

# Extending the Hurwitz action to shelves that are not racks

Patrick DEHORNOY  
Université de Caen, France

It is well-known that, whenever  $(S, *)$  is a rack, then putting

$$(1) \quad (x_1, \dots, x_n) \bullet \sigma_i = (x_1, \dots, x_{i-1}, x_{i+1}, x_i * x_{i+1}, x_{i+2}, \dots, x_n),$$

induces a well-defined action of the braid group  $B_n$  on  $S^n$  [1, 14]. When the operation  $*$  is the conjugacy of a group, this action is called the *Hurwitz action*, and it is natural to use the same terminology in the case of an arbitrary rack.

When  $(S, *)$  is a shelf, but not a rack, that is, if  $*$  is a right self-distributive operation on  $S$  but it is not assumed that its right translations are bijective, then the Hurwitz action of  $B_n$  on  $S^n$  is defined only for positive braids, that is, for braids that can be expressed without using any negative generator  $\sigma_i^{-1}$ . The aim of this text is to explain how this limitation can be avoided, at least in some cases, at the expense of allowing for a partial action (see precise definition below). The proofs are nontrivial and rely on a specific braid word tool called subword reversing.

The current approach was first developed in [6] and it appears (in its left counterpart version) in [12, Chapter IV], but with arguments only sketched. At the expense of resorting to some combinatorial results involving braid word equivalence, the current text gives a full exposition of the topological part of the the argument.

## 1 The Hurwitz action on a rack

A *shelf* is an algebraic structure  $(S, *)$  consisting of a set  $S$  equipped with a binary operation  $*$  that obeys the right-distributivity law

$$(2) \quad (x * y) * z = (x * z) * (y * z).$$

It is well-known that (2) is closely connected with Reidemeister moves of type III or, equivalently, with the braid relation  $\sigma_1 \sigma_2 \sigma_1 = \sigma_2 \sigma_1 \sigma_2$ . As a result, whenever  $(S, *)$  is a *shelf*, then using (1) and extending it multiplicatively provides a well-defined right action of the braid *monoid*  $B_n^+$  on the  $n$ th power  $S^n$ .

The above action, hereafter called the *Hurwitz action*, can be easily interpreted in terms of colorings of braid diagrams. By definition, an  $n$ -strand braid diagram is the concatenation of finitely many elementary  $n$ -strand diagrams corresponding to  $\sigma_i$  and  $\sigma_i^{-1}$ , and, therefore, every  $n$ -strand braid diagram is encoded in an  $n$ -strand *braid word*, namely a finite sequence of letters  $\sigma_i$  and  $\sigma_i^{-1}$ . Hereafter, it will be important to distinguish between braids and braid words: the braid group  $B_n$  admits the presentation

$$(3) \quad \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{for } |i - j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{for } |i - j| = 1 \end{array} \right\rangle,$$

which means that an  $n$ -strand braid, that is, an element of  $B_n$ , is an equivalence class of  $n$ -strand braid words: two braid words  $w, w'$  represent the same braid if, and only if, they are equivalent with respect to the least equivalence relation that is compatible with multiplication and contains the pairs listed in (3). We shall write  $[w]$  for the braid represented by a braid word  $w$ , that is, for its  $\equiv$ -equivalence class: thus  $w \equiv w'$  is equivalent to  $[w] = [w']$ . To avoid confusion between braids and braid words, we shall use the symbol  $|$  for word concatenation. Then the (obvious) connection between braid word concatenation and braid multiplication is

$$(4) \quad [w_1|w_2] = [w_1] \cdot [w_2].$$

Note that, as usual, we shall write  $\sigma_i$  both for the length-one braid word and for the braid it represents, and similarly for  $\sigma_i^{-1}$ . But we shall distinguish between, say, the braid word  $\sigma_1|\sigma_2|\sigma_1$  and the braid  $\sigma_1\sigma_2\sigma_1$  it represents.

In this framework, the Hurwitz action of braids can be visualized using braid diagram colorings. We first consider the special case of positive braid diagrams (no  $\sigma_i^{-1}$  crossing). Then the base principle (which goes back at least to Alexander) consists in putting colors from  $S$  on the left (input) ends of the strands, and propagating the colors to the right using at every crossing the rule

$$(5) \quad \begin{array}{c} y \quad \diagdown \quad x * y \\ \quad \quad \quad \diagup \\ x \quad \diagup \quad y \end{array}$$

We then look at the right (output) colors: if  $\mathbf{x}$  is the initial sequence of colors, and  $w$  is the (positive) braid word encoding the diagram — throughout the text, we use  $\mathbf{x}$  as a generic notation for sequences, and then  $x_i$  for the corresponding  $i$ th entry — then, by definition, the final sequence colors, denoted  $\mathbf{x} \cdot w$ , is defined by (1) and the induction rule

$$(6) \quad \mathbf{x} \cdot w|\sigma_i = (\mathbf{x} \cdot w) \cdot \sigma_i.$$

We then wonder this action of positive braid *words* induces a well-defined action of the braid monoid  $B_n^+$ . It is known since Garside [16] that  $B_n^+$  admits, as a monoid, the presentation (3), so the question is whether positive braid diagrams that are equivalent with respect to the relations of (3) lead to the same output colors. The (easy) answer is what explains the specific interest of shelves here:

**Proposition 1.1.** *The action of  $n$ -strand positive braid words on  $S^n$  defined in (1) induces a well-defined action of the positive braid monoid  $B_n^+$  if, and only if,  $(S, *)$  is a shelf.*

*Proof.* It is clear that, for  $|i - j| \geq 2$ , the braid words  $\sigma_i|\sigma_j$  and  $\sigma_j|\sigma_i$  act in the same way. For  $|i - j| = 1$ , the diagrams of Figure 1 show that  $\sigma_i|\sigma_j|\sigma_i$  and  $\sigma_j|\sigma_i|\sigma_j$  act in the same way precisely if, and only if, the operation  $*$  on  $S$  obeys the law (2).  $\square$

