THE BRAID SHELF

Patrick Dehornoy

THE BRAID SHELF

PATRICK DEHORNOY

Abstract. The braids of B_∞ 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_∞, 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_∞ 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_∞, 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, parenthesied 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_∞. 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_∞.

The selfdistributivity law comes in two versions:

(LD) *left* selfdistributivity: $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$,

(RD) *right* selfdistributivity: $(x \triangleleft y) \triangleleft z = (x \triangleleft z) \triangleleft (y \triangleleft z)$.

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 mth *right* and *left* powers of a inductively defined by

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

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

$$\left\langle \sigma_1, ..., \sigma_{n-1} \;\middle|\; \begin{array}{lll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{for} & |i-j| \geqslant 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{for} & |i-j| = 1 \end{array} \right\rangle. \tag{2.2}$$

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

From the presentation, it is clear that mapping σ_i to σ_{i+1} for every i defines an endomorphism sh of B_∞, hereafter called the *shift* endomorphism. Note that sh is not surjective: σ_1 does not lie in $\mathsf{Im}(\mathsf{sh})$.

Definition 2.2 (shifted conjugation). For β_1, β_2 in B_∞, we put

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

The braid $\beta_1 \triangleright \beta_2$ is a sort of conjugate of β_2 under β_1, but with shifts and an additional factor σ_1 added, see Fig. 1. The reader can check the values

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

and, more generally, $1^{[m]} = \sigma_{m-1}\cdots\sigma_2\sigma_1$ for every $m \geqslant 1$. 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_∞ only, and it induces no well-defined operation on B_n for any finite n.

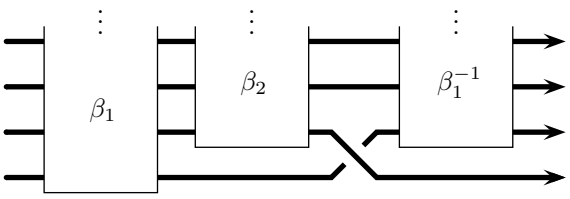


FIGURE 1. Braid diagram for $\beta_1 \triangleright \beta_2$: a sort of conjugation of β_2 under β_1, with shifts and one σ_1 added.

Our interest in the operation $\triangleright$ on B_∞ 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 $\beta_1, \beta_2, \beta_3$

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

As σ_1 commutes with every braid in $\mathsf{Im}(\mathsf{sh}^2)$ and $\sigma_1\sigma_2\sigma_1\sigma_2^{-1} = \sigma_2\sigma_1$ holds, we find $\beta_1 \triangleright (\beta_2 \triangleright \beta_3) = (\beta_1 \triangleright \beta_2) \triangleright (\beta_1 \triangleright \beta_3) = \beta_1 \cdot \mathsf{sh}(\beta_2) \cdot \mathsf{sh}^2(\beta_3) \cdot \sigma_2\sigma_1 \cdot \mathsf{sh}^2(\beta_2)^{-1} \cdot \mathsf{sh}(\beta_1)^{-1}$, 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

$$\beta \neq \beta \triangleright \beta, \tag{2.4}$$

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

On the other hand, we have $1 \triangleright \beta = \mathsf{sh}(\beta)\,\sigma_1$. As σ_1 does not belong to the image of 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. □

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

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

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_{LD} generated by an infinite family of elements LD_α indexed by finite sequences of 0s and 1s and subject to an explicit list of relations $\mathsf{Rel}_{\mathrm{LD}}$. 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

$$g^{[n+1]} = a \triangleright g^{[n]} \tag{2.6}$$

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

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

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_{LD}. From there, the four equalities in (2.7) are encoded in a product of four elements in G_{LD}, and they correspond to defining on G_{LD} a binary operation $*$ by

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

where sh_1 is the endomorphism that maps each element LD_α to $\mathrm{LD}_{1\alpha}$ (appending an initial 1 in the finite sequence α). The operation $*$ on G_{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 sh_0 that maps LD_α to $\mathrm{LD}_{0\alpha}$ for each α. As a consequence, when the subgroup $\mathsf{sh}_0(G_{\mathrm{LD}})$ is collapsed, the operation $*$ on G_{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 $G_{\mathrm{LD}}/\mathsf{sh}_0(G_{\mathrm{LD}})$ is (isomorphic to) the braid group B_∞, and that the operation induced by $*$ on B_∞ is the operation $\triangleright$ of (2.3). More precisely, collapsing $\mathsf{sh}_0(G_{\mathrm{LD}})$ amounts to collapsing all elements LD_α such that α contains 0. All relations of $\mathsf{Rel}_{\mathrm{LD}}$ then become trivial, except the following ones:

$$\mathrm{LD}_{1^i}\,\mathrm{LD}_{1^j}\,\mathrm{LD}_{1^i} = \mathrm{LD}_{1^j}\,\mathrm{LD}_{1^i}\,\mathrm{LD}_{1^j}\,\mathrm{LD}_{1^i 0} \qquad \text{for } j = i+1 \geqslant 1$$
$$\mathrm{LD}_{1^i}\,\mathrm{LD}_{1^j} = \mathrm{LD}_{1^j}\,\mathrm{LD}_{1^i} \qquad \text{for } j \geqslant i+2 \geqslant 2.$$

Then collapsing $\mathrm{LD}_{1^i 0}$ and mapping LD_{1^i} to σ_{i+1} defines the expected epimorphism from G_{LD} onto B_∞. Then (2.8) projects to (2.3), since sh_1 projects to sh, and $\mathrm{LD}_\emptyset$ is mapped to σ_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 β, the left translation L_β is injective, that is, $(B_\infty, \triangleright)$ is left cancellative.*

