ACTION OF BRAIDS ON SELF-DISTRIBUTIVE SYSTEMS

Patrick DEHORNOY

Abstract. This paper is a survey of recent work about the action of braids on self-distributive systems. We show how the braid word reversing technique allows one to use new self-distributive systems, leading in particular to a natural linear ordering of the braids.

AMS Subject Classification: 20F36, 20N02.

It has been observed for many years that there exist a connection between braids and left self-distributive systems (LD-systems for short), defined as those algebraic systems consisting of a set equipped with a binary operation $*$ that satisfies the left self-distributivity identity

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

In particular, D. Joyce [14] and S. Matveev [17], in independent works, have associated with every knot a particular LD-system that characterizes the isotopy type of the knot, and several variants of this approach have been subsequently proposed, with different names.

Here, we do not try to associate with a given braid or knot a particular LD-system that gives information about it, but we fix an LD-system, and try to use it to get information about arbitrary braids. To this end, we can use the intuition of *braid colouring*: assuming that $(S, *)$ is an LD-system, we use the elements of S as colours that we put on the strands of the braids, with the rule that $a * b$ is the new colour obtained when a strand of colour a overcrosses a strand of colour b. The left self-distributivity identity arises naturally as the compatibility condition needed for the colouring to be invariant under positive braid isotopy. In this way, we obtain for every LD-system S a well-defined action on S^n of the monoid B_n^+ of n-strand positive braids. In order to define an action of the whole group B_n, we must assume that the LD-system S has the additional property that all left translations are bijective, *i.e.*, left division is always possible with a unique well-defined result. Such particular LD-systems have been called *automorphic sets* by E. Brieskorn [2], or *racks* by R. Fenn and C. Rourke [12]. So, in this way, we obtain an action of B_n on the n-th power of every automorphic set. Considering the known examples of automorphic sets leads to several classical representations of the braid groups, in particular Artin's representation in the automorphisms of a free group and Burau representation.

Automorphic sets are LD-systems of a very special type, in particular they are idempotent, or close to. In the recent years, new examples of LD-systems have appeared, in connection with results of set theory involving some strange LD-system [7]. These new examples are quite different from automorphic sets, and the question arises of extending the existence of a braid action to them. The aim of this paper is to explain how this can be done, at the expense of replacing an everywhere defined action with a partial action, in the case of a left cancellative LD-system, *i.e.*, when we assume that the left translations are injective, but not necessarily surjective. Such a result makes most of the new examples of LD-systems eligible for a braid action. In particular, considering the action in the case of a certain left

semf-distributive operation on the braids themselves leads to defining a linear ordering of the braids.

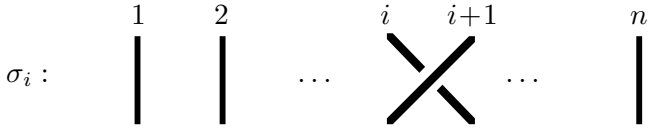
The author wishes to thank S. Matveev and the organizers of the Chelyabinsk Conference, as well as A. Sossinsky, for their constant and friendly help during his visit to Russia in August 1999.

1. Braid colourings

We use standard notations for braids, as introduced for instance in [18]. Thus B_n denotes the n-strand braid group; it admits the presentation

$$\langle \sigma_1, \dots, \sigma_{n-1} \ ; \ \sigma_i\sigma_j = \sigma_j\sigma_i \ \text{ for } |i-j| \geq 2, \ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \ \text{ for } |i-j| = 1 \rangle, \qquad (1.1)$$

where σ_i corresponds to the elementary braid diagram



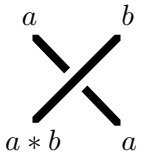
We use B_∞ for the direct limit of the groups B_n when B_n is embedded in B_{n+1} by adding an additional strand on the right. Then B_∞ admits the above presentation (1.1) with an infinite sequence of generators σ_1, σ_2, ...

By construction, an element of B_n is an equivalence class of *braid words* that live in the free monoid over the $2n-2$ letters σ_1, ..., σ_{n-1}, σ_1^{-1}, ..., σ_{n-1}^{-1}. It will be crucial in the sequel to carefully distinguish between the braids and the braid words that represent them. We write $\equiv$ for braid word equivalence. For b a braid and w a braid word, we say that w is an expression of b to mean that b is the $\equiv$-equivalence class of w in B_n. We say that a braid word is positive if it involves no letter σ_i^{-1}; we say that a braid is positive if admits at least one expression by a positive braid word. Positive n-strand braid form a submonoid B_n^+ of B_n.

