  $j \geq 3$  on the right of the shifted products. These entries are invariant under the action of  $\sigma_1$ , and  $\sigma_1$  commutes with all of them, so (2.13) remains valid.  $\square$

**Remark 2.11.** Formula (2.13) is instrumental in subsequent applications of  $\triangleright$ , in particular in the construction of a braid orderings in Section 3.3. This is where using left selfdistributivity LD, and not its right counterpart RD, matters. With the right version, a shifted product starting from the right should be considered: the problem is that one needs to consider braid sequences of arbitrary length, with



no fixed position to start from. It is certainly possible to translate the statements, but at the expense of losing naturalness.

### 3. SPECIAL BRAIDS

The braid shelf  $(B_\infty, \triangleright)$  is a large structure, about which little is known, see for instance Questions 5.1 and 5.4. Here we consider a substructure of the braid shelf, namely the one generated (as a left-shelf) by the unit braid 1. This structure is much better understood, as we shall explain now.

We begin by recalling (without proof) a few general results about monogenerated left-shelves, in particular a useful freeness criterion (Subsection 3.1). Then special braids and the canonical braid decompositions they lead to are described in Subsection 3.2. Finally, we recall in Subsection 3.3 the connection between special braids and the canonical (Dehornoy) braid order, leading to the Laver conjecture, a deep open question.

**3.1. Monogenerated left-shelves.** Every braid  $\beta$  generates under  $\triangleright$  a substructure of  $(B_\infty, \triangleright)$ , hence a sub-left-shelf. By definition, such left-shelves are monogenerated, that is, generated by a single element. This implies a number of consequences because of the so-called comparison property involving left division.

**Definition 3.1 (division relation).** For  $\triangleright$  a binary operation on  $S$  and  $a, b$  in  $S$ , we say that  $a$  (left) divides  $b$ , written  $a \sqsubset b$ , if  $a \triangleright x = b$  holds for some  $x$ . We write  $\sqsubset^*$  for the transitive closure of  $\sqsubset$ .

If  $\triangleright$  is associative, there is no need to distinguish between  $\sqsubset$  and  $\sqsubset^*$ , since we then have  $(a \triangleright x_1) \triangleright x_2 = a \triangleright (x_1 \triangleright x_2)$ , but, in general,  $\sqsubset$  need not be transitive.

The following result about selfdistributivity is fundamental:

**Lemma 3.2 (comparison property).** *If  $(S, \triangleright)$  is a monogenerated left-shelf and  $a, b$  belong to  $S$ , then at least one of  $a \sqsubset^* b$ ,  $a = b$ ,  $b \sqsubset^* a$  holds.*

If  $\phi$  is a morphism,  $a \sqsubset^* b$  implies  $\phi(a) \sqsubset^* \phi(b)$ , so the point is to prove Lemma 3.2 when  $S$  is a free left-shelf with one generator. We use the result (which is nontrivial) as a black box, referring for instance to [26] for an idea of the proof.

One of the interests of the comparison property is to provide a simple criterion for recognizing *free* monogenerated left-shelves. We recall the formal definition:

**Definition 3.3 (free family, free shelf).** If  $(S, \triangleright)$  is left-shelf, a subfamily  $X$  of  $S$  is said to be *free* in  $S$  if, for every left-shelf  $S^\sharp$ , every map from  $X$  to  $S^\sharp$  extends in a morphism from the subshelf of  $S$  generated by  $X$  to  $S^\sharp$ . We say that  $(S, \triangleright)$  is *free based on  $X$*  if  $X$  generates  $S$  and is free in  $S$ .

**Lemma 3.4 (freeness criterion).** *If  $(S, \triangleright)$  is a left-shelf generated by a single element  $g$  and division has no cycle in  $S$ , then  $(S, \triangleright)$  is free based on  $g$ . Moreover, the relation  $\sqsubset^*$  is a (strict) linear order on  $S$ , and, for all  $a, b, c$  in  $S$ , we have*

$$(3.1) \quad a \sqsubset^* a \triangleright b, \quad \text{and} \quad b \sqsubset^* c \Leftrightarrow a \triangleright b \sqsubset^* a \triangleright c.$$

*Proof.* By definition, the relation  $\sqsubset^*$  is transitive, and the assumption that  $\sqsubset$  has no cycle implies that  $\sqsubset^*$  is irreflexive ( $a \sqsubset^* a$  is always false). Hence,  $\sqsubset^*$  is a strict order on  $S$ . The comparison property implies that this order is linear. The relation  $a \sqsubset a \triangleright b$  holds by definition, hence so does  $a \sqsubset^* a \triangleright b$ . Moreover,  $b \sqsubset c$ , say  $b \triangleright x = c$ , implies  $(a \triangleright b) \triangleright (a \triangleright x) = a \triangleright c$  by LD, hence  $a \triangleright b \sqsubset a \triangleright c$ . Thus,  $b \sqsubset^* c$  implies

$a \triangleright b \sqsubset^* a \triangleright c$ . The converse implication must hold, since  $\sqsubset^*$  is a strict linear order:  $a \triangleright b \sqsubset a \triangleright c$  excludes  $b = c$  and  $b \sqsubset^* c$ , so  $b \sqsubset^* c$  is the only possibility. So (3.1) is satisfied.

Let  $S^\sharp$  be an arbitrary left-shelf, and let  $g^\sharp$  lie in  $S^\sharp$ . By assumption, every element of  $S$  is the evaluation at  $g$  of some expression  $T(x)$  involving a variable  $x$  and  $\triangleright$  (a “term”). We construct a morphism  $\phi$  from  $S$  to  $S^\sharp$  by mapping  $T(g)$ , that is,  $T(x)$  evaluated at  $g$  in  $S$ , to  $T(g^\sharp)$ , that is,  $T(x)$  evaluated at  $g^\sharp$  in  $S^\sharp$ . The problem is that an element of  $S$  is the evaluation of several terms, whose evaluations need not a priori coincide.

Let  $\text{Term}_\triangleright(x)$  be the family of all terms constructed from  $x$  and  $\triangleright$ , and let  $=_{\text{LD}}$  be the congruence on  $\text{Term}_\triangleright(x)$  generated by the instances of the law LD: two terms  $T, T'$  are  $=_{\text{LD}}$ -equivalent if, and only if, one can go from  $T$  to  $T'$  by repeatedly applying the law LD. If  $T =_{\text{LD}} T'$  holds, the assumption that  $(S^\sharp, \triangleright)$  obeys the law LD implies  $T(g^\sharp) = T'(g^\sharp)$  in  $S^\sharp$ . Now assume  $T \neq_{\text{LD}} T'$ . By construction,  $\text{Term}_\triangleright(x)/=_{\text{LD}}$  is a monogenerated left-shelf, hence it satisfies the comparison property. The assumption  $T \neq_{\text{LD}} T'$  means that the classes of  $T$  and  $T'$  do not coincide, hence they must be connected by  $\sqsubset^*$  or  $\sqsubset^*$ . Assume the former. By definition, this means that there exists  $n \geq 1$  and terms  $T_1, \dots, T_n$  satisfying

$$(\dots ((T \triangleright T_1) \triangleright T_2) \triangleright \dots) \triangleright T_n =_{\text{LD}} T',$$

which in turn implies in the left-shelf  $S$

$$(\dots ((T(g) \triangleright T_1(g)) \triangleright T_2(g)) \triangleright \dots) \triangleright T_n(g) =_{\text{LD}} T'(g),$$

whence  $T(g) \sqsubset^* T'(g)$  and, a fortiori,  $T(g) \neq T'(g)$ . So, finally,  $T(g) = T'(g)$  can occur only when  $T =_{\text{LD}} T'$  holds, and, therefore, it implies  $T(g^\sharp) = T'(g^\sharp)$  in  $S^\sharp$ . So the morphism  $\phi$  is well defined, and  $S$  is free.  $\square$

The previous criterion is important here because of the following results.

**Lemma 3.5 ( $\sigma_1$ -positivity).** *Call a braid  $\sigma_1$ -positive if it admits at least one expression in which the letter  $\sigma_1$  occurs and no letter  $\sigma_1^{-1}$  does. Then, for all braids  $\beta, \beta'$ , the relation  $\beta \sqsubset^* \beta'$  in  $B_\infty$  implies that  $\beta^{-1}\beta'$  is  $\sigma_1$ -positive.*

*Proof.* By definition,  $\beta \sqsubset^* \beta'$  holds if, and only if, there exist  $n \geq 1$  and  $\beta_1, \dots, \beta_n$  satisfying

$$(3.2) \quad (\dots ((\beta \triangleright \beta_1) \triangleright \beta_2) \triangleright \dots) \triangleright \beta_n = \beta'.$$

According to the definition of  $\triangleright$ , this expands into an equality of the form

$$(3.3) \quad \beta^{-1}\beta' = \text{sh}(\gamma_0) \sigma_1 \text{sh}(\gamma_1) \sigma_1 \dots \sigma_1 \text{sh}(\gamma_n),$$

where the right hand term is explicitly  $\sigma_1$ -positive.  $\square$

**Lemma 3.6 (no cycle).** [13] *Division has no cycle in  $(B_\infty, \triangleright)$ .*

*Proof (sketch).* By Lemma 3.5, a cycle for  $\sqsubset^*$ , hence a relation  $\beta \sqsubset^* \beta$ , would provide a  $\sigma_1$ -positive braid that is trivial (equal to 1). Hence, for excluding (3.2), it suffices to prove that a  $\sigma_1$ -positive braid is never trivial.