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

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

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

whence $\mathsf{sh}(\gamma) = \mathsf{sh}(\gamma')$ as cancellation is legal in the group B_∞. This implies $\gamma = \gamma'$, as 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 β in B_∞,

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

Indeed, if β belongs to the image of sh, then $\mathsf{sh}(\beta)$ belongs to the image of sh^2, hence it commutes with σ_1 in the group B_∞. Conversely, for every β in B_n, the handle trick of Fig. 2 gives

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

So, if $\mathsf{sh}(b)$ and σ_1 commute, we obtain $\beta = \sigma_n^{-1} \dots \sigma_2^{-1}\, \mathsf{sh}(\beta)\, \sigma_2 \cdots \sigma_n$, which belongs to $\mathsf{sh}(B_\infty)$ explicitly.

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

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

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

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

which expresses that $\mathsf{sh}(\beta^{-1}\, \gamma\, \mathsf{sh}(\beta)\, \sigma_1^{-1})$ and σ_1 commute. By (2.9), this implies that $\beta^{-1}\, \gamma\, \mathsf{sh}(\beta)\, \sigma_1^{-1}$ belongs to $\mathsf{sh}(B_\infty)$, hence there exists β' satisfying $\beta^{-1}\, \gamma\, \mathsf{sh}(\beta)\, \sigma_1^{-1} = \mathsf{sh}(\beta')$. The latter equality is $\gamma = \beta \triangleright \beta'$. Hence, γ lies in the image of the left translation L_β. □

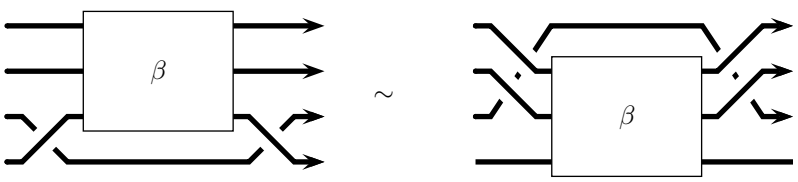


FIGURE 2. The handle trick.

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 β of B_∞ 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

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

Assume $\beta \in B_n$. Then β 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 $\sigma_n \cdots \sigma_1 \cdot \mathsf{sh}(\beta)$, implying $\beta \triangleright 1^{[n]} = 1^{[n+1]}$.

Conversely, assume $\beta \notin B_n$. Let $m > n$ be minimal such that β belongs to B_m. By [17], we know that β admits an expression where exactly one of σ_{m-1}, σ_{m-1}^{-1} occurs. It follows that $\mathsf{sh}(\beta)$ has an expression where exactly one of σ_m, σ_m^{-1} occurs, and the same holds for $\beta \cdot 1^{[n+1]} \cdot \mathsf{sh}(\beta)^{-1} \cdot (1^{[n+1]})^{-1}$, since β, $1^{[n+1]}$, 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. □

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 $\overline{\triangleright}$ for the inverse operation so that $a \triangleright b = c$ is equivalent to $a \overline{\triangleright} c = b$, it is well known that the formulas

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

$$(a_1, ..., a_n) \bullet \sigma_i^{-1} = (a_1, ..., a_{i-1}, a_{i+1}, a_{i+1} \mathbin{\overline{\triangleright}} a_i, a_{i+2}, ..., a_n) \tag{2.11}$$

define an action of B_n on S^n. This action can be described in terms of strand colorings: for β 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 β 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 σ_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 $\overline{\triangleright}$ for the *partial* operation on S such that $a \triangleright b = c$ is equivalent to $a \overline{\triangleright} c = b$ *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]):

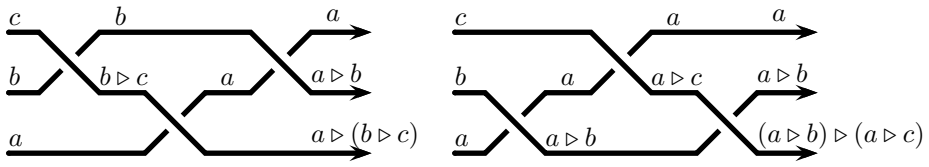


FIGURE 3. Standard translation of Reidemeister III move into the language of selfdistributivity: when colours from a set S are put on the left ends of the strands and then propagated so that a b-coloured strand becomes $a \triangleright b$-coloured when it overcrosses an a-coloured arc, then the output 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 $w, ..., w_p$, there exists a sequence $\vec{a}$ in S^n such that $\vec{a} \bullet w_i$ is defined for every i;*

(ii) *If w and w' represent the same braid of B_∞ and both $\vec{a} \bullet w$ and $\vec{a} \bullet w'$ are defined, then they are equal.*

In the above context, $\vec{a} \bullet \beta$ can be unambiguously defined to be $\vec{a} \bullet w$ for any word w such that w represents β and $\vec{a} \bullet w$ 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_∞^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 $(\beta_1, ..., \beta_n)$ in B_∞^n, define*

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

Then, for all $(\beta_1, ..., \beta_n)$ in B_∞^n and β in B_n^+, we have

$$\prod^{\mathsf{sh}}((\beta_1, ..., \beta_n) \bullet \beta) = \prod^{\mathsf{sh}}(\beta_1, ..., \beta_n) \cdot \beta. \tag{2.13}$$