Assume that S is a fixed nonempty set. Let us use the elements of S to colour the strands of the braids. To this end, we attribute to each top end of a strand a colour from S, and we propagate the colour along the strands of the diagram. The general principle will be to try to recover information about the considered braid by comparing the initial sequence of colours with the final sequence.

If the colours are propagated without change along the strands, the final sequence of colours is a permutation of the initial sequence, and the only piece of information about the braid we get in this way is its projection in the symmetric group.

Things become more interesting when we allow colours to change at crossings. We begin with the case of positive braid words. According to the idea of propagating the colours downwards from the top of the braid diagram, it is natural to fix the rules of colouring so that the colours after a crossing (the 'new' colours) are determined by the colours before the crossings (the 'old' colours). Keeping the colours corresponds to the simplest function, namely identity. The next step in complexity is to assume that only one colour may change, say the colour of the front strand, and the new colour depends only on the two colours of the strands that have crossed. This amounts to using a function of $S \times S$ into S, *i.e.*, a binary operation $*$ on S, so that the rule for propagating colours is



Formally, the construction consists in defining a (right) action of n-strand positive braid words on S^n by the inductive rule

$$\vec{a} \cdot \varepsilon = \vec{a}, \qquad \vec{a} \cdot \sigma_i w = (a_1, \dots, a_i * a_{i+1}, a_i, a_{i+2}, \dots, a_n) \cdot w, \tag{1.2}$$

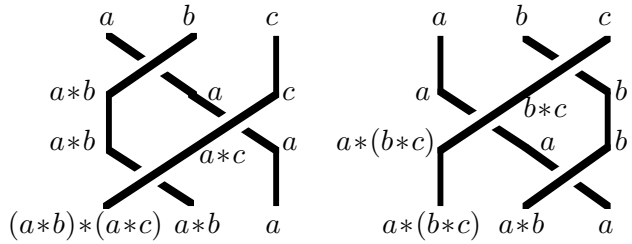
where ε denotes the empty word (everywhere in the sequel, when $\vec{a}$ denotes a sequence, we use a_1, a_2, ... for the successive entries of that sequence).

As we are interested in braids rather than in braid words, we wish the previous action to induce a well-defined action of braids. This means that the colourings have to be invariant under braid relations.

Lemma 1.1. *Assume that $(S, *)$ is a binary system. The right action of positive braid words on S^n defined in* (1.2) *is invariant under braid relations* (1.1) *if and only if $(S, *)$ satisfies the left self-distributivity identity*

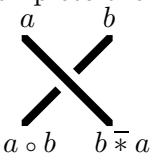
$$x * (y * z) = (x * y) * (x * z). \tag{LD}$$

Proof. Compare the diagrams:



The lower colours on the left strand coincide for every initial choice of a, b, c if and only if the operation $*$ satisfies Identity (LD). ■

Let us now consider arbitrary braid words. We try to define an action of arbitrary words on sequences of colours. We have to choose a rule for colouring negative crossings. In order to have a flexible definition, let us first assume that the set of colours S is equipped with three binary operations, say $*$, $\circ$ and $\overline{*}$. We complete the previous definition with the rule



This amounts to extending the action of braid words on sequences of colours by defining, for $\vec{a} = (a_1, \dots, a_n)$,

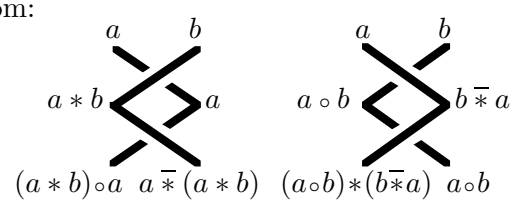
$$\vec{a} \cdot \sigma_i^{-1} w = (a_1, \dots, a_i \circ a_{i+1}, a_{i+1} \mathbin{\overline{*}} a_i, a_{i+2}, \dots, a_n) \cdot w. \tag{1.3}$$

Lemma 1.2. *Assume that $(S, *, \circ, \overline{*})$ is a triple binary system. The right action of braid words on S^n defined by* (1.2) *and* (1.3) *is invariant under the relations $\sigma_i \sigma_i^{-1} = \sigma_i^{-1} \sigma_i = \varepsilon$ if and only if the identities*

$$x \circ y = y, \qquad x * (x \mathbin{\overline{*}} y) = x \mathbin{\overline{*}} (x * y) = y$$

are satisfied in S.