Several arguments exist, see in particular [13, 17]. The simplest argument is the one, due to D. Larue [43], that appeals to the Artin representation of  $B_\infty$  in  $\text{Aut}(F_\infty)$ , where  $F_\infty$  is a free group based on an infinite family  $\{x_i \mid i \geq 1\}$ ,

identified with the family of freely reduced words on  $\{x_i^{\pm 1} \mid i \geq 1\}$ . Artin's representation is defined by the rules

$$\rho(\sigma_i)(x_i) := x_i x_{i+1} x_i^{-1}, \quad \rho(\sigma_i)(x_{i+1}) := x_i, \quad \rho(\sigma_i)(x_k) := x_k \text{ for } k \neq i, i+1,$$

and simple arguments about free reduction show that, if  $\gamma$  is a  $\sigma_1$ -positive braid, then  $\rho(\gamma)$  maps  $x_1$  to a reduced word that finishes with the letter  $x_1^{-1}$  and, therefore,  $\gamma$  cannot be trivial, since  $\rho(1)$  maps  $x_1$  to  $x_1$ , which does not finish with  $x_1^{-1}$ .  $\square$

Merging Lemma 3.6 with the criterion of Lemma 3.4, we deduce

**Proposition 3.7 (free).** *For every braid  $\beta$ , the substructure  $\langle \beta \rangle$  of  $(B_\infty, \triangleright)$  generated by  $\beta$  is free based on  $\{\beta\}$ . Moreover, the division relation provides a linear order on  $\langle \beta \rangle$  that satisfies (3.1).*

Another consequence of Lemma 3.6 is that the sufficient freeness condition of Lemma 3.4 is also necessary:

**Corollary 3.8.** *Division in a free left-shelf has no cycle.*

*Proof.* Let  $(S, \triangleright)$  be a free left-shelf based on  $X$ . By the universal property of free left-shelves, the map from  $X$  to  $B_\infty$  sending every element to the braid 1 extends to a morphism  $\pi$  from  $(S, \triangleright)$  to  $(B_\infty, \triangleright)$ . Then the image under  $\pi$  of a cycle for  $\sqsubset$  in  $S$  would be a cycle for  $\sqsubset$  in  $B_\infty$ . By Lemma 3.6, such a cycle cannot exist.  $\square$

**3.2. Special braids and special decompositions.** Hereafter, we concentrate on the particular case of the substructure of  $(B_\infty, \triangleright)$  generated by 1 (unit braid).

**Definition 3.9 (special braid).** We denote by  $B_\infty^{\text{sp}}$  the closure of  $\{1\}$  in  $(B_\infty, \triangleright)$ . The elements of  $B_\infty^{\text{sp}}$  are called *special braids*.

A braid is special if it admits an expression that exclusively involves the braid 1 and the operation  $\triangleright$ —in other words, if it is the evaluation at 1 of a term of  $\text{Term}_\triangleright(x)$  in  $(B_\infty, \triangleright)$ . For instance,  $1, \sigma_1, \sigma_2\sigma_1, \sigma_1^2\sigma_2^{-1}$  are special braids, as we have

$$\sigma_1 = 1 \triangleright 1, \quad \sigma_2\sigma_1 = 1 \triangleright (1 \triangleright 1), \quad \sigma_1^2\sigma_2^{-1} = (1 \triangleright 1) \triangleright 1.$$

Similarly, the braid  $\sigma_m \cdots \sigma_2\sigma_1$  is special, as we saw above that it is the right power  $1^{[m+1]}$ . On the other hand, lots of braids are not special: for instance, Lemma 3.17 below implies that  $\sigma_i$  is not special for  $i \geq 2$ .

Let us begin with a closure property of  $B_\infty^{\text{sp}}$ .

**Lemma 3.10 (closure).** *Special braids are closed under left division, in the sense that, if  $\beta$  and  $\gamma$  are special and  $\beta \triangleright \beta' = \gamma$  holds, then  $\beta'$  is necessarily special.*

*Proof (sketch).* By the easy direction of Prop. 2.5, the existence of  $\beta'$  in  $B_\infty$  satisfying  $\beta \triangleright \beta' = \gamma$  implies  $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$  in  $B_\infty$ , hence in  $B_\infty^{\text{sp}}$ . Conversely, it is known that, since  $(B_\infty^{\text{sp}}, \triangleright)$  is a free monogenerated left-shelf,  $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$  implies the existence in  $B_\infty^{\text{sp}}$  of  $\beta''$  satisfying  $\beta \triangleright \beta'' = \gamma$ : this is a highly nontrivial result about free shelves based on the existence of an explicit normal form [19]. Then left cancellativity forces  $\beta' = \beta''$ , hence  $\beta' \in B_\infty^{\text{sp}}$ .  $\square$

As it is a substructure of  $(B_\infty, \triangleright)$ , the structure  $(B_\infty^{\text{sp}}, \triangleright)$  is a left-shelf, hence eligible for Lemma 2.8, and, moreover, it is left cancellative, hence eligible for Lemma 2.9. Therefore, there exists a (total) action of  $B_n^+$  on  $(B_\infty^{\text{sp}})^n$ , and a partial action of  $B_n$  on  $(B_\infty^{\text{sp}})^n$ . These actions are fundamental in the sequel.

The first result is a characterization of special braids in terms of the action.

**Lemma 3.11 (special vs. action).** (See Fig. 4.) A braid  $\beta$  is special if, and only if,  $(1, 1, 1, \dots) \bullet \beta$  exists and is equal to  $(\beta, 1, 1, \dots)$ .

*Proof.* First, we inductively show that the condition is satisfied for every special braid  $\beta$ . It is obvious for  $\beta = 1$ . For  $\beta = \beta_1 \triangleright \beta_2$  with  $\beta_1, \beta_2$  special, we find

$$\begin{aligned} (1, 1, \dots) \bullet \beta &= (((1, 1, \dots) \bullet \beta_1) \bullet \text{sh}(\beta_2)) \bullet \sigma_1 \bullet \text{sh}(\beta_1)^{-1} \\ &= (((\beta_1, 1, 1, \dots) \bullet \text{sh}(\beta_2)) \bullet \sigma_1) \bullet \text{sh}(\beta_1)^{-1} \\ &= ((\beta_1, \beta_2, 1, 1, \dots) \bullet \sigma_1) \bullet \text{sh}(\beta_1)^{-1} \\ &= (\beta, \beta_1, 1, 1, \dots) \bullet \text{sh}(\beta_1)^{-1} = (\beta, 1, 1, 1, \dots). \end{aligned}$$

For the last step, the induction hypothesis for  $\beta_1$  implies that  $(1, 1, 1, \dots) \bullet \beta_1$  is defined and equal to  $(\beta_1, 1, 1, \dots)$ . By reversing the diagram, we deduce that that  $(\beta_1, 1, 1, \dots) \bullet \beta_1^{-1}$  is defined and equal to  $(1, 1, \dots)$ , and, from there, that  $(\beta, \beta_1, 1, 1, \dots) \bullet \text{sh}(\beta_1)^{-1}$  is defined and equal to  $(\beta, 1, 1, \dots)$ , as expected.

Conversely, we claim that, whenever  $(1, 1, 1, \dots) \bullet w = (\beta_1, \beta_2, \dots)$  holds, then all braids  $\beta_i$  are special. The claim is true when  $w$  is empty. It is preserved under adding a positive letter  $\sigma_i$ , because special braids are closed under  $\triangleright$ , and it is preserved under adding a negative letter  $\sigma_i^{-1}$  because of Lemma 3.10. So, in particular,  $(1, 1, 1, \dots) \bullet \beta = (\beta, 1, 1, \dots)$  implies that  $\beta$  is special.  $\square$

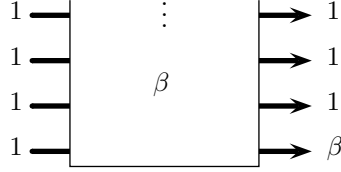


FIGURE 4. A special braid is a braid that produces itself using braid coloring and starting from unit braids.

We now arrive at the main result, namely decompositions of arbitrary braids in terms of special braids.

**Proposition 3.12 (special decomposition).** (i) For every braid  $\beta$  in  $B_n^+$ , there is a unique sequence of special braids  $\beta_1, \dots, \beta_n$  satisfying

$$(3.4) \quad \beta = \beta_1 \cdot \text{sh}(\beta_2) \cdot \dots \cdot \text{sh}^{n-1}(\beta_n).$$

(ii) For every braid  $\beta$  in  $B_n$ , there are special braids  $\beta_1, \dots, \beta_n, \beta'_1, \dots, \beta'_n$  satisfying

$$(3.5) \quad \beta = \text{sh}^{n-1}(\beta_n^{-1}) \cdot \dots \cdot \text{sh}(\beta_2^{-1}) \cdot \beta_1^{-1} \cdot \beta'_1 \cdot \text{sh}(\beta'_2) \cdot \dots \cdot \text{sh}^{n-1}(\beta'_n).$$

*Proof.* (i) Starting from  $\beta$  in  $B_n^+$ , define  $(\beta_1, \dots, \beta_n) := (1, \dots, 1) \bullet \beta$ . As the input sequence  $(1, \dots, 1)$  consists of special braids and  $B_\infty^{\text{sp}}$  is closed under  $\triangleright$ , all braids involved in the coloring of a positive diagram representing  $\beta$  are special. So, in particular, the output colours  $\beta_1, \dots, \beta_n$  are special. Next, we have  $\prod^{\text{sh}}(1, \dots, 1) = 1$ , so applying (2.13) directly gives (3.4).

As for uniqueness, assume  $\beta = \beta'_1 \cdot \text{sh}(\beta'_2) \cdot \dots \cdot \text{sh}^{n-1}(\beta'_n)$  with  $\beta'_1, \dots, \beta'_n$  special. Then Lemma 3.11 implies  $(1, 1, \dots) \bullet \beta'_i = (\beta'_i, 1, 1, \dots)$  for every  $i$ . Using  $\frown$  for concatenation of finite sequences, we deduce

$$\begin{aligned} (1, 1, \dots) \bullet \beta'_1 \cdot \text{sh}(\beta'_2) &= (\beta'_1, 1, \dots) \bullet \text{sh}(\beta'_2) = (\beta'_1) \frown (1, 1, \dots) \bullet \beta'_2 \\ &= (\beta'_1) \frown (\beta'_2, 1, 1, \dots) = (\beta'_1, \beta'_2, 1, 1, \dots), \end{aligned}$$

whence, repeating the argument,

$$(1, 1, 1, \dots) \bullet \beta'_1 \cdot \text{sh}(\beta'_2) \cdot \dots \cdot \text{sh}^{n-1}(\beta'_n) = (\beta'_1, \beta'_2, \dots, \beta'_n),$$

which is  $(1, 1, 1, \dots) \bullet \beta = (\beta'_1, \dots, \beta'_n)$ . It follows that  $(\beta'_1, \dots, \beta'_n)$  must be the result of the action of  $\beta$  on  $(1, 1, 1, \dots)$ , which is unique by Lemma 2.9.