In order to extend the Hurwitz action on  $S^n$  from the monoid  $B_n^+$  to the braid group  $B_n$ , we have to define an action of  $\sigma_i^{-1}$  on sequences of colors. To lose no generality, assume that the coloring of negative crossings takes the form

$$(7) \quad \begin{array}{c} y \quad \diagdown \quad y \bar{*} x \\ \quad \quad \quad \diagup \\ x \quad \diagup \quad y \bar{*} x \end{array}$$

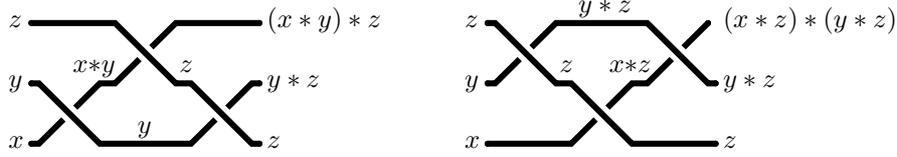


Figure 1: Whenever the operation  $*$  obeys the right-distributivity law (2), the output colors are the same when the diagrams encoded by the braid words  $\sigma_1|\sigma_2|\sigma_1$  and  $\sigma_2|\sigma_1|\sigma_2$  are colored.

where  $\bar{*}$  and  $\underline{*}$  are two new binary operations on  $S$ . Then we obtain an action of arbitrary (signed) braid words and want the latter to be invariant under the braid relations of (3)—which follows from Proposition 1.1—and under the free group relations  $\sigma_i\sigma_i^{-1} = \sigma_i^{-1}\sigma_i = 1$ .

**Lemma 1.2.** *Completing the action of (5) with (7) provides a well-defined action of the braid group  $B_n$  if, and only if, the operations  $\bar{*}$  and  $\underline{*}$  satisfy*

$$(8) \quad y \underline{*} x = x \quad \text{and} \quad (y \bar{*} x) * x = (y * x) \bar{*} x = y.$$

In this case, for every  $x$  in  $S$ , the right translation of  $*$  associated with  $x$  is a bijection, and then  $\bar{*}$  is defined from  $*$  by

$$(9) \quad y \bar{*} x = \text{the unique } y' \text{ satisfying } y' * x = y.$$

*Proof.* Expressing that, for all  $x, y$  in  $S$ , one has  $(x, y) \cdot \sigma_1|\sigma_1^{-1} = (x, y) \cdot \sigma_1^{-1}|\sigma_1 = (x, y)$  directly translates into the formulas of (8). The rest is then straightforward.  $\square$

Lemma 1.2 says that the only way to complete the definition of diagram coloring is to assume that the right translations of  $(S, *)$  are bijections and to put

$$(10) \quad \begin{array}{c} y \quad x \\ \diagdown \quad \diagup \\ x \end{array} \text{the unique } y' \text{ satisfying } y' * x = y,$$

which amounts to completing (1) with

$$(11) \quad \mathbf{x} \cdot \sigma_i^{-1} = (x_1, \dots, x_{i-1}, x', x_i, x_{i+2}, \dots, x_n), \text{ for } x' \text{ satisfying } x' * x_i = x_{i+1}.$$

In this way, we obtain the classical result:

**Proposition 1.3** (Brieskorn [1], Fenn–Rourke [14]). *Say that a shelf  $(S, *)$  is a rack if all right translations of  $*$  are bijections. Then, for every  $n$ , the relations (1) and (11) provide a well-defined action of the braid group  $B_n$  on  $S^n$ .*

Many racks are known. In particular, every group equipped with the conjugacy operation  $x * y = y^{-1}xy$  is a rack. The Hurwitz action of braids on powers of various racks leads to a number of results, in particular in terms of representations of the braid groups (Artin representation, Burau representation, etc.). In the same way as the RD-law corresponds to an invariance under Reidemeister move III, the laws of (8) correspond to an invariance under Reidemeister move II.

Going one step further, one then checks that Reidemeister move I corresponds to the idempotency law  $x * x = x$ . Therefore, if one defines a *quandle* to be an idempotent rack, one obtains an isotopy invariant [17, 20], and, from there, applications in Knot Theory, in particular using the homological approach initiated in [15] and [2]. All this is now well-known, see for instance the survey [3].

## 2 Shelves that are not racks

The above approach however is perhaps not the end of History, because there exist many racks that are not quandles, and many shelves that are not racks. Here is one typical example.

**Example 2.1.** [6] On the infinite braid group  $B_\infty$ , define

$$(12) \quad x * y = \text{sh}(y)^{-1} \cdot \sigma_1 \cdot \text{sh}(x) \cdot y,$$

where  $\text{sh} : B_\infty \rightarrow B_\infty$  is the *shift* endomorphism defined to map  $\sigma_i$  to  $\sigma_{i+1}$  for every  $i$ , see Figure 2. Once the definition (12) (which comes from the approach to self-distributivity developed in [8]) is given, it is easy to check that the operation  $*$  obeys the self-distributive law (2), that is,  $(B_\infty, *)$  is a shelf. This (remarkable) shelf is not a rack: for instance, (12) implies, for every  $x$  in  $B_\infty$ , the equality  $x * 1 = \sigma_1 \text{sh}(x)$ , whence  $x * 1 \neq 1$ , since  $\sigma_1^{-1}$  does not lie in the image of  $\text{sh}$ , which is the subgroup of  $B_\infty$  generated by  $\sigma_2, \sigma_3, \dots$ . Hence, the right translation of  $(B_\infty, *)$  associated with 1 is not surjective, and a fortiori not bijective. See [8] for more about this weird braid operation.

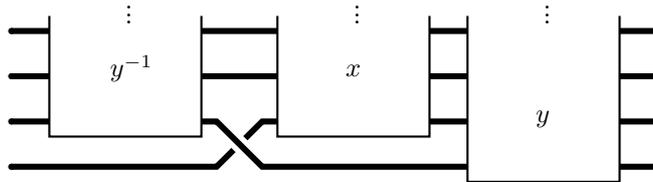


Figure 2: A “strange” self-distributive operation on the braid group  $B_\infty$  (here in its right version): on the diagram, applying the shift endomorphism  $\text{sh}$  amounts to adding one bottom unbraided strand.