Proof. For an induction, it suffices to consider the case $\beta = \sigma_i$. Next, because the action of σ_i keeps the first $i-1$ entries fixed and is a shifting of the action of σ_1, it is even sufficient to consider the case $\beta = \sigma_1$. For $n = 2$, we find

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

Finally, going from $n = 2$ to $n \geqslant 3$ amounts to append some entries $\mathsf{sh}^{j-1}(\beta_j)$ with $j \geqslant 3$ on the right of the shifted products. These entries are invariant under the action of σ_1, and σ_1 commutes with all of them, so (2.13) remains valid. □

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 β 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 ϕ 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*

$$a \sqsubset^* a \triangleright b, \qquad \text{and} \qquad b \sqsubset^* c \;\Leftrightarrow\; a \triangleright b \sqsubset^* a \triangleright c. \tag{3.1}$$

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

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

which in turn implies in the left-shelf S

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

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

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

Lemma 3.5 (σ_1**-positivity).** *Call a braid* σ_1-positive *if it admits at least one expression in which the letter* σ_1 *occurs and no letter* σ_1^{-1} *does. Then, for all braids* β, β'*, the relation* $\beta \sqsubset^* \beta'$ *in* B_∞ *implies that* $\beta^{-1}\beta'$ *is* σ_1*-positive.*

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

$$(\cdots ((\beta \triangleright \beta_1) \triangleright \beta_2) \cdots) \triangleright \beta_n = \beta'. \tag{3.2}$$

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

$$\beta^{-1}\beta' = \mathsf{sh}(\gamma_0)\, \sigma_1\, \mathsf{sh}(\gamma_1)\, \sigma_1 \ \cdots\ \sigma_1\, \mathsf{sh}(\gamma_n), \tag{3.3}$$

where the right hand term is explicitly σ_1-positive. □

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 σ_1-positive braid that is trivial (equal to 1). Hence, for excluding (3.2), it suffices to prove that a σ_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_∞ in $\mathsf{Aut}(F_\infty)$, where F_∞ is a free group based on an infinite family $\{x_i \mid i \geqslant 1\}$,

identified with the family of freely reduced words on $\{x_i^{\pm 1} \mid i \geqslant 1\}$. 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 γ is a σ_1-positive braid, then $\rho(\gamma)$ maps x_1 to a reduced word that finishes with the letter x_1^{-1} and, therefore, γ cannot be trivial, since $\rho(1)$ maps x_1 to x_1, which does not finish with x_1^{-1}. □

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

Proposition 3.7 (free). *For every braid β, the substructure $\langle\beta\rangle$ of $(B_\infty, \triangleright)$ generated by β 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_∞ sending every element to the braid 1 extends to a morphism π from $(S, \triangleright)$ to $(B_\infty, \triangleright)$. Then the image under π of a cycle for $\sqsubset$ in S would be a cycle for $\sqsubset$ in B_∞. By Lemma 3.6, such a cycle cannot exist. □

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_∞^{sp} the closure of $\{1\}$ in $(B_\infty, \triangleright)$. The elements of B_∞^{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 $\mathsf{Term}_\triangleright(x)$ in $(B_\infty, \triangleright)$. For instance, 1, σ_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 σ_i is not special for $i \geqslant 2$.

Let us begin with a closure property of B_∞^{sp}.

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

Proof (sketch). By the easy direction of Prop. 2.5, the existence of β' in B_∞ satisfying $\beta \triangleright \beta' = \gamma$ implies $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$ in B_∞, hence in B_∞^{sp}. Conversely, it is known that, since $(B_\infty^{\mathsf{sp}}, \triangleright)$ is a free monogenerated left-shelf, $\beta \triangleright \gamma = \beta^{[2]} \triangleright \gamma$ implies the existence in B_∞^{sp} of β'' 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 $\beta' \in B_\infty^{\mathsf{sp}}$. □

As it is a substructure of $(B_\infty, \triangleright)$, the structure $(B_\infty^{\mathsf{sp}}, \triangleright)$ 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 $(B_\infty^{\mathsf{sp}})^n$, and a partial action of B_n on $(B_\infty^{\mathsf{sp}})^n$. 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 β is special if, and only if, $(1,1,1,\cdots)\bullet\beta$ exists and is equal to $(\beta,1,1,\cdots)$.*

Proof. First, we inductively show that the condition is satisfied for every special braid β. It is obvious for $\beta=1$. For $\beta=\beta_1\triangleright\beta_2$ with β_1,β_2 special, we find

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

For the last step, the induction hypothesis for β_1 implies that $(1,1,1,\cdots)\bullet\beta_1$ is defined and equal to $(\beta_1,1,1,\cdots)$. By reversing the diagram, we deduce that that $(\beta_1,1,1,\cdots)\bullet\beta_1^{-1}$ is defined and equal to $(1,1,\cdots)$, and, from there, that $(\beta,\beta_1,1,1,\cdots)\bullet\mathsf{sh}(\beta_1)^{-1}$ is defined and equal to $(\beta,1,1,\cdots)$, as expected.

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

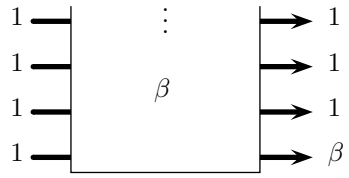


FIGURE 4. A special braid is a braid that produces itself using braid coloring and starting from unit braids.