Proof. This follows from:



First, we see on the rightmost strand that $a \circ b$ must coincide with b. Then looking at the remaining strands gives the relations between the operations $*$ and $\overline{*}$. ■

We are thus led to the following definitions.

Definition. (i) An *LD-system* is defined to be a set equipped with a binary operation that satisfies Identity (LD).

(ii) An *LD-quasigroup* is defined to be an LD-system equipped with an additional operation $\overline{*}$ that satisfies the identity

$$x * (x \mathbin{\overline{*}} y) = x \mathbin{\overline{*}} (x * y) = y. \tag{1.4}$$

As it stands, an LD-quasigroup is defined as a set equipped with two binary operations. Actually, each operation determines the other one. Indeed, if $(Q, *, \overline{*})$ is an LD-quasigroup, then, for all a, b in Q, we have

$$a \mathbin{\overline{*}} b = \text{ the unique } c \text{ satisfying } a * c = b. \tag{1.5}$$

Conversely, if $(S, *)$ is an LD-system where all left translations are bijective, *i.e.*, an automorphic set in the sense of [2] or a rack in the sense of [12], then using (1.5) to define a second operation $\overline{*}$ gives S the structure of an LD-quasigroup.

So, at this point, we have the following result, which can be traced back at least to [2]:

Proposition 1.3. *(i) Assume that $(S, *)$ is an LD-system. Then, for every n, Formula* (1.2) *defines an action of the braid monoid B_n^+ on S^n.*

(ii) Assume that $(S, *, \overline{*})$ is an LD-quasigroup. Then, for every n, Formulas (1.2) *and* (1.3) *(with $a \circ b = b$) define an action of the braid group B_n on S^n.*

In the current context, for $\vec{a}$ a sequence of elements of S, and b a braid, we shall write $\vec{a} \cdot b$ for the result of applying b to $\vec{a}$, *i.e.*, for $\vec{a}w$ where w is an arbitrary expression of b. The question we raised above is to extract information about the braid b from the comparison of the sequences $\vec{a}$ and $\vec{a} \cdot b$. Let us first consider some classical examples of LD-quasigroups.

Example 1.4. (trivial) Let S be an arbitrary set. Then the trivial operations

$$a * b = b, \qquad a \mathbin{\overline{*}} b = b \tag{1.6}$$

turn S into an LD-quasigroup. Using such a structure to colour the strands of the braids amounts to keeping the colours unchanged. Then, for every braid b in B_n, and every sequence $\vec{a}$ in S^n, we have

$$\vec{a} \cdot b = \mathrm{perm}(b)^{-1}(\vec{a}), \tag{1.7}$$

where $\mathrm{perm}(b)$ denotes the permutation that specifies the initial positions of the strands in terms of their final positions (this choice is needed for perm to be a homomorphism with composition of permutations). Thus, using this particular LD-quasigroup leads to the surjective homomorphism

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

Example 1.5. (shift) Let $\mathbf{Z}$ denote the set of all integers. Then the operations

$$a * b = b + 1, \qquad a \mathbin{\overline{*}} b = b - 1 \tag{1.8}$$

turn $\mathbf{Z}$ into an LD-quasigroup. For every braid b in B_n, and every sequence $\vec{a}$ in $\mathbf{Z}^n$, we find

$$\sum(\vec{a} \cdot b) = \sum \vec{a} + \mathrm{sum}(b), \tag{1.9}$$

where $\sum \vec{a}$ denotes $a_1 + \ldots + a_n$, and $\mathrm{sum}(b)$ denotes the exponent sum of b, defines to be the difference between the number of positive and legative letters in any expression of b. Thus, using this LD-quasigroup leads (in particular) to the homomorphism

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

Observe that the above two LD-quasigroups belong to the more general type

$$a * b = f(b), \qquad a \mathbin{\overline{*}} b = f^{-1}(b) \tag{1.10}$$

where f is an arbitrary bijection of the considered domain.

Example 1.6. (mean) Assume that E be a $\mathbf{Z}[t,t^{-1}]$-module. The binary operations

$$a*b=(1-t)a+tb, \qquad a\mathbin{\overline{*}}b=(1-t^{-1})a+t^{-1}b \tag{1.11}$$

turn E into an LD-quasigroup. For every n-strand braid b, and every sequence $\vec{a}$ in E^n, the output colours $\vec{a}\cdot b$ are linear combinations of $\vec{a}$. There exists an $n\times n$-matrix $r_B(b)$ satisfying

$$\vec{a}\cdot b=\vec{a}\times r_B(b). \tag{1.12}$$

Thus, using the current LD-quasigroup leads to a linear representation

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

This linear representation of B_n is known as the (unreduced) Burau representation. Observe that Example 1.4 corresponds to the specialization $t=1$ in the current example.