In this text, we do not address the question of extending quandle tools to racks that are not quandles (for this, see [21, 22, 4, 5] among others), but we shall address the question of extending (some of) the rack tools to shelves that are not racks. More specifically, we address

**Question 2.2.** *Can one obtain a well-defined action of the group  $B_n$  on  $S^n$  when  $S$  is a shelf that is not a rack?*

Our claim is that, in spite of Lemma 1.2, a positive answer can be given, at the expense of weakening the conclusion into the existence of a *partial* action, in a sense that we shall now make precise.

Hereafter, we use  $BW_n$  (*resp.*  $BW_n^+$ ) for the (free) monoid of all  $n$ -strand braid words (*resp.* positive  $n$ -strand braid words). If  $w, w'$  are positive braid words, we write  $w \equiv^+ w'$  if  $w$  and  $w'$  represent the same element of the monoid  $BW_n^+$ , that is, if one can transform  $w$  into  $w'$  using the relations of (3) exclusively (no introduction of negative generator  $\sigma_i^{-1}$  allowed). Garside’s fundamental embedding result [16] says that  $\equiv^+$  is merely the restriction of  $\equiv$  to  $BW_n^+$ : if two positive braid words are equivalent, they are positively equivalent. With such notation, what Proposition 1.1 says is that, if  $(S, *)$  is a shelf, then, for every  $n$ , (1) defines an action of  $BW_n^+$  on  $S^n$  such that

$$(13) \quad \text{For all } \mathbf{x} \text{ in } S^n \text{ and } w, w' \text{ in } BW_n^+ \text{ satisfying } w \equiv^+ w', \text{ we have } \mathbf{x} \bullet w = \mathbf{x} \bullet w'.$$

This is the statement we shall extend.

**Definition 2.3.** A shelf  $(S, *)$  is called right-cancellative if  $x * y = x' * y$  implies  $x = x'$  for all  $x, x', y$  in  $S$ .

This is the standard notion of right-cancellativity for a set equipped with a binary operation. Racks are those racks in which right translations are both injective and surjective; in a right-cancellative shelf, we only keep half of the assumptions.

**Example 2.4.** The shelf  $(B_\infty, *)$  of Example 2.1 is not a rack, since right translations are not surjective. However, it is right-cancellative: indeed,  $x * y = x' * y$  expands into  $\text{sh}(y)^{-1} \cdot \sigma_1 \cdot \text{sh}(x) \cdot y = \text{sh}(y)^{-1} \cdot \sigma_1 \cdot \text{sh}(x') \cdot y$ , leading to  $\text{sh}(x) = \text{sh}(x')$ , whence  $x' = x$  since the shift endomorphism  $\text{sh}$  is injective.

Let us observe that, if  $(S, *)$  is a right-cancellative shelf, then (9) still makes sense when the involved element  $x'$  exists, since, given  $x$  and  $y$  in  $S$ , there exists *at most one*  $x'$  in  $S$  satisfying  $x' * y = x$ . However, there is no guarantee that such an element  $x'$  exists in general. This amounts to extending (9) into

$$(14) \quad \begin{array}{c} y \quad \diagdown \quad x \\ \quad \diagup \quad \diagdown \\ x \quad \diagup \quad \diagdown \end{array} \text{the unique } y' \text{ satisfying } y' * x = y, \text{ if it exists.}$$

In this way, we obtain a partial action of  $BW_n$  on  $S^n$ : by definition,  $\mathbf{x} \bullet u|v$  exists if and only if  $\mathbf{x} \bullet u$  and  $(\mathbf{x} \bullet u) \bullet v$  exist, and, in this case, we have  $\mathbf{x} \bullet u|v = (\mathbf{x} \bullet u) \bullet v$ . The question is whether this partial action of braid words induces a (partial) action of braids. We shall establish the following positive answer:

**Proposition 2.5.** Assume that  $(S, *)$  is a right-cancellative shelf. Then, for every  $n$ , (1) and (14) define a partial action of  $BW_n$  on  $S^n$  with the following properties:

- (15) For all  $\mathbf{x}$  in  $S^n$  and  $w$  in  $BW_n^+$ , the sequence  $\mathbf{x} \bullet w$  is defined.
- (16) For all  $w_1, \dots, w_p$  in  $BW_n$ , there exists  $\mathbf{x}$  in  $S^n$  such that  $\mathbf{x} \bullet w_k$  is defined for each  $k$ .
- (17) For all  $\mathbf{x}$  in  $S^n$  and  $w, w'$  in  $BW_n$  satisfying  $w \equiv w'$ , we have  $\mathbf{x} \bullet w = \mathbf{x} \bullet w'$  whenever the latter are defined.

Proposition 2.5 says that we obtain a well-defined partial action of  $B_n$  on  $S^n$  that extends the (total) action of  $B_n^+$  by defining  $\mathbf{x} \bullet b = \mathbf{y}$  whenever  $\mathbf{x} \bullet w = \mathbf{y}$  holds for some braid word  $w$  representing  $b$ : (17) guarantees the invariance under braid equivalence, whereas (16) ensures that, though partial, the action is nevertheless meaningful in that there always exist sequences for which it is defined.

### 3 Subword reversing

From now on, our aim is to establish Proposition 2.5. This turns out to be a nontrivial task, requiring subtle techniques involving the algebraic properties of braid monoids as investigated after Garside [16]. These techniques, based on word transformations generically called *subword reversing*, have their own interest and can be useful in a number of

situations. Here we shall survey some of their properties only (see [10] for a more complete account).

For all subsequent arguments, it is absolutely necessary to go down to the level of braid words: considering braids, that is, equivalence classes of braid words, would not enable us to control the situation precisely enough. The main idea is to introduce (proper) subrelations of the braid equivalence relation  $\equiv$ , namely two relations  $\curvearrowright$  and  $\curvearrowleft$  on braid words such that  $w \curvearrowright w'$  and  $w \curvearrowleft w'$  both imply  $w \equiv w'$ , but the converse implication need not be true in general. By very definition, the relations  $\curvearrowright$  and  $\curvearrowleft$  involve the various representatives of one braid, and their only counterpart at the level of braids is an identity.