(ii) It is known that every braid in  $B_n$  can be expressed as a quotient  $\beta'^{-1} \cdot \beta''$  with  $\beta', \beta''$  in  $B_n^+$ . The result then follows from applying (i) to  $\beta'$  and  $\beta''$ .  $\square$

**Example 3.13.** Consider  $\beta = \sigma_1^{-2} \sigma_2 \sigma_1$ , which is  $\beta'^{-1} \beta''$  with  $\beta' = \sigma_1^2$  and  $\beta'' = \sigma_2 \sigma_1$ . By (2.10), we find  $(1, 1, 1) \bullet \beta' = (\sigma_1^2 \sigma_2^{-1}, \sigma_1, 1)$ , and  $(1, 1, 1) \bullet \beta'' = (\sigma_2 \sigma_1, 1, 1)$ . We deduce the expression

$$\beta = \text{sh}^2(1)^{-1} \cdot \text{sh}(\sigma_1)^{-1} \cdot (\sigma_1^2 \sigma_2^{-1})^{-1} \cdot (\sigma_2 \sigma_1) \cdot \text{sh}(1) \cdot \text{sh}^2(1),$$

or, using the trivial braid 1 and the operations  $\triangleright, ^{-1}$  and  $\text{sh}$  exclusively,

$$(3.6) \quad \beta = \text{sh}^2(1)^{-1} \cdot \text{sh}(1 \triangleright 1)^{-1} \cdot ((1 \triangleright 1) \triangleright 1)^{-1} \cdot (1 \triangleright (1 \triangleright 1)) \cdot \text{sh}(1) \cdot \text{sh}^2(1),$$

that is, when trivial terms are removed,  $\text{sh}(1^{[2]})^{-1} \cdot (1_{[3]})^{-1} \cdot 1^{[3]}$ .

**Remark 3.14.** For  $\beta$  in  $B_n^+$ , Prop. 3.12 gives  $\beta = \beta_1 \text{sh}(\beta_2) \dots \text{sh}^{n-1}(\beta_n)$  with  $\beta_1, \dots, \beta_n$  special. However, the braids  $\beta_i$  need not lie in  $B_n$ : for instance, the decomposition of  $\sigma_1^2$ , a braid of  $B_2$ , is  $(\sigma_1^2 \sigma_2^{-1}) \text{sh}(\sigma_1)$ , with  $\sigma_1^2 \sigma_2^{-1} \notin B_2$ .

The previous results imply that for a braid to be special is a decidable property.

**Proposition 3.15 (decidability).** *There is an algorithm that decides whether a given braid word represents a special braid, and, if so, returns an expression of this braid in terms of 1 and  $\triangleright$ .*

*Proof (sketch).* Let  $w$  be a braid word. We can decide whether  $w$  represents a special braid as follows. First, we reverse  $w$  into an equivalent braid word  $uv^{-1}$  with  $u, v$  positive using the reversing method of [24]. Next, we compute  $(1, 1, 1, \dots) \bullet uv^{-1}$ . By [13], it is known that, if  $\vec{a} \bullet w$  is defined, then so is  $\vec{a} \bullet uv^{-1}$  when  $u$  and  $v$  are obtained as above, namely so as to ensure that the elements of  $B_\infty^+$  representing  $u$  and  $v$  have no common right divisor. By Lemma 3.11,  $w$  represents a special braid if, and only if, the computation is successful and it leads to a sequence of the form  $(\beta, 1, 1, \dots)$ , that is, all components from the second are trivial. The latter point can be tested using any algorithm for the word problem of braids. Moreover, there exists an effective left division algorithm in free monogenerated shelves [14]. Hence, we can effectively obtain an expression of the special braids involved in  $(1, 1, 1, \dots) \bullet uv^{-1}$  in terms of 1 and  $\triangleright$ .  $\square$

**Example 3.16.** Let  $w := \sigma_2^{-1} \sigma_1^{-1} \sigma_2^2 \sigma_1$ . Reversing  $w$  yields the equivalent positive–negative word  $\sigma_1^2 \sigma_2^{-1}$ , so, here,  $u$  is  $\sigma_1^2$ , and  $v$  is  $\sigma_2$ . Then we compute the value of  $(1, 1, 1) \bullet \sigma_1^2$ , namely  $(\sigma_1^2 \sigma_2^{-1}, \sigma_1, 1)$ , that is,  $(1_{[3]}, 1^{[2]}, 1)$ . Then, in order to apply  $v^{-1}$ , we have to left divide  $1^{[2]}$  by 1. In the present case, the result is obvious: division is possible and the quotient is 1. So we obtain  $(1, 1, 1) \bullet \sigma_1^2 \sigma_2^{-1} = (1_{[3]}, 1, 1)$ , and we conclude that  $w$  represents the special braid  $1_{[3]}$ .

We conclude with a characterisation first of braids that are positive and special, and of braids whose special decomposition only contains positive braids.

**Lemma 3.17 (positive special).** *For every  $m$ , there is a unique special positive braid of length  $m$ , namely  $1^{[m+1]}$ .*

*Proof.* We saw above the equality  $1^{[m+1]} = \sigma_m \cdots \sigma_2 \sigma_1$ , a positive braid of length  $m$ . Conversely, assume that  $\beta$  is positive and special of length  $m$ . We use induction on  $m$ . For  $m = 0$ , the only possibility is  $\beta = 1 = 1^{[1]}$ . Assume  $m \geq 1$ , and write  $\beta = \beta' \sigma_i$ . By Lemma 3.11, the assumption that  $\beta$  is special implies the equality  $(1, 1, 1, \dots) \bullet \beta = (\beta, 1, 1, \dots)$ . Since  $\beta'$  is positive,  $(1, 1, \dots) \bullet \beta'$  exists. Call it  $(\beta'_1, \beta'_2, \dots)$ . If we had  $i \geq 2$ , the  $i$ th entry in  $(1, 1, \dots) \bullet \beta' \sigma_i$  would be  $\beta'_i \triangleright \beta'_{i+1}$ , which cannot be 1. Thus we must have  $i = 1$ , whence  $\beta = \beta'_1 \triangleright \beta'_2$ ,  $\beta'_1 = \beta'_3 = \dots = 1$ , that is,  $(1, 1, \dots) \bullet \beta' = (1, \beta'_2, 1, 1, \dots)$ . By (3.4), we deduce  $\beta' = \text{sh}(\beta'_2)$ . Hence  $\beta'_2$  is positive and special. The induction hypothesis implies  $\beta'_2 = 1^{[m]}$ , and we deduce  $\beta = 1 \triangleright 1^{[m]} = 1^{[m+1]}$ .  $\square$

**Proposition 3.18 (positive special decomposition).** *A braid  $\beta$  admits a special decomposition consisting of positive braids if, and only if,  $\beta$  is a positive simple braid, that is, there exists an integer  $n$  such that  $\beta$  divides Garside's fundamental braid  $\Delta_n$  in the monoid  $B_\infty^+$ .*

*Proof.* Assume  $\beta = \prod^{\text{sh}}(\beta_1, \dots, \beta_n)$  with  $\beta_1, \dots, \beta_n$  special and positive. Then, as seen in the proof of Prop. 3.12,  $(1, 1, 1, \dots) \bullet \beta$  is defined and equal to  $(\beta_1, \beta_2, \dots)$ . Hence, by Lemma 3.17, there exists for each  $i$  a number  $m_i$  satisfying  $\beta_i = 1^{[m_i+1]}$ . Then (3.4) expands into

$$(3.7) \quad \beta = (\sigma_{m_1} \cdots \sigma_1) \cdot \text{sh}(\sigma_{m_2} \cdots \sigma_1) \cdot \cdots$$

This shows that  $\beta$  is a positive braid, in which any two strands cross at most once, thus a divisor of  $\Delta_n$  for  $n$  large enough.

Conversely, assume that  $\beta$  is a positive simple braid. Then it is known that  $\beta$  admits a decomposition of the form (3.7), where  $m_i + 1$  is the initial position of the strand that finishes at position  $i$  in  $\beta$ . By uniqueness, this decomposition coincides with the one associated with  $(1, 1, 1, \dots) \bullet \beta$ , meaning that the entries of  $(1, 1, 1, \dots) \bullet \beta$  are the positive braids  $1^{[m_i+1]}$ .  $\square$

In particular, the special decomposition of  $\Delta_n$  is

$$\Delta_n = (\sigma_{n-1} \cdots \sigma_1) \cdot \text{sh}(\sigma_{n-2} \cdots \sigma_1) \cdot \cdots \cdot \text{sh}^{n-2}(\sigma_1).$$

In contrast to Lemma 3.17, which completely describes special braids lying in  $B_n^+$ , very little is known about special braids that lie in  $B_n$ . Inductively defining the *complexity* of a special braid  $\beta$  by  $c(1) := 0$  and

$$c(\beta) := \min\{\sup\{c(\beta_1), c(\beta_2)\} + 1 \mid \beta = \beta_1 \triangleright \beta_2\},$$

one easily checks that  $c(\beta) \leq n$  implies  $\beta \in B_n$ .

**Question 3.19 (special  $n$ -strand braids).** *Is the converse true, that is, does  $c(\beta) \leq n$  hold for every special braid  $\beta$  that lies in  $B_n$ ?*

A positive answer would in particular imply that there are at most  $2^n$  special braids in  $B_n$ .