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 β in B_n^+, there is a unique sequence of special braids $\beta_1,...,\beta_n$ satisfying*

$$\beta=\beta_1\cdot\mathsf{sh}(\beta_2)\cdot\cdots\cdot\mathsf{sh}^{n-1}(\beta_n). \tag{3.4}$$

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

$$\beta=\mathsf{sh}^{n-1}(\beta_n^{-1})\cdot\cdots\cdot\mathsf{sh}(\beta_2^{-1})\cdot{\beta_1}^{-1}\cdot\beta'_1\cdot\mathsf{sh}(\beta'_2)\cdot\cdots\cdot\mathsf{sh}^{n-1}(\beta'_n). \tag{3.5}$$

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

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

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

whence, repeating the argument,

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

which is $(1,1,1,\cdots)\bullet\beta=(\beta'_1,...,\beta'_n)$. It follows that $(\beta'_1,...,\beta'_n)$ must be the result of the action of β on $(1,1,1,\cdots)$, 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 β',β'' in B_n^+. The result then follows from applying (i) to β' and β''. □

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

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

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

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

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

Remark 3.14. For β in B_n^+, Prop. 3.12 gives $\beta=\beta_1\,\mathsf{sh}(\beta_2)\cdots\mathsf{sh}^{n-1}(\beta_n)$ with $\beta_1,...,\beta_n$ special. However, the braids β_i need not lie in B_n: for instance, the decomposition of σ_1^2, a braid of B_2, is $(\sigma_1^2\sigma_2^{-1})\,\mathsf{sh}(\sigma_1)$, 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 $(1,1,1,\cdots)\bullet uv^{-1}$. 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_∞^+ 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 $(\beta,1,1,\cdots)$, 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 $(1,1,1,\cdots)\bullet uv^{-1}$ in terms of 1 and $\triangleright$. □

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 σ_1^2, and v is σ_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 β is positive and special of length m. We use induction on m. For $m = 0$, the only possibility is $\beta = 1 = 1^{[1]}$. Assume $m \geqslant 1$, and write $\beta = \beta'\sigma_i$. By Lemma 3.11, the assumption that β is special implies the equality $(1, 1, 1, \cdots) \bullet \beta = (\beta, 1, 1, \dots)$. Since β' is positive, $(1, 1, \cdots) \bullet \beta'$ exists. Call it $(\beta'_1, \beta'_2, \cdots)$. If we had $i \geqslant 2$, the ith entry in $(1, 1, \cdots) \bullet \beta'\sigma_i$ would be $\beta'_i \triangleright \beta'_{i+1}$, which cannot be 1. Thus we must have $i = 1$, whence $\beta = \beta'_1 \triangleright \beta'_2$, $\beta'_1 = \beta'_3 = \cdots = 1$, that is, $(1, 1, \cdots) \bullet \beta' = (1, \beta'_2, 1, 1, \cdots)$. By (3.4), we deduce $\beta' = \mathsf{sh}(\beta'_2)$. Hence β'_2 is positive and special. The induction hypothesis implies $\beta'_2 = 1^{[m]}$, and we deduce $\beta = 1 \triangleright 1^{[m]} = 1^{[m+1]}$. □

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

Proof. Assume $\beta = \prod^{\mathsf{sh}}(\beta_1, ..., \beta_n)$ with $\beta_1, ..., \beta_n$ special and positive. Then, as seen in the proof of Prop. 3.12, $(1, 1, 1, \cdots) \bullet \beta$ is defined and equal to $(\beta_1, \beta_2, \cdots)$. 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

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

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

Conversely, assume that β is a positive simple braid. Then it is known that β 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 β. By uniqueness, this decomposition coincides with the one associated with $(1, 1, 1, \cdots) \bullet \beta$, meaning that the entries of $(1, 1, 1, \cdots) \bullet \beta$ are the positive braids $1^{[m_i+1]}$. □

In particular, the special decomposition of Δ_n is

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

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 β 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 $c(\beta) \leqslant n$ implies $\beta \in B_n$.

Question 3.19 (**special n-strand braids**). *Is the converse true, that is, does $c(\beta) \leqslant n$ hold for every special braid β 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_∞^{sp}. As every braid admits a decomposition in terms of special braids, it is not surprising that the linear order on B_∞^{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_∞, 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 β is said to be σ_1-*positive* if it admits at least one expression where σ_1 occurs and σ_1^{-1} does not. We define σ_1-*negative* (no σ_1 and at least one σ_1^{-1}) and σ_1-*free* (no σ_1 and no σ_1^{-1}) accordingly.

Lemma 3.20 (order on special). *If β, β' are special braids, the relation $\beta \sqsubset^* \beta'$ in B_∞^{sp} is equivalent to $\beta^{-1}\beta'$ being σ_1-positive.*

Proof. We saw in Lemma 3.5 that, if $\beta \sqsubset^* \beta'$ holds in B_∞, hence in particular if $\beta \sqsubset^* \beta'$ holds in B_∞^{sp}, then $\beta^{-1}\beta'$ is σ_1-positive. Conversely, assume that β and β' are special and $\beta^{-1}\beta'$ is σ_1-positive. By Lemma 3.2, at least one of $\beta \sqsubset^* \beta'$, $\beta = \beta'$, or $\beta \sqsupset^* \beta'$ holds in B_∞^{sp}. The second option implies that $\beta^{-1}\beta'$ is trivial, hence, by Lemma 3.6, not σ_1-positive. The third option implies that $\beta'^{-1}\beta$ is σ_1-positive, which again contradicts the σ_1-positivity of $\beta^{-1}\beta'$, as the product of the σ_1-positive braids $\beta^{-1}\beta'$ and $\beta'^{-1}\beta$, which is 1, would be σ_1-positive. So $\beta \sqsubset^* \beta'$ is the only possibility. □