**Definition 3.1.** [10] Assume that  $w, w'$  are braid words. We say that  $w$  is *right-reversible* to  $w'$ , written  $w \curvearrowright w'$ , if  $w'$  can be obtained from  $w$  by iteratively

- deleting a subword  $\sigma_i^{-1}|\sigma_i$ , or
- replacing a subword  $\sigma_i^{-1}|\sigma_j$  with  $|i - j| \geq 2$  by  $\sigma_j|\sigma_i^{-1}$ , or
- replacing a subword  $\sigma_i^{-1}|\sigma_j$  with  $|i - j| = 1$  by  $\sigma_j|\sigma_i|\sigma_j^{-1}|\sigma_i^{-1}$ .

**Example 3.2.** Let  $w$  be the length-5 braid word  $\sigma_1|\sigma_2^{-1}|\sigma_3|\sigma_2^{-1}|\sigma_1$ . Then  $w$  contains the factor  $\sigma_2^{-1}|\sigma_3$ , so it is right-reversible to  $w_1 = \sigma_1|\sigma_3|\sigma_2|\sigma_3^{-1}|\sigma_2^{-1}|\sigma_2^{-1}|\sigma_1$ . Note that  $w$  also contains the factor  $\sigma_2^{-1}|\sigma_1$ , implying that it is also right-reversible to  $w'_1 = \sigma_1|\sigma_2^{-1}|\sigma_3|\sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$ . Restarting from  $w_1$ , the latter contains  $\sigma_2^{-1}|\sigma_1$ , hence it is right-reversible to  $w_2 = \sigma_1|\sigma_3|\sigma_2|\sigma_3^{-1}|\sigma_2^{-1}|\sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$ , etc. The reader can check that every sequence of right-reversings from  $w$  leads in six steps to the length-11 braid word

$$\sigma_1|\sigma_3|\sigma_2|\sigma_1|\sigma_2|\sigma_3|\sigma_2^{-1}|\sigma_3^{-1}|\sigma_1^{-1}|\sigma_1^{-1}|\sigma_2^{-1}.$$

The latter word cannot be right-reversed, since it contains no factor of the form  $\sigma_i^{-1}\sigma_j$ .

The definition makes it obvious that  $w \curvearrowright w'$  implies  $w \equiv w'$ , since each elementary right-reversing step consists in replacing a factor of the considered word by an equivalent word. Conversely, for a given braid word  $w$ , it is false that every braid word equivalent to  $w$  can be obtained by right-reversing from  $w$ : for instance, starting from the word  $\sigma_1|\sigma_1^{-1}$ , we cannot reach the empty word: actually, we can reach no word other than  $\sigma_1|\sigma_1^{-1}$  since the latter contains no factor of the form  $\sigma_i^{-1}|\sigma_j$ .

Right-reversing is a word transformation that takes advantage of the particular form of the braid relations to replace a negative–positive pattern of length two by a positive–negative pattern of length zero, two, or four, depending on the distance between the indices of the initial letters.

As already noted in Example 3.2, the braid words that are terminal with respect to right-reversing, that is, those that cannot be further reversed, are the words that contain no factor of the form  $\sigma_i^{-1}|\sigma_j$ , hence the words of the form  $u|v^{-1}$ , where  $u$  and  $v$  are positive words (no negative letter). As right-reversing may increase the word-length (in Example 3.2, we start with a word of length 5 and finish with a word of length 11), it is not a priori obvious that every braid word is right-reversible to a terminal word. However, it is:

**Lemma 3.3.** *For every braid word  $w$ , there exist positive braid words  $u, v$  such that  $w$  is right-reversible to  $u|v^{-1}$ .*

*Proof (Sketch).* This is a termination problem. We have to show that, starting from a word  $w$ , at least one sequence of reversing steps leads in finitely many right-reversing steps to a positive–negative word. It is not hard to see that it is sufficient to do it when the initial word  $w$  is a negative–positive braid word, that is, we have  $w = u^{-1}|v$  for some positive braid words  $u$  and  $v$ . Let  $R(u, v)$  be the family of all braid words that can be derived from  $u^{-1}|v$  using right-reversing. The point is that, in the braid monoid  $B_n^+$ , the braids represented by  $u$  and  $v$  admit a least common right-multiple, say  $b$ , and that every word  $w$  of  $R(u, v)$  has the property that, for every prefix  $w'$  of  $w$ , the braid  $[u|w']$  is positive and it left-divides  $b$ . The number of such braids is finite, hence so is the family  $R(u, v)$ .  $\square$

By definition, the braid relations of (3) are symmetric, and we can consider a left counterpart of right-reversing where, instead of transforming negative–positive factors into positive–negative words, we transform positive–negative factors into negative–positive words.

**Definition 3.4.** [10] Assume that  $w, w'$  are braid words. We say that  $w$  is *left-reversible* to  $w'$ , written  $w \curvearrowright w'$ , if  $w'$  can be obtained from  $w$  by iteratively

- deleting a subword  $\sigma_i \sigma_i^{-1}$ , or
- replacing a subword  $\sigma_i \sigma_j^{-1}$  with  $|i - j| \geq 2$  by  $\sigma_j^{-1} \sigma_i$ , or
- replacing a subword  $\sigma_i \sigma_j^{-1}$  with  $|i - j| = 1$  by  $\sigma_j^{-1} \sigma_i^{-1} \sigma_j \sigma_i$ .

**Example 3.5.** As in Example 3.2 above, consider  $w = \sigma_1 | \sigma_2^{-1} | \sigma_3 | \sigma_2^{-1} | \sigma_1$ . Then  $w$  contains the factor  $\sigma_1 | \sigma_2^{-1}$ , so it is left-reversible to  $w_1 = \sigma_2^{-1} | \sigma_1^{-1} | \sigma_2 | \sigma_1 | \sigma_3 | \sigma_2^{-1} | \sigma_1$ . Then  $w_1$  contains the factor  $\sigma_3 | \sigma_2^{-1}$ , so it is left-reversible to  $w_2 = \sigma_2^{-1} | \sigma_1^{-1} | \sigma_2 | \sigma_1 | \sigma_2^{-1} | \sigma_3^{-1} | \sigma_2 | \sigma_3 | \sigma_1$ , etc. The reader can check that all sequences of left-reversings from  $w$  leads in six steps to the word  $\sigma_2^{-1} | \sigma_1^{-1} | \sigma_1^{-1} | \sigma_3^{-1} | \sigma_2^{-1} | \sigma_2 | \sigma_3 | \sigma_1 | \sigma_2 | \sigma_3 | \sigma_1$ . The latter word cannot be left-reversed, for it contains no factor of the form  $\sigma_i | \sigma_j^{-1}$ .