**3.3. Ordering braids.** Together with the acyclicity result of Lemma 3.6, the comparison property of Lemma 3.2 implies that the iterated division relation  $\sqsubset^*$  is a linear ordering on the family of all special braids  $B_\infty^{\text{sp}}$ . As every braid admits a decomposition in terms of special braids, it is not surprising that the linear order on  $B_\infty^{\text{sp}}$  extends to a linear order on arbitrary braids. We briefly recall the construction. The interest here is not to establish the orderability of  $B_\infty$ , now a standard

result [27], but to explain the connection with the shelf operation  $\triangleright$  and state the Laver conjecture.

We recall from Lemma 3.5 that a braid  $\beta$  is said to be  $\sigma_1$ -positive if it admits at least one expression where  $\sigma_1$  occurs and  $\sigma_1^{-1}$  does not. We define  $\sigma_1$ -negative (no  $\sigma_1$  and at least one  $\sigma_1^{-1}$ ) and  $\sigma_1$ -free (no  $\sigma_1$  and no  $\sigma_1^{-1}$ ) accordingly.

**Lemma 3.20 (order on special).** *If  $\beta, \beta'$  are special braids, the relation  $\beta \sqsubset^* \beta'$  in  $B_\infty^{\text{sp}}$  is equivalent to  $\beta^{-1}\beta'$  being  $\sigma_1$ -positive.*

*Proof.* We saw in Lemma 3.5 that, if  $\beta \sqsubset^* \beta'$  holds in  $B_\infty$ , hence in particular if  $\beta \sqsubset^* \beta'$  holds in  $B_\infty^{\text{sp}}$ , then  $\beta^{-1}\beta'$  is  $\sigma_1$ -positive. Conversely, assume that  $\beta$  and  $\beta'$  are special and  $\beta^{-1}\beta'$  is  $\sigma_1$ -positive. By Lemma 3.2, at least one of  $\beta \sqsubset^* \beta'$ ,  $\beta = \beta'$ , or  $\beta \sqsupset^* \beta'$  holds in  $B_\infty^{\text{sp}}$ . The second option implies that  $\beta^{-1}\beta'$  is trivial, hence, by Lemma 3.6, not  $\sigma_1$ -positive. The third option implies that  $\beta'^{-1}\beta$  is  $\sigma_1$ -positive, which again contradicts the  $\sigma_1$ -positivity of  $\beta^{-1}\beta'$ , as the product of the  $\sigma_1$ -positive braids  $\beta^{-1}\beta'$  and  $\beta'^{-1}\beta$ , which is 1, would be  $\sigma_1$ -positive. So  $\beta \sqsubset^* \beta'$  is the only possibility.  $\square$

Using the special decomposition of Prop. 3.12, we immediately deduce:

**Proposition 3.21 (order).** *Every braid is  $\sigma_1$ -positive,  $\sigma_1$ -negative, or  $\sigma_1$ -free, each possibility excluding the others.*

*Proof.* Let  $\beta \in B_n$ . By Prop. 3.12, there exist  $\beta_1, \dots, \beta_n, \beta'_1, \dots, \beta'_n$  special satisfying

$$\beta = \text{sh}^{n-1}(\beta_n^{-1}) \cdot \dots \cdot \text{sh}(\beta_2^{-1}) \cdot \beta_1^{-1} \cdot \beta'_1 \cdot \text{sh}(\beta_2) \cdot \dots \cdot \text{sh}^{n-1}(\beta'_n),$$

which has the form  $\beta = \text{sh}(\gamma) \cdot \beta_1^{-1}\beta'_1 \cdot \text{sh}(\gamma')$ . By Lemma 3.20,  $\beta_1^{-1}\beta'_1$  is either  $\sigma_1$ -positive, in which case so is  $\beta$ , or equal to 1, in which case  $\beta$  is  $\sigma_1$ -free, or  $\sigma_1$ -negative, in which case so is  $\beta$ . The three cases exclude one another by Lemma 3.6.  $\square$

**Remark 3.22.** The previous simple argument takes place in  $B_\infty$ , and does not guarantee that a braid of  $B_n$  necessarily admits a  $\sigma_1$ -positive expression by an  $n$ -strand braid word. The latter property is true, but it requires a further proof [17].

From that point, it is straightforward to define an order on  $B_\infty$ .

**Corollary 3.23 (order).** *Say that a braid is  $\sigma_i$ -positive if it is the image of a  $\sigma_1$ -positive braid under  $\text{sh}^{i-1}$ . For  $\beta_1, \beta_2$  in  $B_\infty$ , define  $\beta_1 < \beta_2$  to mean that  $\beta_1^{-1}\beta_2$  is  $\sigma_i$ -positive for some  $i$ . Then the relation  $<$  is a linear order on  $B_\infty$ ; it is compatible with multiplication on the left, and extends the order  $\sqsubset^*$  on  $B_\infty^{\text{sp}}$ .*

It is then easy to check that the order so defined on  $B_\infty$  is a lexicographic extension of the order  $\sqsubset^*$  on special braids: for every braid  $\beta$ , the relation  $\beta > 1$  holds if, and only if, whenever  $\beta_1, \dots, \beta_n, \beta'_1, \dots, \beta'_n$  are special and we have

$$(\beta_1, \dots, \beta_n) \bullet \beta = (\beta'_1, \dots, \beta'_n),$$

the sequence  $(\beta_1, \dots, \beta_n)$  is smaller than  $(\beta'_1, \dots, \beta'_n)$  with respect to the lexicographical extension of  $\sqsubset^*$  (look at the first  $i$  such that  $\beta_i$  and  $\beta'_i$  do not coincide).

Let us return to the monoid  $B_\infty^+$ . The following was proved by R. Laver [46], and then made more precise by S. Burckel [7] and J. Fromentin [35, 36, 37]:

**Proposition 3.24 (well-order).** *For every  $n$ , the restriction of the braid order  $<$  to  $B_n^+$  is a well-order of order type the Cantor ordinal  $\omega^{\omega^{n-2}}$ ; the restriction of  $<$  to  $B_\infty^+$  is a well-order of order type  $\omega^{\omega^\omega}$ .*

If  $\beta$  is a positive  $n$ -strand braid, Lemma 2.8 guarantees that  $(\beta_1, \dots, \beta_n) \bullet \beta$  is defined for every sequence of braids  $(\beta_1, \dots, \beta_n)$ . Thus, reversing the perspective and starting from the sequence  $(\beta_1, \dots, \beta_n)$ , we see that the family of all braids  $\beta$  for which  $(\beta_1, \dots, \beta_n) \bullet \beta$  is defined includes the monoid  $B_n^+$ .

**Question 3.25 (Laver conjecture).** *For every sequence of braids  $(\beta_1, \dots, \beta_n)$ , is the family of all braids  $\beta$  for which  $(\beta_1, \dots, \beta_n) \bullet \beta$  is defined well-ordered by  $<$ ?*

R. Laver conjectured a positive answer. A similar question can be raised for every left-shelf  $(S, \triangleright)$ , and, in some cases, the family in question reduces to  $B_n^+$  [43]. But this is not the case in general, in particular in the case of  $B_\infty$ , and the question remains open, and it seems difficult. Note that this is a pure question of topology, in that it exclusively involves braids and no other structure.

#### 4. QUOTIENTS

We now summarize results about the selfdistributive operations obtained from the braid operation  $\triangleright$  by quotienting the group or shelf structure. Although several natural and simple questions arise, little is known here. We successively consider the case of the symmetric group (Subsection 4.1) and of the Burau representation (Subsection 4.2), which arise when the group structure is quotiented, and the case of Laver tables, which arise when the shelf structure is quotiented (Subsection 4.3).

**4.1. Permutations.** For every  $n$ , a well understood quotient of the group  $B_n$  appears when the elements  $\sigma_i^2$  are collapsed, namely the symmetric group  $\mathfrak{S}_n$ . Geometrically, the projection corresponds to associating with a braid  $\beta$  the permutation  $\text{perm}(\beta)$  so that, for  $1 \leq i < n$ , the strand finishing at position  $i$  begins at position  $\text{perm}(\beta)(i)$  in any braid diagram representing  $\beta$ . The projection extends to  $B_\infty$ , the image being the symmetric group  $\mathfrak{S}_\infty$  of all permutations of  $\mathbb{Z}_{>0}$  that move finitely many entries, equipped with composition.

We denote by  $s_i$  the projection of  $\sigma_i$ , that is, the transposition exchanging  $i$  and  $i + 1$ . We use  $\text{sh}$  for the *shift* endomorphism of  $\mathfrak{S}_\infty$  defined, for  $f$  in  $\mathfrak{S}_\infty$ , by  $\text{sh}(f)(1) := 1$  and  $\text{sh}(f)(n) := f(n - 1) + 1$  for  $n \geq 2$ .

As the operation  $\triangleright$  on  $B_\infty$  is defined from the group multiplication and the endomorphism  $\text{sh}$ , every group morphism from  $B_\infty$  to a group  $G$  that carries  $\text{sh}$  to some convenient endomorphism of  $G$  induces a  $\triangleright$ -morphism, and the image operation automatically obeys the selfdistributivity law LD. In this way, we obtain:

**Proposition 4.1 (permutation shelf).** *For  $f, g$  in  $\mathfrak{S}_\infty$ , define*

$$(4.1) \quad f \triangleright g := f \cdot \text{sh}(g) \cdot s_1 \cdot \text{sh}(f)^{-1}.$$

*Then  $(\mathfrak{S}_\infty, \triangleright)$  is a left-shelf, and  $\text{perm}$  is a surjective morphism from  $(B_\infty, \triangleright)$  to  $(\mathfrak{S}_\infty, \triangleright)$ .*

On the shape of what was done for braids in Section 3, it is natural to consider the substructure of  $(\mathfrak{S}_\infty, \triangleright)$  generated by the identity map  $\text{id}$  of  $\mathbb{Z}_{>0}$ .