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

Proposition 3.21 (order). *Every braid is σ_1-positive, σ_1-negative, or σ_1-free, each possibility excluding the others.*

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

$$\beta = \mathsf{sh}^{n-1}(\beta_n^{-1}) \cdot \cdots \cdot \mathsf{sh}(\beta_2^{-1}) \cdot \beta_1^{-1} \cdot \beta'_1 \cdot \mathsf{sh}(\beta'_2) \cdot \cdots \cdot \mathsf{sh}^{n-1}(\beta'_n),$$

which has the form $\beta = \mathsf{sh}(\gamma) \cdot \beta_1^{-1}\beta'_1 \cdot \mathsf{sh}(\gamma')$. By Lemma 3.20, $\beta_1^{-1}\beta'_1$ is either σ_1-positive, in which case so is β, or equal to 1, in which case β is σ_1-free, or σ_1-negative, in which case so is β. The three cases exclude one another by Lemma 3.6. □

Remark 3.22. The previous simple argument takes place in B_∞, and does not guarantee that a braid of B_n necessarily admits a σ_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_∞.

Corollary 3.23 (order). *Say that a braid is σ_i-positive if it is the image of a σ_1-positive braid under sh^{i-1}. For β_1, β_2 in B_∞, define $\beta_1 < \beta_2$ to mean that $\beta_1^{-1}\beta_2$ is σ_i-positive for some i. Then the relation $<$ is a linear order on B_∞; it is compatible with multiplication on the left, and extends the order $\sqsubset^*$ on B_∞^{sp}.*

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

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

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

Let us return to the monoid B_∞^+. 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_∞^+ is a well-order of order type ω^{ω^ω}.*

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

Question 3.25 (Laver conjecture). *For every sequence of braids $(\beta_1, ..., \beta_n)$, is the family of all braids β for which $(\beta_1, ..., \beta_n) \bullet \beta$ 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_∞, 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 σ_i^2 are collapsed, namely the symmetric group $\mathfrak{S}_n$. Geometrically, the projection corresponds to associating with a braid β the permutation $\mathsf{perm}(\beta)$ so that, for $1 \leqslant i < n$, the strand finishing at position i begins at position $\mathsf{perm}(\beta)(i)$ in any braid diagram representing β. The projection extends to B_∞, 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 σ_i, that is, the transposition exchanging i and $i+1$. We use sh for the *shift* endomorphism of $\mathfrak{S}_\infty$ defined, for f in $\mathfrak{S}_\infty$, by $\mathsf{sh}(f)(1) := 1$ and $\mathsf{sh}(f)(n) := f(n-1)+1$ for $n \geqslant 2$.

As the operation $\triangleright$ on B_∞ is defined from the group multiplication and the endomorphism sh, every group morphism from B_∞ to a group G that carries 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*

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

Then $(\mathfrak{S}_\infty, \triangleright)$ is a left-shelf, and 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 id of $\mathbb{Z}_{>0}$.

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

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

the unit braid. One easily checks that, for every n, the right power $\mathsf{id}^{[n]}$ is the n-cycle $s_{n-1}\cdots s_2s_1$. The left powers $\mathsf{id}_{[n]}$ are more mysterious; the first values are

$$\mathsf{id}_{[2]} = s_1, \quad \mathsf{id}_{[3]} = s_2, \quad \mathsf{id}_{[4]} = s_2s_3s_1, \quad \mathsf{id}_{[5]} = s_3s_4s_2s_3s_4, \ \ldots$$

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

$\mathfrak{S}_\infty^{\mathsf{sp}}$	id	s_1	s_2	$s_2s_3s_1$	$\cdots$
id	s_1	s_2s_1	s_3s_1	$s_3s_4s_2s_1$	$\cdots$
s_1	s_2	s_2s_1	s_3s_2	$s_3s_4s_2s_1$	$\cdots$
s_2	$s_2s_3s_1$	s_3s_1	s_2s_1	$s_3s_4s_2s_3s_4s_1$	$\cdots$
$s_2s_3s_1$	$s_3s_4s_2s_3s_4$	$s_3s_4s_2s_3s_4s_1$	s_4s_3	s_3s_1	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

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

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

$$s_2s_1 = ((s_2s_1) \ \triangleright \ s_1) \ \triangleright \ s_2s_3s_1, \tag{4.2}$$

whence $s_2s_1 \sqsubset^* s_2s_1$. It follows from Corollary 3.8 that $(\mathfrak{S}_\infty^{\mathsf{sp}}, \triangleright)$ is not a free left-shelf: typically, (4.2) translates into $\mathsf{id}^{[3]} = (\mathsf{id}^{[3]} \triangleright \mathsf{id}_{[2]}) \triangleright \mathsf{id}_{[4]}$, a nontrivial relation whose counterpart fails in B_∞^{sp}.

Question 4.3 (presentation). *Does the left-shelf $(\mathfrak{S}_\infty^{\mathsf{sp}}, \triangleright)$ 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*

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

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 $\mathsf{Im}(f \triangleright g) = f(\mathsf{Im}(g)) \cup \mathsf{coIm}(f)$ and $\mathsf{coIm}(f \triangleright g) = f(\mathsf{coIm}(g))$. 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 $\mathsf{Im}(f \cdot g)$, and to n otherwise. Thus $\triangleright$ obeys the selfdistributivity law LD.