As in the case of right-reversing relation  $\curvearrowleft$ , it is obvious that  $w \curvearrowright w'$  implies  $w \equiv w'$ . Note that  $w \curvearrowright w'$  does not imply  $w' \curvearrowleft w$ : for instance, we have  $\sigma_i^{-1} | \sigma_i \curvearrowright \varepsilon$  (the empty word), but  $\varepsilon \not\curvearrowleft \sigma_i^{-1} | \sigma_i$ .

The braid words that are terminal with respect to left-reversing are the words that contain no factor  $\sigma_i | \sigma_j^{-1}$ , hence the words of the form  $u^{-1}|v$  with  $u, v$  positive. By an argument symmetric to the one used for Lemma 3.3, one obtains

**Lemma 3.6.** *For every braid word  $w$ , there exist positive braid words  $u, v$  such that  $w$  is left-reversible to  $u^{-1}|v$ .*

## 4 Proof of Proposition 2.5

With reversing transformations at hand, we can come back to the Hurwitz action of  $n$ -strand braid words on  $S^n$  when  $(S, *)$  is a right-cancellative shelf. We begin with two results that connect colorings with the right- and left-reversing relations of Section 3. These two results are the technical core of the argument.

**Lemma 4.1.** *Assume that  $(S, *)$  is a right-cancellative shelf and  $w, w'$  are  $n$ -strand braid words satisfying  $w \curvearrowright w'$ . Then, for every sequence  $\mathbf{x}$  in  $S^n$ , if  $\mathbf{x} \bullet w$  is defined, so is  $\mathbf{x} \bullet w'$ , and we have  $\mathbf{x} \bullet w' = \mathbf{x} \bullet w$ .*

*Proof.* It suffices to treat the case of a one-step right-reversing. The cases of  $\sigma_i^{-1}|\sigma_i \curvearrowright \varepsilon$  and  $\sigma_i^{-1}|\sigma_j \curvearrowright \sigma_j|\sigma_i^{-1}$  with  $|i - j| \geq 2$  are straightforward, so the point is to prove the result for  $\sigma_i^{-1}|\sigma_j$  with  $|i - j| = 1$ . Hence, it is sufficient to consider the cases of  $\sigma_1^{-1}|\sigma_2$  and  $\sigma_2^{-1}|\sigma_1$  (which do not coincide).

So we first assume that  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2$  is defined. By definition, we have  $\sigma_1^{-1}|\sigma_2 \curvearrowright \sigma_2|\sigma_1|\sigma_2^{-1}|\sigma_1^{-1}$ , so we aim at proving that  $(x, y, z) \bullet \sigma_2|\sigma_1|\sigma_2^{-1}|\sigma_1^{-1}$  is defined as well and equal to  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2$ . Now the assumption that  $(x, y, z) \bullet \sigma_1^{-1}$  is defined implies that there exists  $y'$  satisfying  $y' * x = y$ . Using (2), we deduce

$$(y' * z) * (x * z) = (y' * x) * z = y * z,$$

and the top diagrams in Figure 3 witness that  $(x, y, z) \bullet \sigma_2|\sigma_1|\sigma_2^{-1}|\sigma_1^{-1}$  is indeed defined and equal to  $(y', z, x * z)$ , hence equal to  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2$ .

Assume now that  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$  is defined. By definition, we have  $\sigma_2^{-1}|\sigma_1 \curvearrowright \sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$ , so our aim is to prove that  $(x, y, z) \bullet \sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$  is defined and equal to  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$ . Then the assumption that  $(x, y, z) \bullet \sigma_2^{-1}$  is defined implies that there exists  $z'$  satisfying  $z' * y = z$ . Using (2), we deduce

$$(x * z') * y = (x * y) * (z' * y) = (x * y) * z,$$

and the bottom diagrams in Figure 3 witness that  $(x, y, z) \bullet \sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$  is defined and equal to  $(z', x * z', y)$ , hence equal to  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$ .  $\square$

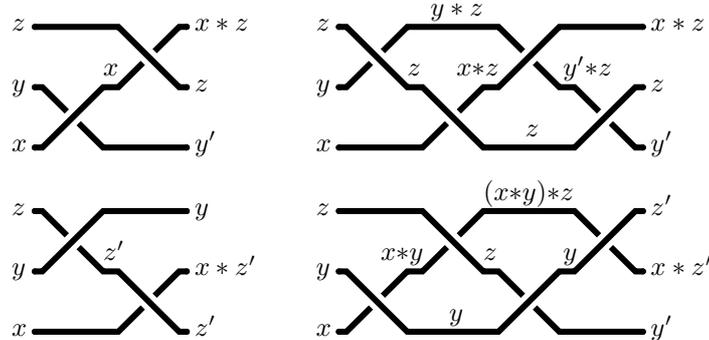


Figure 3: Colorability *vs.* right-reversing: if  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2$  exists, then so does  $(x, y, z) \bullet \sigma_2|\sigma_1|\sigma_2^{-1}|\sigma_1^{-1}$  and it takes the same value (top diagrams); similarly, if  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$  exists, then so does  $(x, y, z) \bullet \sigma_1|\sigma_2|\sigma_1^{-1}|\sigma_2^{-1}$  and it takes the same value (bottom diagrams).

We now consider left-reversing, for which we obtain a symmetric (but not parallel) result: if  $w$  left-reverses to  $w'$ , then the colorability of  $w'$  implies that of  $w$ .