**Definition 4.2 (special permutation).** We denote by  $\mathfrak{S}_\infty^{\text{sp}}$  the closure of  $\{\text{id}\}$  in  $(\mathfrak{S}_\infty, \triangleright)$ . The elements of  $\mathfrak{S}_\infty^{\text{sp}}$  are called *special* permutations.

Clearly,  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  is a monogenerated left-shelf, and  $\text{perm}$  induces a surjective morphism from  $(B_\infty^{\text{sp}}, \triangleright)$  onto  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$ , since  $\text{id}$  is the permutation associated with



the unit braid. One easily checks that, for every  $n$ , the right power  $\text{id}^{[n]}$  is the  $n$ -cycle  $s_{n-1} \cdots s_2 s_1$ . The left powers  $\text{id}_{[n]}$  are more mysterious; the first values are

$$\text{id}_{[2]} = s_1, \quad \text{id}_{[3]} = s_2, \quad \text{id}_{[4]} = s_2 s_3 s_1, \quad \text{id}_{[5]} = s_3 s_4 s_2 s_3 s_4, \dots$$

see Fig. 5 for an embryo of the table of  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  starting with left powers.

$\mathfrak{S}_\infty^{\text{sp}}$	id	$s_1$	$s_2$	$s_2 s_3 s_1$	...
id	$s_1$	$s_2 s_1$	$s_3 s_1$	$s_3 s_4 s_2 s_1$	...
$s_1$	$s_2$	$s_2 s_1$	$s_3 s_2$	$s_3 s_4 s_2 s_1$	...
$s_2$	$s_2 s_3 s_1$	$s_3 s_1$	$s_2 s_1$	$s_3 s_4 s_2 s_3 s_4 s_1$	...
$s_2 s_3 s_1$	$s_3 s_4 s_2 s_3 s_4$	$s_3 s_4 s_2 s_3 s_4 s_1$	$s_4 s_3$	$s_3 s_1$	...
...	...	...	...	...	...

FIGURE 5. An embryo of the table of  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  based on left powers of id.

In the left-shelf  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$ , the division relation  $\sqsubset$  of Def. 3.1 admits cycles: for instance, one can check the equality

$$(4.2) \quad s_2 s_1 = ((s_2 s_1) \triangleright s_1) \triangleright s_2 s_3 s_1,$$

whence  $s_2 s_1 \sqsubset^* s_2 s_1$ . It follows from Corollary 3.8 that  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  is not a free left-shelf: typically, (4.2) translates into  $\text{id}^{[3]} = (\text{id}^{[3]} \triangleright \text{id}_{[2]}) \triangleright \text{id}_{[4]}$ , a nontrivial relation whose counterpart fails in  $B_\infty^{\text{sp}}$ .

**Question 4.3 (presentation).** *Does the left-shelf  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  admit a finite presentation in terms of its generator id?*

Nothing is known. One of the very few results about  $(\mathfrak{S}_\infty, \triangleright)$  known so far is an alternative definition of  $\triangleright$  using conjugation of injections.

**Proposition 4.4 (injection shelf).** *Let  $\mathfrak{I}_\infty$  be the monoid of all injections from  $\mathbb{Z}_{>0}$  to itself equipped with composition, and let SH be the element of  $\mathfrak{I}_\infty$  (“shift”) that maps  $n$  to  $n + 1$  for every  $n$ . For  $f, g$  in  $\mathfrak{I}_\infty$ , define  $f \triangleright g$  in  $\mathfrak{I}_\infty$  by*

$$(4.3) \quad f \triangleright g(n) := f(g(f^{-1}(n))) \text{ for } n \in \text{Im}(f), \text{ and } f \triangleright g(n) := n \text{ otherwise.}$$

*Then  $(\mathfrak{I}_\infty, \triangleright)$  is a left-shelf, and the map  $\phi : f \mapsto f \cdot \text{SH}$  defines an embedding from  $(\mathfrak{S}_\infty, \triangleright)$  into  $(\mathfrak{I}_\infty, \triangleright)$ .*

*Proof.* For all  $f, g$ , the definition implies  $\text{Im}(f \triangleright g) = f(\text{Im}(g)) \cup \text{colm}(f)$  and  $\text{colm}(f \triangleright g) = f(\text{colm}(g))$ . From there, one easily checks that, for every  $n$ , both  $f \triangleright (g \triangleright h)$  and  $(f \triangleright g) \triangleright (f \triangleright h)$  map  $n$  to  $f(g(h(g^{-1}(f^{-1}(n)))))$  for  $n$  in  $\text{Im}(f \cdot g)$ , and to  $n$  otherwise. Thus  $\triangleright$  obeys the selfdistributivity law LD.

To prove that  $\phi$  is a morphism, carefully applying the definitions shows that, for all  $f, g$  in  $\mathfrak{S}_\infty$ , both  $\phi(f \triangleright g)$  and  $\phi(f) \triangleright \phi(g)$  keep  $f(1)$  fixed, and map  $n$  to  $f(g(f^{-1}(n)) + 1)$  for  $n \neq f(1)$ . Finally,  $\phi(f) = \phi(f')$  implies  $\text{sh}(f) = \text{sh}(f')$ , whence  $f = f'$ , so  $\phi$  is injective.  $\square$

By definition, the morphism  $\phi$  of Prop. 4.4 maps the identity permutation id to the injection SH. Hence it induces an isomorphism from the left-shelf  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  to its image, which is the substructure  $\mathfrak{I}_\infty^{\text{sp}}$  of  $(\mathfrak{I}_\infty, \triangleright)$  generated by SH. The left-shelf  $(\mathfrak{I}_\infty^{\text{sp}}, \triangleright)$  is directly reminiscent of the left-shelf  $\text{Iter}(j)$  constructed in set theory using the iterations of an elementary embedding  $j$  under the “application” operation, see [45] or [18, Chapter XII]: the latter structure implies the existence of

an injection  $\widetilde{\text{SH}}$  in  $\mathfrak{J}_\infty$  and of a partial selfdistributive operation  $\widetilde{\triangleright}$  on (a subset of)  $\mathfrak{J}_\infty$  such that  $\widetilde{\triangleright}$  is everywhere defined on the substructure generated by  $\widetilde{\text{SH}}$ , and  $f \widetilde{\triangleright} g(n) = f(g(f^{-1}(n)))$  holds for  $n$  in  $\text{Im}(f)$ , but, instead of “stupidly” completing with  $f \triangleright g(n) := n$  for  $n$  in  $\text{colm}(f)$  as in (4.3), the operation  $\widetilde{\triangleright}$  is constructed so that  $f \widetilde{\triangleright} g$  is increasing when defined. The latter condition implies that the injection  $\widetilde{\text{SH}}$  must be a fast growing function [29, 30, 38], and its existence is currently proved only from a large cardinal axiom (“Laver cardinal”) [18, Chapter XIII].

**Question 4.5 (increasing injections).** *Can one define without any set theoretical assumption a selfdistributive operation on increasing injections of  $\mathbb{Z}_{>0}$ ?*

The question seems very difficult. J.T. Moore wondered whether there could be a connection with the Følner function of Thompson’s group  $F$  [52].

**4.2. Linear representations.** Linear representations of braid groups provide further quotients. The Lawrence–Krammer representation is known to be faithful [1, 42], so its image is just isomorphic to its domain, and nothing new seems to be expectable here.

By contrast, the Burau representation is not faithful [48], and, therefore, its image is a proper quotient. To work with  $B_\infty$ , we have to consider the direct limit  $\text{GL}_\infty(\mathbb{Z}[t, t^{-1}])$  of the groups  $\text{GL}_n(\mathbb{Z}[t, t^{-1}])$  (identified with invertible  $n$ -matrices) with the top–left embeddings of matrices. The (unreduced) version of the representation is defined by

$$\rho(\sigma_i) = \Sigma_i := \text{sh}^{i-1} \left( \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \right),$$

where  $\text{sh}$  is the obvious bottom–right shift of matrices.

Projecting the braid operation  $\triangleright$  yields a selfdistributive operation on the image of  $\rho$ . The latter turns out to extend to arbitrary elements of  $\text{GL}_\infty(\mathbb{Z}[t, t^{-1}])$ :

**Proposition 4.6 (Burau shelf).** *For  $A, B$  in  $\text{GL}_\infty(\mathbb{Z}[t, t^{-1}])$ , define*

$$(4.4) \quad A \triangleright B := A \cdot \text{sh}(B) \cdot \Sigma_1 \cdot \text{sh}(A)^{-1}.$$

*Then  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$  is a left-shelf, and the Burau representation is a morphism from  $(B_\infty, \triangleright)$  to  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$ .*

The verification is the same as for  $B_\infty$ : the point is that  $\Sigma_1$  commutes with every matrix in the image of  $\text{sh}^2$ , and that  $\Sigma_1 \Sigma_2 \Sigma_1 \Sigma_2^{-1}$  is equal to  $\Sigma_2 \Sigma_1$ . We may wonder whether the identity matrix generates under  $\triangleright$  a free left-shelf. The answer must be negative: if so, the division relation would have no cycle in  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$ , implying that the Burau image of a  $\sigma_1$ -positive braid would never be trivial, implying in turn that  $\rho$  is injective—which is false. By the way, an example of a  $\sigma_1$ -positive braid (with five  $\sigma_1$  and no  $\sigma_1^{-1}$ ) whose Burau image is trivial is constructed in [15]. This corresponds to a cycle of length 5 for division in  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$ .

Of course, on the model of Question 4.3, we may ask for a presentation of the subshelf of  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$  generated by the identity matrix. But so little is known about the matrix operation  $\triangleright$  that the question seems out of reach. Clearly, (4.4) implies the relation  $\det(A \triangleright B) = -t \cdot \det(B)$ . A similar but more exotic relation is

$$\text{shtr}(A \triangleright B) = \text{shtr}(B) + t,$$

where  $\text{shtr}(A)$  (“shifted trace”) is the sum of all overdiagonal entries  $\sum_i A_{i, i+1}$ .