To prove that ϕ 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 $\mathsf{sh}(f) = \mathsf{sh}(f')$, whence $f = f'$, so ϕ is injective. □

By definition, the morphism ϕ of Prop. 4.4 maps the identity permutation id to the injection SH. Hence it induces an isomorphism from the left-shelf $(\mathfrak{S}_\infty^{\mathsf{sp}}, \triangleright)$ to its image, which is the substructure $\mathfrak{I}_\infty^{\mathsf{sp}}$ of $(\mathfrak{I}_\infty, \triangleright)$ generated by SH. The left-shelf $(\mathfrak{I}_\infty^{\mathsf{sp}}, \triangleright)$ is directly reminiscent of the left-shelf $\mathsf{Iter}(j)$ 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 $\widetilde{\mathrm{SH}}$ in $\mathfrak{I}_\infty$ and of a partial selfdistributive operation $\widetilde{\triangleright}$ on (a subset of) $\mathfrak{I}_\infty$ such that $\widetilde{\triangleright}$ is everywhere defined on the substructure generated by $\widetilde{\mathrm{SH}}$, and $f\,\widetilde{\triangleright}\,g(n) = f(g(f^{-1}(n)))$ holds for n in $\mathsf{lm}(f)$, but, instead of "stupidly" completing with $f \triangleright g(n) := n$ for n in $\mathsf{colm}(f)$ 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 $\widetilde{\mathrm{SH}}$ 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_∞, we have to consider the direct limit $\mathrm{GL}_\infty(\mathbb{Z}[t,t^{-1}])$ of the groups $\mathrm{GL}_n(\mathbb{Z}[t,t^{-1}])$ (identified with invertible n-matrices) with the top–left embeddings of matrices. The (unreduced) version of the representation is defined by

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

where sh is the obvious bottom–right shift of matrices.

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

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

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

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

The verification is the same as for B_∞: the point is that Σ_1 commutes with every matrix in the image of 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 $(\mathrm{GL}_\infty(\mathbb{Z}[t,t^{-1}]), \triangleright)$, implying that the Burau image of a σ_1-positive braid would never be trivial, implying in turn that ρ is injective—which is false. By the way, an example of a σ_1-positive braid (with five σ_1 and no σ_1^{-1}) whose Burau image is trivial is constructed in [15]. This corresponds to a cycle of length 5 for division in $(\mathrm{GL}_\infty(\mathbb{Z}[t,t^{-1}]), \triangleright)$.

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

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

where $\mathsf{shtr}(A)$ ("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 $\{1, ..., N\}$ that satisfies $x \triangleright 1 = x + 1 \mod N$ 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 *nth 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_0	1
1	1

A_1	1	2
1	2	2
2	1	2

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

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

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 $(B_\infty^{\mathsf{sp}}, \triangleright)$ is a free monogenerated left-shelf, there must exist for every n a congruence $\equiv_n$ on $(B_\infty^{\mathsf{sp}}, \triangleright)$ such that $B_\infty^{\mathsf{sp}}/\equiv_n$ is isomorphic to A_n.

Question 4.7 (A_n **as quotient of** B_∞**).** *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 $\mathsf{cl}(f)$ *of a permutation f in $\mathfrak{S}_\infty$ to be $f^{-1}(1)$. Let $\mathfrak{S}_\infty^{\mathsf{sm}} := \{f \in \mathfrak{S}_\infty \mid \mathsf{cl}(f) \leqslant 2\}$ (“small class” permutations).*

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

(ii) *Class equality is a congruence on the left-shelf $(\mathfrak{S}_\infty^{\mathsf{sm}}, \triangleright)$, hence on $(\mathfrak{S}_\infty^{\mathsf{sp}}, \triangleright)$. 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 $\mathsf{sh}(f')s_1 s_2 \cdots s_{n-1}$ for some f'. In particular, the elements of $\mathfrak{S}_\infty^{\mathsf{sm}}$ are of the form $\mathsf{sh}(f')$ or $\mathsf{sh}(f')s_1$.

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

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

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

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

explicitly of class 1. Finally, assume that f has class 2, say $f = \mathsf{sh}(f')s_1$, and g has class 2, say $g = \mathsf{sh}(g')s_1$. Using now $s_1s_2s_1s_2 = s_2s_1$, we find

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

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

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

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 β of class n if, in any braid diagram representing β, the strand starting at position 1 finishes at position n. Let $B_\infty^{\mathsf{sm}} := \{\beta \in B_\infty \mid \mathsf{cl}(\beta) \leqslant 2\}$. Then B_∞^{sm} is closed under $\triangleright$ and includes B_∞^{sp}. Class equality is a congruence on $(B_\infty^{\mathsf{sm}}, \triangleright)$ and $(B_\infty^{\mathsf{sp}}, \triangleright)$, 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_∞, namely B_∞^{sm}. However, the situation with A_2 is worse:

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

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

$$1 \triangleright 1_{[3]} \neq 1_{[3]} \triangleright 1_{[2]}, \tag{4.5}$$

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

$$\mathsf{id} \triangleright \mathsf{id}_{[3]} = s_3 s_1 = \mathsf{id}_{[3]} \triangleright \mathsf{id}_{[2]} : \tag{4.6}$$

this contradicts the assumption that ϕ is a homomorphism. □

The above fact does not prove that there is no answer to Question 4.7, but it shows that, for $n \geqslant 2$, 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 $(\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}]), \triangleright)$?*

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 $\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}])$.