**Lemma 4.2.** *Assume that  $(S, *)$  is a right-cancellative shelf and  $w, w'$  are  $n$ -strand braid words satisfying  $w \curvearrowleft w'$ . Then, for every sequence  $\mathbf{x}$  in  $S^n$ , if  $\mathbf{x} \bullet w'$  is defined, so is  $\mathbf{x} \bullet w$ , and we have  $\mathbf{x} \bullet w' = \mathbf{x} \bullet w$ .*

*Proof.* As above, it suffices to treat the case of a one-step left-reversing, and the cases of  $\sigma_i|\sigma_i^{-1} \cup \varepsilon$  and  $\sigma_i|\sigma_j^{-1} \cup \sigma_j^{-1}|\sigma_i$  with  $|i - j| \geq 2$  are straightforward. So the point is to prove the result for  $\sigma_i|\sigma_j^{-1}$  with  $|i - j| = 1$ . Hence, it is sufficient to consider the cases of  $\sigma_1|\sigma_2^{-1}$  and  $\sigma_2|\sigma_1^{-1}$ . By definition, we have  $\sigma_1|\sigma_2^{-1} \cup \sigma_2^{-1}|\sigma_1^{-1}|\sigma_2|\sigma_1$  and  $\sigma_2|\sigma_1^{-1} \cup \sigma_1^{-1}|\sigma_2^{-1}|\sigma_1|\sigma_2$ .

Assume first that  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1^{-1}|\sigma_2|\sigma_1$  is defined. We want to prove that  $(x, y, z) \bullet \sigma_1|\sigma_2^{-1}$  is defined and equal. The assumption that  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1^{-1}$  is defined implies that there exist  $z'$  and  $z''$  satisfying  $z' * y = z$  and  $z'' * x = z'$ . Using (2), we deduce

$$(z'' * y) * (x * y) = (z'' * x) * y = z' * y = z,$$

and the top diagrams in Figure 4 witness that  $(x, y, z) \bullet \sigma_1|\sigma_2^{-1}$  is defined and equal to  $(y, z'' * y, x * y)$ , hence equal to  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1^{-1}|\sigma_2|\sigma_1$ .

Assume now that  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2^{-1}|\sigma_1|\sigma_2$  is defined. The assumption that  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2^{-1}$  is defined implies that there exist  $y'$  and  $z'$  satisfying  $y' * x = y$  and  $z' * x = z$ . Using (2), we deduce

$$(y' * z') * x = (y' * x) * (z' * x) = y * z,$$

and the bottom diagrams in Figure 4 witness that  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$  is defined and equal to  $(z', x, y * z)$ , hence equal to  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2^{-1}|\sigma_1|\sigma_2$ .  $\square$

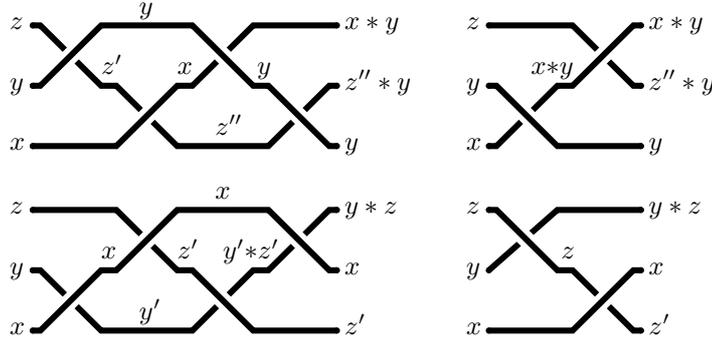


Figure 4: Colorability vs. left-reversing: if  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1^{-1}|\sigma_2|\sigma_1$  is defined, then so is  $(x, y, z) \bullet \sigma_1|\sigma_2^{-1}$  and it takes the same value (top diagrams); similarly, if  $(x, y, z) \bullet \sigma_1^{-1}|\sigma_2^{-1}|\sigma_1|\sigma_2$  is defined, then so is  $(x, y, z) \bullet \sigma_2^{-1}|\sigma_1$  and it takes the same value (bottom diagrams).

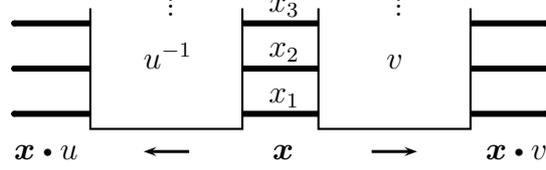
We can now establish Proposition 2.5.

*Proof of Proposition 2.5.* Owing to the rules (5) and (14), for each initial sequence  $\mathbf{x}$  in  $S^n$  and each  $n$ -strand braid word  $w$ , either the initial colours can be propagated throughout the diagram  $D(w)$  encoded by  $w$  and there is exactly one output sequence which is denoted by  $\mathbf{x} \bullet w$ , or there exists at least one negative crossing where the division is impossible and then  $\mathbf{x} \bullet w$  does not exist.

The point is to guarantee that  $S$ -colorings satisfy (15), (16), and (17). First, (15) follows from Proposition 1.1 and from the assumption that  $(S, *)$  is a shelf.

Let us now consider (16), that is, the existence of at least one sequence of colors eligible for a braid word or, more generally, a finite sequence of braid words. We first consider

the case of one unique braid word  $w$ . By Lemma 3.6, there exist positive braid words  $u, v$  satisfying  $w \curvearrowright u^{-1}|v$ . We observe that, if  $\mathbf{x}$  is *any* sequence in  $S^n$ , then starting from the colors  $\mathbf{x}$  in the middle of the diagram  $D(u^{-1}|v)$  and propagating the colors to the left through  $u^{-1}$  and to the right through  $v$  as in the diagram



provides a legal  $S$ -coloring. In other words, one has, for every sequence  $\mathbf{x}$ ,

$$(\mathbf{x} \cdot u) \cdot u^{-1}|v = \mathbf{x} \cdot v.$$

Since  $w \curvearrowright u^{-1}|v$  holds, Lemma 4.2 then implies  $(\mathbf{x} \cdot u) \cdot w = \mathbf{x} \cdot v$ , showing that  $\mathbf{y} \cdot w$  is defined for any initial sequence of colors  $\mathbf{y}$  of the form  $\mathbf{x} \cdot u$ .