Example 1.7. (conjugacy) Let G be a group. Then the binary operations defined by

$$x*y=xyx^{-1}, \qquad x\mathbin{\overline{*}}y=x^{-1}yx \tag{1.13}$$

turn G into an LD-quasigroup. In particular, let F_n be the free group based on $\{x_1,\dots,x_n\}$. For b an n-strand braid, let $\widetilde{b}$ denote the image of b under the antiautomorphism of B_∞ that is the identity on the generators σ_i: thus an expression of $\widetilde{b}$ is obtained from an expression of b by reversing the orders of the letters. Then define elements y_1, …, y_n of G by

$$(y_1,\dots,y_n)=(x_1,\dots,x_n)\cdot\widetilde{b},$$

and let $\varphi(b)$ be the endomorphism of F_n that maps x_i to y_i for every i. Then φ is an endomorphism of B_n into $\mathrm{End}(F_n)$, and, as $\varphi(b^{-1})=\varphi(b)^{-1}$ holds by construction, the image of φ is actually included in $\mathrm{Aut}(F_n)$. As in Example 1.4, using here $\widetilde{b}$ is necessary because we consider a right action of B_∞, while, by definition, composition of automorphisms corresponds to a left action. Thus, using the current LD-quasigroup leads to Artin's representation

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

which is known to be faithful. Using the framework of free differential calculus, it can be seen that the mean operations of Example 1.6 as projections of the operations of the current example, this corresponding to the fact that the Burau matrix of a braid can be deduced from the associated automorphism of a free group.

This more or less completes the list of the classical examples of LD-quasigroups. As using them leads to nontrivial representation results for the braid groups, it is natural to raise the following question:

Question 1.8. *Can we find new examples of LD-quasigroups, and deduce further properties of braids?*

The answer to the first part is positive, but it seems that the answer to the second part seems to be essentially negative. To explain this, let us introduce one more example.

Example 1.9. (half-conjugacy) Let again G be a group, and X be a subset of G. The binary operations defined by

$$(a,x)*(b,y)=(axa^{-1}b,y), \qquad (a,x)\mathbin{\overline{*}}(b,y)=(ax^{-1}a^{-1}b,y) \tag{1.14}$$

turn $G\times X$ into an LD-quasigroup. These operations can be called "half-conjugacy" because it is related to conjugacy as follows: let f be the mapping of $G\times X$ to G defined by $f((a,x))=axa^{-1}$; then f is a surjective homomorphism of $G\times X$ equipped with the current operations onto G equipped with the operations of Example 1.7.

Half-conjugacy of a group gives, in some sense, the most general LD-quasigroup: indeed, if we denote by F_X the free group based on X, then the LD-quasigroup consisting of $F_X \times X$ with the half-conjugacy operations of (1.14) is a free LD-quasigroup based on X: every LD-quasigroup generated by X is a quotient of $F_X \times X$, and, therefore, the optimal results about braids we can expect to obtain using LD-quasigroups are those coming from $F_X \times X$. The mapping f of Example 1.8 is not an embedding, and, in theory, we could perhaps obtain more using $F_X \times X$ with half-conjugacy than using F_X with conjugacy, but the distance between the two structures is short—half-conjugacy is a sort of semidirect product of conjugacy with the trivial operations of Example 1.5—and we have no positive result in this direction.

The LD-quasigroups of Examples 1.4 (trivial), 1.6 (mean), and 1.7 (conjugacy) all are idempotent, *i.e.*, they satisfy the identity

$$x * x = x.$$

This is not true for the LD-quasigroups of Example 1.5 (shift) and 1.8 (half-conjugacy), but a weak form of idempotency is also satisfied.