**4.3. Laver tables.** For every positive integer  $N$ , there exists a unique binary operation  $\triangleright$  on  $\{1, \dots, N\}$  that satisfies  $x \triangleright 1 = x + 1 \pmod N$  and obeys the law  $x \triangleright (y \triangleright 1) = (x \triangleright y) \triangleright (x \triangleright 1)$ ; the structure so obtained is a left-shelf if, and only if,  $N$  is a power of 2. The structure with  $2^n$  elements is called the  $n$ th Laver table, usually denoted by  $A_n$ , see Fig. 6 for the first four tables. Laver tables appear as the elementary building bricks for constructing all (finite) monogenerated shelves [31, 32, 53], and can adequately be seen as counterparts of cyclic groups in the SD-world. We refer to [19, Chapter X], [25, Chapitre XIV] (in French), or to [33] for a more complete introduction. For every  $n$ , projection modulo  $2^n$  defines a surjective homomorphism from  $A_{n+1}$  to  $A_n$ . It is conjectured that the inverse limit of the system so obtained is free. A proof of the conjecture is known under some large cardinal axiom [47], a very unusual and puzzling situation.

				$A_3$	1	2	3	4	5	6	7	8						
				1	2	4	6	8	2	4	6	8						
			$A_2$	1	2	3	4	3	4	7	8	3	4	7	8			
	$A_0$	1	1	1	2	2	2	4	4	8	8	4	8	4	8			
	1	1	1	1	2	2	2	2	3	4	5	6	7	8	8			
			2	1	2	3	4	4	4	5	6	8	8	6	8	6	8	
			4	1	2	3	4	4	4	6	7	8	7	8	7	8	7	8
									7	8	8	8	8	8	8	8	8	8
									8	1	2	3	4	5	6	7	8	8

FIGURE 6. The first four Laver tables; observe the periodic behaviour of the rows, which consist of the repetition of a pattern whose length is itself a power of 2, a general phenomenon.

Because of the fundamental position of Laver tables in the world of monogenerated left-shelves, a natural question is to connect them with the braid shelf  $(B_\infty, \triangleright)$ . As  $(B_\infty^{\text{sp}}, \triangleright)$  is a free monogenerated left-shelf, there must exist for every  $n$  a congruence  $\equiv_n$  on  $(B_\infty^{\text{sp}}, \triangleright)$  such that  $B_\infty^{\text{sp}}/\equiv_n$  is isomorphic to  $A_n$ .

**Question 4.7** ( $A_n$  as quotient of  $B_\infty$ ). *Does there exist a simple topological/algebraic/combinatorial characterization of the relation  $\equiv_n$  on special braids? Can this relation be extended to arbitrary braids in a natural way?*

At the moment, almost nothing is known about the question. In lack of an answer, we can look at the possible connection between the known quotient of  $(B_\infty, \triangleright)$ , namely the left-shelf  $(\mathfrak{S}_\infty, \triangleright)$  of Section 4.1, and Laver tables. Such a connection exists typically for the 2-element Laver table  $A_1$ .

**Proposition 4.8** ( $A_1$  as quotient of  $\mathfrak{S}_\infty$ ). *Define the class  $\text{cl}(f)$  of a permutation  $f$  in  $\mathfrak{S}_\infty$  to be  $f^{-1}(1)$ . Let  $\mathfrak{S}_\infty^{\text{sm}} := \{f \in \mathfrak{S}_\infty \mid \text{cl}(f) \leq 2\}$  (“small class” permutations).*

(i) *The set  $\mathfrak{S}_\infty^{\text{sm}}$  is closed under  $\triangleright$ , and it includes  $\mathfrak{S}_\infty^{\text{sp}}$ .*

(ii) *Class equality is a congruence on the left-shelf  $(\mathfrak{S}_\infty^{\text{sm}}, \triangleright)$ , hence on  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$ .*

*In both cases, the quotient is the Laver table  $A_1$ .*

*Proof.* (i) As  $s_{n-1} \cdots s_2 s_1$  maps 1 to  $n$ , a permutation  $f$  in  $\mathfrak{S}_\infty$  is of class  $n$  if, and only if,  $f s_{n-1} \cdots s_1$  is of class 1. On the other hand, a permutation  $f$  in  $\mathfrak{S}_\infty$  keeps 1 fixed if, and only if, it lies in the image of the shift mapping. Thus, for every  $n$ , a permutation  $f$  has class  $n$  if, and only if, it can be written as  $\text{sh}(f') s_1 s_2 \cdots s_{n-1}$  for some  $f'$ . In particular, the elements of  $\mathfrak{S}_\infty^{\text{sm}}$  are of the form  $\text{sh}(f')$  or  $\text{sh}(f') s_1$ .

Assume that  $f$  has class 1, say  $f = \text{sh}(f')$ . For every  $g$  in  $\mathfrak{S}_\infty$ , we find

$$f \triangleright g = \text{sh}(f') \text{sh}(g) s_1 \text{sh}^2(f')^{-1} = \text{sh}(f') \text{sh}(g) \text{sh}^2(f')^{-1} s_1,$$

of class 2. Assume now that  $f$  has class 2, say  $f = \text{sh}(f')s_1$ , and  $g$  has class 1, say  $g = \text{sh}(g')$ . Using again that  $s_1$  commutes with  $\text{sh}^2(f')$  and  $s_1^2 = 1$ , we find

$$f \triangleright g = \text{sh}(f') s_1 \text{sh}^2(g') s_1 s_2 \text{sh}^2(f')^{-1} = \text{sh}(f') \text{sh}^2(g') s_2 \text{sh}^2(f')^{-1},$$

explicitly of class 1. Finally, assume that  $f$  has class 2, say  $f = \text{sh}(f')s_1$ , and  $g$  has class 2, say  $g = \text{sh}(g')s_1$ . Using now  $s_1 s_2 s_1 s_2 = s_2 s_1$ , we find

$$f \triangleright g = \text{sh}(f') s_1 \text{sh}^2(g') s_2 s_1 s_2 \text{sh}^2(f')^{-1} = \text{sh}(f') \text{sh}^2(g') s_2 \text{sh}^2(f')^{-1} s_1,$$

of class 1. Thus, applying  $\triangleright$  to permutations in  $\mathfrak{S}_\infty^{\text{sm}}$  yields permutations in  $\mathfrak{S}_\infty^{\text{sm}}$ , that is,  $\mathfrak{S}_\infty^{\text{sm}}$  is closed under  $\triangleright$ . Because  $\text{id}$  belongs to  $\mathfrak{S}_\infty^{\text{sm}}$  (it has class 1), the substructure of  $(\mathfrak{S}_\infty, \triangleright)$  generated by  $\text{id}$ , which is  $\mathfrak{S}_\infty^{\text{sp}}$ , is included in  $\mathfrak{S}_\infty^{\text{sm}}$ .

(ii) Let  $\equiv$  denote class equality on  $\mathfrak{S}_\infty^{\text{sm}}$ . The above three computations show that  $\equiv$  is compatible with the operation  $\triangleright$ , and that the table of  $\mathfrak{S}_\infty^{\text{sm}}/\equiv$  coincides with that of the Laver table  $A_1$ , as displayed in Fig. 6.  $\square$

Composing with the projection of braids to permutations, we deduce a partial answer to Question 4.7 in the case of  $A_1$ :

**Corollary 4.9.** *Call a braid  $\beta$  of class  $n$  if, in any braid diagram representing  $\beta$ , the strand starting at position 1 finishes at position  $n$ . Let  $B_\infty^{\text{sm}} := \{\beta \in B_\infty \mid \text{cl}(\beta) \leq 2\}$ . Then  $B_\infty^{\text{sm}}$  is closed under  $\triangleright$  and includes  $B_\infty^{\text{sp}}$ . Class equality is a congruence on  $(B_\infty^{\text{sm}}, \triangleright)$  and  $(B_\infty^{\text{sp}}, \triangleright)$ , and the quotient is the Laver table  $A_1$ .*

This answer is not fully satisfactory, in that the considered equivalence relation is defined only on a proper subset of  $B_\infty$ , namely  $B_\infty^{\text{sm}}$ . However, the situation with  $A_2$  is worse:

**Fact 4.10.** *There is no congruence on  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  such that the quotient is isomorphic to a Laver table  $A_n$  with  $n \geq 2$ .*

*Proof.* As  $A_2$  is a quotient of every table  $A_n$  with  $n \geq 2$ , it suffices to consider  $A_2$ . Assume that  $\phi$  is a morphism from  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  to  $A_2$ . As  $\text{id}$  is the unique generator of  $(\mathfrak{S}_\infty^{\text{sp}}, \triangleright)$  and 1 is the unique generator of  $A_2$ , we necessarily have  $\phi(\text{id}) = 1$ . Now, we see on Fig. 6 that, in  $A_2$ , we have  $1 \triangleright 3 = 2$  and  $3 \triangleright 2 = 4$ , hence

$$(4.5) \quad 1 \triangleright 1_{[3]} \neq 1_{[3]} \triangleright 1_{[2]},$$

whereas, in  $\mathfrak{S}_\infty^{\text{sp}}$ , we read in Fig. 5

$$(4.6) \quad \text{id} \triangleright \text{id}_{[3]} = s_3 s_1 = \text{id}_{[3]} \triangleright \text{id}_{[2]} :$$

this contradicts the assumption that  $\phi$  is a homomorphism.  $\square$

The above fact does not prove that there is no answer to Question 4.7, but it shows that, for  $n \geq 2$ , the relation  $\equiv_n$  cannot be defined in terms of the associated permutations. It might be interesting to try further quotients of the braid groups [12], or linear representations. Typically, considering the Burau representation of Section 4.2 leads to

**Question 4.11 (Burau).** *Is the Laver table  $A_2$  a quotient of  $(\text{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$ ?*

At the least, writing  $I$  for the identity matrix, one checks  $I \triangleright I_{[3]} \neq I_{[3]} \triangleright I_{[2]}$ , so the obstruction (4.6) in  $\mathfrak{S}_\infty$  vanishes in  $\text{GL}_\infty(\mathbb{Z}[t, t^{-1}])$ .