Consider now a finite family of braid words  $w_1, \dots, w_p$  with  $p \geq 2$ . For every  $k$ , there exist positive braid words  $u_k, v_k$  satisfying  $w_k \curvearrowright u_k^{-1}|v_k$ . Then, in the involved braid monoid  $B_n^+$ , the braids  $[u_1], \dots, [u_p]$  admit a common left-multiple [16], that is, there exist positive braid words  $u'_1, \dots, u'_p$  satisfying  $u'_1|u_1 \equiv \dots \equiv u'_p|u_p$ . Let  $\mathbf{x}$  be an arbitrary sequence in  $S^n$ . Then, for every  $k$ , the sequence  $\mathbf{x} \cdot u'_k|u_k$  is defined since  $u'_k|u_k$  is a positive braid word. Let  $\mathbf{y} = \mathbf{x} \cdot u'_1|u_1$ . Then, for every  $k$ , as we have  $u'_k|u_k \equiv u'_1|u_1$ , whence  $u'_k|u_k \equiv^+ u'_1|u_1$  since all involved words are positive, and, therefore, (13) implies  $\mathbf{x} \cdot u'_k|u_k = \mathbf{y}$ . Hence, as before,  $\mathbf{y} \cdot (u'_k|u_k)^{-1}$ , that is,  $\mathbf{y} \cdot u_k^{-1}|u'_k$ , is defined, and it is equal to  $\mathbf{x}$ . So, a fortiori,  $\mathbf{y} \cdot u_k^{-1}$  is defined for every  $k$ , and so is  $\mathbf{y} \cdot u_k^{-1}|v_k$  since  $v_k$  is positive. Finally, since  $w_k \curvearrowright u_k^{-1}|v_k$  holds, Lemma 4.2 implies that  $\mathbf{y} \cdot w_k$  is also defined for every  $k$ , which completes the proof of (16).

Finally, let us consider (17). So assume that  $w, w'$  are equivalent (signed) braid words, and  $\mathbf{x} \cdot w$  and  $\mathbf{x} \cdot w'$  are defined. Write  $\mathbf{y} = \mathbf{x} \cdot w$  and  $\mathbf{y}' = \mathbf{x} \cdot w'$ . We want to show that  $\mathbf{y}$  and  $\mathbf{y}'$  are equal. By Lemma 3.3, there exist positive words  $u, v, u', v'$  such that  $w \curvearrowright u|v^{-1}$  and  $w' \curvearrowright u'|v'^{-1}$ . Then Lemma 4.1 implies  $\mathbf{y} = \mathbf{x} \cdot u|v^{-1}$  (meaning in particular that the latter is defined) and, similarly,  $\mathbf{y}' = \mathbf{x} \cdot u'|v'^{-1}$ . In the monoid  $B_n^+$ , the braids  $[u]$  and  $[u']$  admit a common right-multiple [16], so there exist positive words  $w_0, w'_0$  satisfying  $u|w_0 \equiv^+ u'|w'_0$ , whence  $u|w_0 \equiv u'|w'_0$ . Then the assumption  $w \equiv w'$  implies  $u|v^{-1} \equiv u'|v'^{-1}$ , whence  $v|u^{-1} \equiv v'|u'^{-1}$ , and we deduce

$$v|w_0 \equiv v|u^{-1}|u|w_0 \equiv v'|u'^{-1}|u|w_0 \equiv v'|u'^{-1}|u'|w'_0 \equiv v'|w'_0,$$

which in turn implies  $v|w_0 \equiv^+ v'|w'_0$  since these words are positive and  $B_n^+$  embeds in  $B_n$ . For every sequence  $\mathbf{z}$  in  $S^n$  and every positive  $n$ -strand braid word  $w_1$ , the sequence  $\mathbf{z} \cdot w_1|w_1^{-1}$  is defined and equal to  $\mathbf{z}$ . So the equality  $\mathbf{x} \cdot u|v^{-1} = \mathbf{y}$  implies

$$(18) \quad \mathbf{x} \cdot u|w_0|w_0^{-1}|v^{-1} = \mathbf{y}.$$

Put  $\mathbf{z} = \mathbf{x} \cdot u|w_0$ . Then (18) implies  $\mathbf{z} \cdot w_0^{-1}|v^{-1} = \mathbf{y}$  and, therefore, we have

$$(19) \quad \mathbf{x} \cdot u|w_0 = \mathbf{z} \quad \text{and} \quad \mathbf{y} \cdot v|w_0 = \mathbf{z}.$$

Putting  $\mathbf{z}' = \mathbf{x} \cdot u'|w'_0$ , we similarly obtain

$$(20) \quad \mathbf{x} \cdot u'|w'_0 = \mathbf{z}' \quad \text{and} \quad \mathbf{y}' \cdot v'|w'_0 = \mathbf{z}'.$$

Now, we saw above that  $u|w_0$  and  $u'|w'_0$  on the one hand, and  $v|w_0$  and  $v'|w'_0$  on the other hand, are equivalent positive braid words. By (13), we first deduce  $\mathbf{z} = \mathbf{z}'$ , and then  $\mathbf{y} = \mathbf{y}'$  by uniqueness of the action of negative braids when they are defined. So (17) is satisfied, and the proof of Proposition 2.5 is complete.  $\square$

**Remark 4.3.** It is explained in [12, Chap. IV] how the Hurwitz (partial) action associated with the shelf of Example 2.1 (that is not a rack) allows for constructing a left-invariant linear ordering on the braid group  $B_n$ . It is perhaps worth mentioning that, in [12], the left counterpart of (2), that is, the left version of self-distributivity is considered, and, therefore, what is considered is the symmetric version of the braid operation of Example 2.1. Of course, one obtains entirely symmetric properties by exchanging the left and the right sides in computation. However, in terms of braid colorings, the results are not symmetric, unless the numbering of braid strands is also reversed (starting from the top strand instead of from the bottom one). Nevertheless, in any case and whatever convention is used, the symmetry is *not* complete, because the shift endomorphism  $\text{sh}$  of  $B_\infty$  has no symmetric counterpart: there exists no endomorphism of  $B_\infty$  mapping  $\sigma_i$  to  $\sigma_{i-1}$  for every  $i$ . So some care is definitely needed to adapt the results of [12, Chap. IV] to a right self-distributive context.