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_∞ of charged braids, a natural extension of B_∞, 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_∞ 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_∞ 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 σ_i with $i \geqslant 2$ belongs to the substructure B_∞^{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 exists 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 β_1, β_2, β in B_∞ such that β 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 β 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 β_1 and β_2 contains no special braid. So, in particular, there exists no braid β 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_∞ 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 $n \geqslant 1$, we let CB_n be the extension of B_n obtained by adding mutually commuting elements $\rho_1, ..., \rho_n$ subject to the relations

$$\sigma_i \rho_j = \rho_j \sigma_i \quad \text{for } j < i \text{ or } j \geqslant i+2, \qquad \sigma_i \rho_i \rho_{i+1} = \rho_i \rho_{i+1} \sigma_i. \tag{5.1}$$

In topological terms, CB_n is the group of isotopy classes of enhanced braid diagrams, in which the strands wear integer-valued charges and ρ_i corresponds to adding an elementary charge $+1$ on the ith strand, see Fig. 7. The rule is that charges freely move on the strands, but a charge on the ith 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 ρ_i defines a projection π_n from CB_n to B_n, which is a retraction of the embedding. Note that $\mathsf{Ker}(\pi_n)$ is, already for $n = 2$, quite big: mapping an even length sequence of integers $(e_0, ..., e_{2\ell}, e)$ to

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

produces pairwise distinct elements of $\mathsf{Ker}(\pi_2)$ since the only eligible relations consist in moving the final ρ_2^e and shifting some $\rho_1^{e_i}$ accordingly.

We denote by CB_∞ 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_∞ to CB_∞ by defining $\mathsf{sh}(\rho_i) := \rho_{i+1}$ for every i and keeping (2.3). Then $(CB_\infty, \triangleright)$ is a left-shelf, and, for every $n \geqslant 2$, the family $\{1, \rho_1, ..., \rho_1^{n-1}\}$ is free in $(CB_\infty, \triangleright)$.*

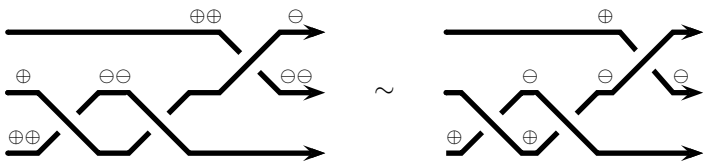


FIGURE 7. Typical charged braid diagrams, represented with $\oplus$ on the ith strand for ρ_i, and $\ominus$ for ρ_i^{-1}: here the diagrams encoded by $\rho_1^2\rho_2\sigma_1\rho_2^{-2}\sigma_1\rho_3^2\sigma_2^{-1}\rho_3^{-1}\rho_2^{-2}$, corresponding to evaluating $(\rho_1^2 \triangleright \rho_1) \triangleright 1$ 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 σ_1, one cancelling one of the $\ominus$, and, similarly, two final $\ominus$ charges have been moved leftwards through σ_2^{-1}, one cancelling one of the $\oplus$.

The proof relies on extending the freeness criterion of Lemma 3.4 to rank $\geqslant 2$, 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

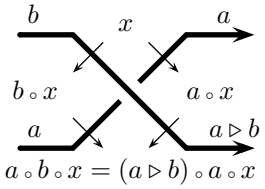
$$(x \circ y) \triangleright z = x \triangleright (y \triangleright z), \qquad x \triangleright (y \circ z) = (x \triangleright y) \circ (x \triangleright z) \tag{5.2}$$

$$x \circ y = (x \triangleright y) \circ x, \qquad 1 \triangleright x = x, \qquad x \triangleright 1 = 1. \tag{5.3}$$

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

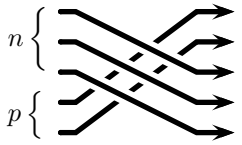
(5.4)



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].

It is therefore natural to look for a possible second operation on $(B_\infty, \triangleright)$. First, the operation $\circ$ cannot be the group multiplication, nor any group operation on B_∞, since (5.3) would then imply $x \triangleright y = x \circ y \circ x^{-1}$, which contradicts $\triangleright$ not being idempotent. Hence, the best we could expect is a monoid structure that properly extends the group structure of B_∞.

Such a structure exists, and it can be defined as a (partial) topological completion of B_∞ [18]. Hereafter, we denote by $\tau_{p,n}$ the positive braid where n strands cross over p strands. So $\tau_{p,0}$ is 1, and $\tau_{2,3}$ is shown on the right.

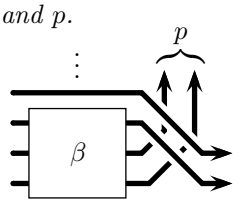


Lemma 5.5 (topology). *For β_1, β_2 in B_∞, put $d(\beta_1, \beta_2) := 0$ for $\beta_1 = \beta_2$ and $d(\beta_1, \beta_2) := 2^{-p}$ for $\beta_1^{-1}\beta_2$ in $\mathsf{lm}(\mathsf{sh}^p) \setminus \mathsf{lm}(\mathsf{sh}^{p-1})$. Then d is an ultrametric distance on B_∞. For every braid β and every p, the sequence $(\beta\tau_{p,n})_{n\geqslant 0}$ is a Cauchy sequence without limit in B_∞. Furthermore, the limits of $(\beta\tau_{p,n})_{n\geqslant 0}$ and $(\gamma\tau_{q,n})_{n\geqslant 0}$ (in a completion) coincide if, and only if, we have $p = q$ and $\beta^{-1}\gamma \in B_p$.*