## 5. EXTENSIONS

We conclude with hints about extensions of the braid operation  $\triangleright$  to larger structures. In Subsection 5.1, we describe the group  $CB_\infty$  of charged braids, a natural extension of  $B_\infty$ , in which extra space enables one to realize free shelves on any number of generators. Next, in Subsection 5.2, we describe the monoid  $EB_\infty$  of extended braids, in which a second, associative operation exists beside the selfdistributive one. Finally, we mention in Subsection 5.3 the group of parenthesized braids  $B_\bullet$ , also called the braided Thompson group  $\widehat{BV}$ , another extension of  $B_\infty$  equipped with a selfdistributive operation.

**5.1. Charged braids.** By Prop. 3.7, every braid generates under the selfdistributive operation  $\triangleright$  a substructure that is a free monogenerated left-shelf. Plenty of space is left aside: for instance, we saw that no generator  $\sigma_i$  with  $i \geq 2$  belongs to the substructure  $B_\infty^{\text{sp}}$  generated by 1.

**Question 5.1 (free family).** *Does  $(B_\infty, \triangleright)$  include a free left-shelf of rank 2, that is, does there exist a cardinal 2 free family in  $(B_\infty, \triangleright)$  (in the sense of Def. 3.3)?*

A negative answer is likely. Indeed, one can show [18] that, for all  $\beta_1, \beta_2, \beta$  in  $B_\infty$  such that  $\beta$  is special,  $\beta_1 \triangleright \beta^{[m]} = \beta_2 \triangleright \beta^{[m]}$  holds for  $m$  large enough, whereas, if  $\{\beta_1, \beta_2\}$  is free in  $(B_\infty, \triangleright)$ , then  $\beta_1 \triangleright \beta = \beta_2 \triangleright \beta$  holds for no  $\beta$  in  $\langle \beta_1, \beta_2 \rangle$ . Therefore, if  $\{\beta_1, \beta_2\}$  is a free family, the subshelf  $\langle \beta_1, \beta_2 \rangle$  generated by  $\beta_1$  and  $\beta_2$  contains no special braid. So, in particular, there exists no braid  $\beta$  such that  $\{1, \beta\}$  is free.

In order to possibly construct a braid realization for free left-shelves of rank larger than 1, it is therefore natural to introduce extensions of  $B_\infty$  in which enough space is explicitly granted. A first solution was described by D. Larue in [44] using a (very large) algebraic extension. Here we briefly mention the alternative solution of [16], which is simpler and admits a natural topological description.

**Definition 5.2 (charged braids).** For  $n \geq 1$ , we let  $CB_n$  be the extension of  $B_n$  obtained by adding mutually commuting elements  $\rho_1, \dots, \rho_n$  subject to the relations

$$(5.1) \quad \sigma_i \rho_j = \rho_j \sigma_i \quad \text{for } j < i \text{ or } j \geq i + 2, \quad \sigma_i \rho_i \rho_{i+1} = \rho_i \rho_{i+1} \sigma_i.$$

In topological terms,  $CB_n$  is the group of isotopy classes of enhanced braid diagrams, in which the strands wear integer-valued charges and  $\rho_i$  corresponds to adding an elementary charge +1 on the  $i$ th strand, see Fig. 7. The rule is that charges freely move on the strands, but a charge on the  $i$ th strand may move through a crossing  $\sigma_i^{\pm 1}$  if, and only if, a similar charge on the  $(i + 1)$ st strand simultaneously does, see Fig. 7.

The group  $B_n$  embeds in  $CB_n$ . On the other hand, erasing charges, that is, collapsing all generators  $\rho_i$  defines a projection  $\pi_n$  from  $CB_n$  to  $B_n$ , which is a retraction of the embedding. Note that  $\text{Ker}(\pi_n)$  is, already for  $n = 2$ , quite big: mapping an even length sequence of integers  $(e_0, \dots, e_{2\ell}, e)$  to

$$\rho_1^{e_0} \sigma_1 \rho_1^{e_1} \sigma_1^{-1} \rho_1^{e_2} \sigma_1 \rho_1^{e_3} \sigma_1^{-1} \dots \sigma_1^{-1} \rho_1^{e_{2\ell}} \rho_2^e$$

produces pairwise distinct elements of  $\text{Ker}(\pi_2)$  since the only eligible relations consist in moving the final  $\rho_2^e$  and shifting some  $\rho_1^{e_i}$  accordingly.

We denote by  $CB_\infty$  the direct limit of the groups  $CB_n$  when  $n$  grows to infinity.

**Proposition 5.3 (charged braid shelf).** *Extend the operation  $\triangleright$  from  $B_\infty$  to  $CB_\infty$  by defining  $\text{sh}(\rho_i) := \rho_{i+1}$  for every  $i$  and keeping (2.3). Then  $(CB_\infty, \triangleright)$  is a left-shelf, and, for every  $n \geq 2$ , the family  $\{1, \rho_1, \dots, \rho_1^{n-1}\}$  is free in  $(CB_\infty, \triangleright)$ .*

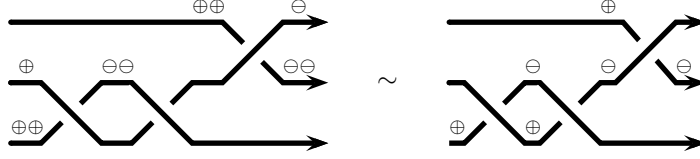


FIGURE 7. Typical charged braid diagrams, represented with  $\oplus$  on the  $i$ th strand for  $\rho_i$ , and  $\ominus$  for  $\rho_i^{-1}$ : here the diagrams encoded by  $\rho_1^2\rho_2\sigma_1\rho_2^{-2}\sigma_1\rho_3^2\sigma_2^{-1}\rho_3^{-1}\rho_2^{-2}$ , corresponding to evaluating  $(\rho_1^2 \triangleright \rho_1) \triangleright 1$  with the operation of Prop. 5.3, and the equivalent diagram  $\rho_1\sigma_1\rho_1\rho_2^{-1}\sigma_1\rho_3\rho_2^{-1}\sigma_2^{-1}\rho_2^{-1}$ , in which two initial  $\oplus$  charges have been moved rightwards through  $\sigma_1$ , one cancelling one of the  $\ominus$ , and, similarly, two final  $\ominus$  charges have been moved leftwards through  $\sigma_2^{-1}$ , one cancelling one of the  $\oplus$ .

The proof relies on extending the freeness criterion of Lemma 3.4 to rank  $\geq 2$ , which is not very hard as, essentially, free shelves of higher rank are sort of lexicographic extensions of rank 1 free shelves [19, Prop. V.6.6].

Let us mention that nothing is known about the following informal question, related to Question 5.1:

**Question 5.4 (generators).** *Does the structure  $(B_\infty, \triangleright)$  admit a natural family of generators?*

**5.2. Extended braids.** Another extension of potential interest in topology involves the monoid of “extended braids” [18]. In a number of (left) shelves  $(S, \triangleright)$ , there exists a second, associative operation  $\circ$ , admitting a unit 1 and connected with  $\triangleright$  by the mixed laws

$$(5.2) \quad (x \circ y) \triangleright z = x \triangleright (y \triangleright z), \quad x \triangleright (y \circ z) = (x \triangleright y) \circ (x \triangleright z)$$

$$(5.3) \quad x \circ y = (x \triangleright y) \circ x, \quad 1 \triangleright x = x, \quad x \triangleright 1 = 1.$$

In particular, if  $G$  is a group and  $\triangleright$  is the conjugation defined by  $x \triangleright y := xyx^{-1}$ , then the multiplication of  $G$  provides such a second operation.

Whereas the selfdistributive operation can be used to label the strands of a (braid or knot) diagram, such a second operation can be used to label the regions between the strands using the convention that crossing from left to right a strand labelled  $a$  multiplies the region label by  $a$ . Then the first law of (5.3) expresses the coherence of region and strand colourings, according to the scheme

$$(5.4) \quad \begin{array}{c} \begin{array}{c} b \qquad \qquad x \qquad \qquad a \\ \diagdown \qquad \diagup \\ \diagup \qquad \diagdown \\ a \qquad \qquad a \triangleright b \end{array} \\ b \circ x \qquad \qquad a \circ x \\ a \circ b \circ x = (a \triangleright b) \circ a \circ x \end{array}$$

It is worth noting that the first law of (5.3) and the associativity of  $\circ$  imply that the map  $(a, x) \mapsto a \circ x$  turns  $S$  into an  $S$ -module (or  $S$ -set), so the region labelling of (5.4) is a particular case of the shadow colorings from knot theory [41]. The second operation  $\circ$  can also be used to color braids with zip and unzip vertices; in this case all the mixed laws for  $\circ$  and  $\triangleright$  receive a topological meaning, appearing as algebraic distillations of R-moves for knotted graphs [3].



**5.3. Parenthesized braids.** We conclude with still another extension of the braid group  $B_\infty$  that contains an interesting selfdistributive structure, namely the braided Thompson group  $\widehat{BV}$  of [5, 6], also described as the group of parenthesized braids and denoted  $B_\bullet$  in [21].