We conclude with an application of Proposition 2.5. Say that a shelf  $(S, *)$  is *orderable* if there exists a linear ordering  $\prec$  on  $S$  that is right-invariant ( $x \prec y$  implies  $x * z \prec y * z$  for every  $z$ ) and satisfies  $y \prec x * y$  for all  $x, y$ . Then, for instance, one can show that the shelf  $(B_\infty, *)$  of Example 2.1 is orderable. As this shelf is right-cancellative, it is eligible for Proposition 2.5 and, therefore, every braid diagram  $D(w)$  is  $(B_\infty, *)$ -colorable in at least one way. Then we immediately deduce:

**Proposition 4.4.** *A braid word in which all generators  $\sigma_i$  with maximal  $i$  are positive (no  $\sigma_i^{-1}$ ) is not trivial, that is, it does not represent the braid 1.*

*Proof.* Assume that  $w$  is an  $n$ -strand braid word in which  $\sigma_{n-1}$  occurs but  $\sigma_{n-1}^{-1}$  does not. We color the diagram  $D(w)$  using  $(B_\infty, *)$  (or any orderable shelf). By Proposition 2.5, there exists at least one sequence  $\mathbf{y}$  that can be propagated through the diagram  $D(w)$ . Then, with the notation of Figure 5, we have

$$y_n \prec x * y_n \prec x' * (x * x_y) \prec \dots,$$

so the output color on the  $n$ th strand is certainly strictly larger than  $y_n$ , whereas, using the same input colors, the output color of the  $n$ th strand in the diagram  $D(\varepsilon)$  is  $y_n$ . Hence,  $w \equiv \varepsilon$  is impossible.  $\square$

So we see in this example that even a partial action may be useful and, therefore, so are techniques like the ones explained above.

To conclude, let us recall that the current techniques only allow for extending the Hurwitz action to shelves that need not be racks but nevertheless are right-cancellative.

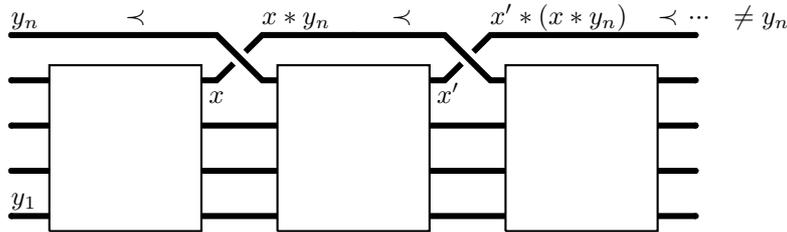


Figure 5: A braid diagram in which all top crossings have the same orientation is not trivial: using the partial action of Proposition 2.5 and coloring the strands using a colorable shelf, the colors keep increasing on the top strand, so the diagram cannot be trivial.

As there exists a number of such structures (in particular, all free shelves are right-cancellative), the range of applications is promising. However, there also exist a number of shelves that are not right-cancellative: here we think in particular of the finite Laver tables [18, 11, 13, 19], which have fascinating combinatorial properties and appear as natural candidates for potential topological applications. So, clearly, further extensions of the techniques explained above are desirable: for instance, one might renounce to considering individual sequences of colors and, instead of going from one sequence of input colours to one sequence of output colours, consider a correspondence involving finite families of sequences.

## References

- [1] E. Brieskorn, *Automorphic sets and braids and singularities*, Braids, Contemp. Math., vol. 78, American Mathematical Society, 1988, pp. 45–117.
- [2] J.S. Carter, D. Jelsovsky, S. Kamada, and M. Saito, *Computation of quandle cocycle invariants of knotted curves and surfaces*, Adv. in Math. **157** (2001), 36–94.
- [3] S. Carter, *A survey of quandle ideas*, Introductory lectures on Knot Theory (L. Kauffman and al., eds.), Series on Knots and Everything, vol. 46, World Scientific, 2012, pp. 22–53.
- [4] W. Chang and S. Nelson, *Rack shadows and their invariants*, J. Knot Theory Ramifications, **20** (2011) 1259–1269.
- [5] A.S. Crans, S. Nelson, and A. Sarkar, *Enhancements of rack counting invariants via dynamical cocycles*, New York J. Math., **18** (2012) 337–351.
- [6] P. Dehornoy, *Braid groups and left-distributive operations*, Trans. Amer. Math. Soc. **345** (1994) no. 1, 115–151.
- [7] ———, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997), 115–137.
- [8] ———, *Strange questions about braids*, J. Knot Theory Ramifications **8** (1999), no. 5, 589–620.

- [9] ———, *Braids and Self-Distributivity*, Progr. Math., vol. 192, Birkhäuser, 2000.
- [10] ———, *The subword reversing method*, Intern. J. Alg. and Comput. **21** (2011), 71–118.
- [11] ———, *Laver’s results and low-dimensional topology*, Arch. Math. Logic, to appear (32 pages), arXiv:1401.3302.
- [12] P. Dehornoy with I. Dynnikov, D. Rolfsen, B. Wiest, *Ordering Braid*, Mathematical Surveys and Monographs vol. 148, Amer. Math. Soc. (2008).
- [13] P. Dehornoy and V. Lebed, *Two- and three-cocycles for Laver tables*, J. Knot Theory Ramifications; **23** (2014) no. 4, 1450017.
- [14] R. Fenn and C.P. Rourke, *Racks and links in codimension 2*, J. Knot Theory Ramifications **1** (1992), 343–406.
- [15] R. Fenn, C.P. Rourke, and B. Sanderson, *James bundles*, Proc. London Math. Soc. **89** (2004), 217–240.
- [16] F.A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford Ser. **20** (1969), 235–254.
- [17] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.
- [18] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108** (1996), no. 1, 81–98.
- [19] V. Lebed, *Cohomology of finite monogenic self-distributive structures*, arXiv:1503:07030.
- [20] S.V. Matveev, *Distributive groupoids in knot theory*, Sb. Math. **119** (1982), no. 1-2, 78–88.
- [21] S. Nelson, *Link invariants from finite racks*, arXiv:0808.0029.
- [22] S. Nelson and R. Wieghard, *Link invariants from finite Coxeter racks*, J. Knot Theory Ramifications, **20** (2011) 1247–1257.

Laboratoire de Mathématiques Nicolas Oresme,  
 CNRS UMR 6139, Université de Caen, F-14032 Caen  
 FRANCE

E-mail address: [dehornoy@math.unicaen.fr](mailto:dehornoy@math.unicaen.fr)

URL address: [www.math.unicaen.fr/~dehornoy/](http://www.math.unicaen.fr/~dehornoy/)