The key point in the proof is the conjugation formula $\tau_{p,n}^{-1}\beta\tau_{p,n} = \mathsf{sh}^n(\beta)$, which holds for every n and every β in B_p, as a picture similar to Fig.2 shows. Using the last statement in Lemma 5.5, it is easy to describe a completion:

Proposition 5.6 (completion). *For $(\beta, p), (\gamma, q)$ in $B_\infty \times \mathbb{N}$, declare $(\beta, p) \equiv (\gamma, q)$ for $p = q$ and $\beta^{-1}\gamma \in B_p$, write $[\beta, p]$ for the $\equiv$-class of (β, q), put $d([\beta, p], [\gamma, q]) := \lim_{n\to\infty} d(\beta\tau_{p,n}, \gamma\tau_{q,n})$, and define EB_∞ to be the family of all $\equiv$-classes. Then mapping β to $[\beta, 0]$ identifies B_∞ with a dense subset of EB_∞, and the latter is obtained by adding $[\beta, p]$ as the limit of $(\beta\tau_{p,n})_{n\geqslant 0}$ for all β and p.*

The elements of EB_∞ are called "*extended braids*". The introduction of $[\beta, p]$ as the limit of the braids $\beta\tau_{p,n}$ when n goes to ∞ makes it natural to associate with the extended braid $[\beta, p]$ the diagram shown on the right, where p strands vanish at infinity.



Now the nice feature is that EB_∞ possesses a rich algebraic structure:

Proposition 5.7 (operations). *For $[\beta, p], [\gamma, q]$ in EB_∞, define*

$$[\beta, p] \cdot [\gamma, q] := [\beta \cdot \mathsf{sh}^p(\gamma), p + q], \tag{5.5}$$

$$[\beta, p] \mathbin{\widehat{\triangleright}} [\gamma, q] := [\beta \cdot \mathsf{sh}^p(\gamma) \cdot \tau_{p,q} \cdot \mathsf{sh}^q(\beta)^{-1}, q]. \tag{5.6}$$

(i) *$(EB_\infty, \cdot, 1)$ is a monoid; B_∞ is its group of units, and EB_∞ is obtained from B_∞ by adding a unique additional element, namely $\tau := [1, 1]$, subject to the relations*

$$\sigma_1\tau^2 = \tau^2 \quad \text{and} \quad \sigma_i\tau = \tau\sigma_{i-1} \quad \text{for } i \geqslant 2.$$

(ii) *$(EB_\infty, \mathbin{\widehat{\triangleright}})$ is a left-shelf; $(EB_\infty, \mathbin{\widehat{\triangleright}}, \cdot)$ obeys the mixed laws* (5.2) *and* (5.3).

Point (i) implies the equality $[\beta, p] = \beta\,\tau^p$ for all β and p. By construction, EB_∞ is the disjoint union of the groups B_∞/B_p. As B_0 and B_1 are trivial, EB_∞ includes two copies of B_∞, namely B_∞, and $B_\infty\tau := \{\beta\tau \mid \beta \in B_\infty\}$. Then the selfdistributive operation $\mathbin{\widehat{\triangleright}}$ leaves each layer B_∞/B_p stable. On B_∞, (5.6) cooks down to group conjugacy: $\beta \mathbin{\widehat{\triangleright}} \gamma = \beta\gamma\beta^{-1}$. By constrast, on the second copy $B_\infty\tau$, (5.6) yields $\beta\tau \mathbin{\widehat{\triangleright}} \gamma\tau = \beta\,\mathsf{sh}(\gamma)\,\sigma_1\,\mathsf{sh}(\beta)^{-1}\,\tau$, in which we recognize the operation $\triangleright$ of (2.3) on B_∞.

So, at the expense of embedding B_∞ into a (moderately) larger space, we obtained a complete positive solution to the initial two operations problem.

5.3. **Parenthesized braids.** We conclude with still another extension of the braid group B_∞ 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_∞ obtained by adding an infinite sequence of generators $a_1, a_2, \dots$ subject to*

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

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

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

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

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 σ_i generate a copy of B_∞, 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 ε 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 σ_is and the a_js, and that the latter is a Zappa–Szep product of the monoids B_∞^+ and F^+. This implies that every element of $B_\bullet$ can be expressed as $f^{-1}\beta g$, with β in B_∞ and f, g in F^+, resulting in diagrams like the one shown in Fig. 8.

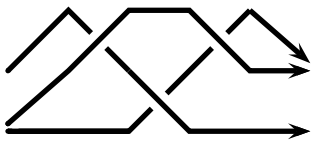


FIGURE 8. Typical parenthesized braid diagram witnessing for the decomposition of $B_\bullet^+$ as a Zappa–Szep product of B_∞^+ and F^+, here $a_1^{-1}\sigma_2^{-1}\sigma_1\sigma_2 a_2$: diverging, braiding, and finally merging.

The selfdistributive structure on $B_\bullet$ is not so perfect as the one on EB_∞ in that the second operation is not associative, and the laws of (5.3) all fail in $(B_\bullet, \triangleright, \circ)$. However, calling $B_\bullet^{\mathsf{sp}}$ 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 $B_\bullet^{\mathsf{sp}}$ 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 $n \geqslant 6$*, 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.

Laboratoire de Mathématiques Nicolas Oresme UMR 6139, Université de Caen, 14032 Caen, France, patrick.dehornoy@unicaen.fr, URL: dehornoy.users.lmno.cnrs.fr