Lemma 1.10. *Every LD-quasigroup satisfies the identity*

$$(x * x) * y = x * y. \tag{1.15}$$

Proof. As $F_X \times X$ equipped with half-conjugacy is a free LD-quasigroup, it suffices to check that (1.15) holds in this particular LD-quasigroup, which is straightforward. However, we can also write directly, using the identities of an LD-quasigroup:

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

Important from our point of view is the fact that Identity (1.15) prevents LD-quasigroups from satisfying some orderability conditions. In the sequel, if $(S, *)$ is an arbitrary binary system, and a, b are elements of S, we say that a is a *left divisor* of b if $b = a * x$ holds for some x. We shall consider below those LD-systems where the left divisibility relation induces an ordering. A necessary condition in this direction (actually also sufficient) is that left division has no cycle, and we are thus led to study the possible cycles of left division. In those LD-systems we have met so far, the answer is the worst possible. In an idempotent system S, every element a is a left divisor of itself, and, therefore (a) is a cycle of length 1 for left division. As we have seen, all LD-quasigroups are not idempotent, but, from the point of view of cycles in left division, the situation is the same:

Proposition 1.11. *In every LD-quasigroup, left division admits cycles of length* 1.

Proof. Assume that $(Q, *)$ is an LD-quasigroup, and a is an arbitrary element of Q. Then we have $(a * a) * a = a * a$, hence $(a * a)$ is a cycle of length 1 for left division. $\blacksquare$

At the end of this first section, we are thus led to the following double question:

Question 1.12. *(i) Do there exist some LD-system (necessarily not an LD-quasigroup) where left division admits no cycle?*

(ii) If so, can we use such an LD-system to colour braids?

We shall see in the sequel that the answer to both questions is positive. For the moment, let us conclude with a last example, which brings a (very) partial answer to Question 1.12.(i).

Example 1.13. (injection bracket, [4]) Let us denote by I_∞ the monoid of all injective, non-bijective mappings of $\mathbf{N}$ into itself equipped with composition. For f, g in I_∞, let us define the injection $f[g]$ by

$$f[g](n) = \begin{cases} fgf^{-1}(n) & \text{if } n \text{ belongs to the image of } f, \\ n & \text{otherwise.} \end{cases} \tag{1.16}$$

It is easy to verify that this bracket operation is left self-distributive, and that the equality

$$\mathrm{coIm}(f[g]) = f(\mathrm{coIm}(g))$$

holds, where $\mathrm{coIm}(f)$ denotes the complement of the image of f. It follows that no equality of the form $f[g] = f$ is possible in I_∞, for $\mathrm{coIm}(f[g])$, being included in $\mathrm{Im}(f)$, is always disjoint from $\mathrm{coIm}(f)$. It follows that left division in $(I_\infty, [\ ])$ admits no cycle of length 1 (but it can be checked that it admits cycles of length 2).

2. Braid word reversing

As they stand, the previous results cannot really be improved. In order to go further, we need new results about braids, or, more precisely, about braid words. In this section, we introduce a specific technique called word reversing, which will give us the needed results. This technique is reminiscent of the tools used by Garside in his solution of the conjugacy problem of B_n [13]. However, our point of view is slightly different as we put the emphasis on braid words rather than on braids. This distinction will be crucial for the application to braid colourings in Section 3.

A trivial observation is that all relations in the standard presentation of the braid group have the form

$$\sigma_i \cdot \ldots = \sigma_j \cdot \ldots,$$

where the dots represent some braid word depending on σ_i and σ_j. Let us denote by Σ the alphabet $\{\sigma_1, \sigma_2, \ldots\}$. We use Σ^* for the set of all words on Σ, *i.e.*, for the set of all positive braid words, and $(\Sigma \cup \Sigma^{-1})^*$ for the set of all words on $\Sigma \cup \{\sigma_1^{-1}, \sigma_2^{-1}, \ldots\}$, *i.e.*, the set of all braid words. Let us consider the function θ_R of $\Sigma \times \Sigma$ into Σ^* defined by

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

Then, according to the presentation (1.1) of B_∞, braid word equivalence is generated by the relations

$$\sigma_i\ \theta_R(\sigma_j, \sigma_i) \equiv \sigma_j\ \theta_R(\sigma_i, \sigma_j) \tag{2.1}$$

for $i \neq j$. We call a monoid or a group presentation of the type above a (right) complemented presentation, for the relations exactly tell us how to complete each pair of generators on the right so as to obtain a common multiple of these generators.

Now we observe that, for all i, j, Relation (2.1) implies the equivalence

$$\sigma_i^{-1}\ \sigma_j \equiv \theta_R(\sigma_j, \sigma_i)\ \theta_R(\sigma_i, \sigma_j)^{-1} \tag{2.2}$$

in the free monoid $(\Sigma \cup \Sigma^{-1})^*$, where, for w a braid word, we denote by w^{-1} the braid word obtained from w by reversing the order of the letters and exchanging σ_i with σ_i^{-1} everywhere. It follows that, if a braid word w' is obtained from another braid word w by repeatedly applying relations of the type (2.2), then w and w' are equivalent, *i.e.*, they represent the same braid.