**Proposition 5.8 (parenthesized braids).** *Let  $B_\bullet$  be the extension of  $B_\infty$  obtained by adding an infinite sequence of generators  $a_1, a_2, \dots$  subject to*

$$(5.7) \quad \sigma_{i+1}\sigma_i a_{i+1} = a_i \sigma_i \quad \text{and} \quad \sigma_i \sigma_{i+1} a_i = a_{i+1} \sigma_i \quad \text{for every } i,$$

$$(5.8) \quad \sigma_i a_j = a_j \sigma_i, \quad a_i a_{j-1} = a_j a_i, \quad \text{and} \quad a_i \sigma_{j-1} = \sigma_j a_i \quad \text{for } j \geq i + 2.$$

*Extending  $\text{sh}$  by  $\text{sh}(a_i) := a_{i+1}$  for every  $i$ , define  $\triangleright$  and  $\circ$  on  $B_\bullet$  by*

$$(5.9) \quad \beta \triangleright \gamma := \beta \cdot \text{sh}(\gamma) \cdot \sigma_1 \cdot \text{sh}(\beta)^{-1} \quad \text{and} \quad \beta \circ \gamma := \beta \cdot \text{sh}(\gamma) \cdot a_1.$$

*Then  $(B_\bullet, \triangleright)$  is a left-shelf, and  $(B_\bullet, \triangleright, \circ)$  obeys the mixed laws (5.2).*

In the (large) group  $B_\bullet$ , the elements  $\sigma_i$  generate a copy of  $B_\infty$ , whereas the elements  $a_i$  generate a copy of R. Thompson’s group  $F$  [8]. Topologically, the elements of  $B_\bullet$  can be thought of as braids in which the distance between adjacent strands need not be constant. Then  $a_i$  corresponds to moving the strand(s) at position  $i + 1$  or infinitely close to position  $i + \varepsilon$  with  $\varepsilon$  infinitely small (but not merging them: a subsequent  $a_i^{-1}$  may separate them back). It is shown in [21] and in [6] that  $B_\bullet$  is a group of right fractions for the submonoid  $B_\bullet^+$  generated by the  $\sigma_i$ s and the  $a_j$ s, and that the latter is a Zappa–Szep product of the monoids  $B_\infty^+$  and  $F^+$ . This implies that every element of  $B_\bullet$  can be expressed as  $f^{-1}\beta g$ , with  $\beta$  in  $B_\infty$  and  $f, g$  in  $F^+$ , resulting in diagrams like the one shown in Fig. 8.



FIGURE 8. Typical parenthesized braid diagram witnessing for the decomposition of  $B_\bullet^+$  as a Zappa–Szep product of  $B_\infty^+$  and  $F^+$ , here  $a_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2a_2$ : diverging, braiding, and finally merging.

The selfdistributive structure on  $B_\bullet$  is not so perfect as the one on  $EB_\infty$  in that the second operation is not associative, and the laws of (5.3) all fail in  $(B_\bullet, \triangleright, \circ)$ . However, calling  $B_\bullet^{\text{sp}}$  the closure of 1 under  $\triangleright$  and  $\circ$  in  $B_\bullet$ , one obtains decompositions of arbitrary parenthesized braids into special ones as in Prop. 3.12. From there, one can order  $B_\bullet$ , and, calling “augmented left-shelf” a left-shelf equipped with a second operation satisfying (5.2), establish that  $B_\bullet^{\text{sp}}$  is a free monogenerated augmented left-shelf [22, 28].

REFERENCES

[1] S. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001) 471–486.  
 [2] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).  
 [3] P. Blain, G. Bowlin, T. Fleming, J. Foisy, J. Hendricks & J. LaCombe, *Some results on intrinsically knotted graphs*, J. Knot Theory Ramifications **16** (2007) 749–760.



- [4] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemporary Maths AMS **78** (1988) 45–117.
- [5] M. Brin, *The algebra of strand splitting. I. A braided version of Thompson’s group V*, J. Group Th.; **10**; 2007; 757–788.
- [6] M. Brin, *The algebra of strand splitting. II. A presentation for the braid group on one strand*, Intern. J. of Algebra and Computation **16** (2006) 203–219.
- [7] S. Burckel, *The wellordering on positive braids*, J. Pure Appl. Algebra **120** (1997) 1–17.
- [8] J.W. Cannon, W.J. Floyd, & W.R. Parry, *Introductory notes on Richard Thompson’s groups*, Ens. Math. **42** (1996) 215–257.
- [9] S. Carter, *A survey of quandle ideas*, in: Introductory lectures on Knot Theory, Kauffmann and al. eds, Series on Knots and Everything vol. 46, World Scientific (2012), pages 22–53.
- [10] J.S. Carter, S. Kamada, & M. Saito, *Geometric interpretations of quandle homology*, J. Knot Theory Ramifications **10** (2001) 345–386.
- [11] J.S. Carter, D. Jelsovsky, S. Kamada, L. Langford, & M. Saito, *Quandle cohomology and state-sum invariants of knotted curves and surfaces*, Trans. Amer. Math. Soc. **355**(10) (2003) 3947–3989.
- [12] H.M.S. Coxeter, *Factor groups of the braid group*, Proc. 4th Canad. Math. Cong. (1959) 95–122.
- [13] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345** (1994) 115–151.
- [14] P. Dehornoy, *A normal form for the free left distributive law*, Internat J. Algebra Comput. **4** (1994) 499–528.
- [15] P. Dehornoy, *Weak faithfulness properties for the Burau representation*, Topology and its Applic **69** (1996) 121–143.
- [16] P. Dehornoy, *Construction of left distributive operations and charged braids*, Internat J. Algebra Comput. **10** (2000) 173–190.
- [17] P. Dehornoy, *A fast method for comparing braids*, Adv. Math. **125** (1997) 200–235.
- [18] P. Dehornoy, *Strange questions about braids*, J. Knot Theory Ramifications **8** (1999) 589–620.
- [19] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser (2000).
- [20] P. Dehornoy, *Geometric presentations of Thompson’s groups*, J. Pure Appl. Algebra **203** (2005) 1–44.
- [21] P. Dehornoy, *The group of parenthesized braids*, Adv. Math. **205** (2006) 354–409.
- [22] P. Dehornoy, *Free augmented LD-systems*, J. Algebra & Appl. **6** (2007) 173–187.
- [23] P. Dehornoy, *Using shifted conjugacy in braid-based cryptography*, Contemp. Math. **418** (2006) 65–73.
- [24] P. Dehornoy, *The subword reversing method*, Internat. J. Algebra Comput. **21** (2011) 71–118.
- [25] P. Dehornoy, *La thorie des ensembles*, Calvage & Mounet (2017).
- [26] P. Dehornoy, *Some aspects of the SD-world*, Proc. 4th Milehigh conference, Denver (2017), Contemp. Math., submitted, arXiv:1711.09792.
- [27] P. Dehornoy, with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braids*, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc. (2008).
- [28] P. Dehornoy and V. van Oostrom, *Using groups for investigating rewrite systems*, Math. Struct. in Comp. Sci. **18** (2008) 1133–1167.
- [29] R. Dougherty, *Critical points in an algebra of elementary embeddings*, Ann. P. Appl. Logic **65** (1993) 211–241.
- [30] R. Dougherty & T. Jech, *Finite left-distributive algebras and embedding algebras*, Adv. Math. **130** (1997) 201–241.
- [31] A. Drápal, *Finite left distributive algebras with one generator*, J. Pure Appl. Algebra **121** (1997) 233–251.
- [32] A. Drápal, *Finite left distributive groupoids with one generator*, Int. J. for Algebra Computation **7** (1997) 723–748.
- [33] A. Drápal, *About Laver tables*, Proc. 4th Milehigh conference, Denver (2017), Contemp. Math., to appear.
- [34] R. Fenn, C.P. Rourke, and B. Sanderson, *James bundles and applications* , <http://www.maths.warwick.ac.uk/~cpr/ftp/james.ps>.
- [35] J. Fromentin, *The well ordering on dual braid monoids*, J. Knot Theory Ramifications **19** (2010) 631–654.

- [36] J. Fromentin, *Every braid admits a short sigma-definite expression*, J. Europ. Math. Soc. **13** (2011) 1591–1631.
- [37] J. Fromentin and L. Paris, *A simple algorithm for finding short sigma-definite representatives*, J. Algebra **350** (2012) 405–415.
- [38] T. Jech, *Large ordinals*, Adv. Math. **125** (1997) 155–170.
- [39] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. of Pure and Appl. Algebra **23** (1982) 37–65;
- [40] A. Kalka, E. Liberman & M. Teicher, *Note on the shifted conjugacy problem in braid groups*, Groups-Complexity-Cryptology **1** (2009) 227–230.
- [41] S. Kamada, *Knot invariants derived from quandles and racks*, Geometry & Topology Monographs vol. 4: Invariants of knots and 3-manifolds (Kyoto 2001), pp. 103–117.
- [42] D. Krammer, *Braid groups are linear*, Ann. Math. **151** (2002) 131–156.
- [43] D.M. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994) 104–112.
- [44] D.M. Larue, *Left-distributive and left-distributive idempotent algebras*, Ph D Thesis, University of Colorado, Boulder (1994).
- [45] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. **91** (1992) 209–231.
- [46] R. Laver, *A division algorithm for the free left distributive algebra*, Oikkonen & al. eds, Logic Colloquium '90, Lect. Notes Logic **2** (1993) 155–162.
- [47] R. Laver, *On the algebra of elementary embeddings of a rank into itself*, Adv. Math. **110** (1995) 334–346.
- [48] D. Long & M. Paton, *The Burau representation is not faithful for  $n \geq 6$* , Topology **32** (1993) 439–447.
- [49] J. Longrigg & A. Ushakov, *Cryptanalysis of shifted conjugacy authentication protocol*, J. Math. Cryptology **2** (2008) 107–114.
- [50] A. Mathas, *Iwahori-Hecke algebras and Schur algebras of the symmetric group*, Univ. Lect. Ser. vol.15, Amer. Math. Soc. (1999)
- [51] S.V. Matveev, *Distributive groupoids in knot theory*, Math. Sbornik **119** (1982) 73–83.
- [52] J.T. Moore, *Fast growth in the Følner function for Thompson's group  $F$* , Groups Geom. Dyn. **7** (2013) 633–651.
- [53] M. Smedberg, *A dense family of well-behaved finite monogenerated left-distributive groupoids*, Arch. Math. Logic **52** (2013) 377–402.