Definition. Assume that w, w' are braid words. We say that w' is obtained from w by k steps of *(right) word reversing* if one can transform w into w' by successively replacing k factors of the type $\sigma_i^{-1}\,\sigma_j$ with the corresponding factor $\theta_R(\sigma_j,\sigma_i)\,\theta_R(\sigma_i,\sigma_j)^{-1}$.

Example 2.1. (word reversing) Let us consider $w = \sigma_1^{-1}\sigma_3^{-1}\sigma_2\sigma_4$. Then w contains the factor $\sigma_3^{-1}\sigma_2$, and this is the only factor of the type $\sigma_i^{-1}\sigma_j$ in w: so applying word reversing to w leads in one step to $w_1 = \sigma_1^{-1}\sigma_2\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_4$. We see that, in w_1, there are two factors of the type $\sigma_i^{-1}\sigma_j$, namely the initial factor $\sigma_1^{-1}\sigma_2$, and the final factor $\sigma_3^{-1}\sigma_4$. Hence two words can be obtained from w by two steps of word reversing, namely $\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\sigma_3\sigma_2^{-1}\sigma_3^{-1}\sigma_4$ and $\sigma_1^{-1}\sigma_2\sigma_3\sigma_2^{-1}\sigma_4\sigma_3\sigma_4^{-1}\sigma_3^{-1}$. The reader can continue, and check that all sequences of word reversing from w end in 16 steps with the word $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1\sigma_4^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_1^{-1}\sigma_3^{-1}\sigma_2^{-1}\sigma_4^{-1}\sigma_3^{-1}$. The latter word can no longer be reversed, for it contains no more factor of the form $\sigma_i^{-1}\sigma_j$.

The existence of a complemented presentation in itself is a rather weak hypothesis, which does not seem to be sufficient to deduce interesting properties of the associated monoid or group in general. Now the point is that, provided the complement mapping satisfies certain effective conditions, which is the case for the braid complement θ_R, then many properties automatically follow. We refer to [6] for a complete development about braid word reversing, and just mention here those results we need in the sequel.

Proposition 2.2. *Assume that w is a braid word. Then there exist an integer $c_R(w)$ and two positive words $N_R(w)$, $D_R(w)$ such that every sequence of word reversing from w leads in $c_R(w)$ steps to the word $N_R(w)D_R(w)^{-1}$.*

For instance, in he case of the word w of Example 2.1, the words $N_R(w)$ and $D_R(w)$ are $\sigma_2\sigma_1\sigma_3\sigma_2\sigma_4\sigma_3\sigma_2\sigma_1$ and $\sigma_3\sigma_4\sigma_2\sigma_3\sigma_1\sigma_2\sigma_3\sigma_4$.

It follows from (2.2) that, if the braid word w is reversible to w', then, in particular, w and w' are equivalent. Thus, Proposition 2.2 implies that

$$w \equiv N_R(w)\; D_R(w)^{-1} \tag{2.3}$$

holds for every braid word w, and, therefore, an application is Garside's well-known result that every braid can be expressed as a right fraction ab^{-1} with a, b in the positive braid monoid B_∞^+. This explains our notation, where N_R means "right numerator", and D_R means "right denominator". However, Proposition 2.2 tells us a little more than a mere equivalence of w and $N_R(w)D_R(w)^{-1}$ as it gives a distinguished way for transforming w into $N_R(w)D_R(w)^{-1}$. The point is that this transformation avoids introducing any new factor of the type $\sigma_i^{-1}\sigma_i$ or $\sigma_i\sigma_i^{-1}$.

About the number $c_R(w)$, an upper bound $O(\ell^2 2^n)$ can be proved for w an n-strand braid word of length ℓ. Hence, when n is not bounded, the only uniform upper bound proved so far is an exponential function of the length. Actually, we have no example with more than a cubic complexity, and we conjecture that the optimal upper bound is polynomial (presumably cubic).

Let us observe that braid word reversing is defined only at the level of braid words, and not of braids. Indeed, the functions N_R and D_R do not induce well-defined mapping of B_∞ into B_∞^+. For instance, let $w = \sigma_1\sigma_1^{-1}$ and $w' = \varepsilon$. Then w and w' are equivalent, as both represent the unit braid. Now, by definition, each of w, w' is terminal with respect to word reversing, as it contains no factor $\sigma_i\sigma_j^{-1}$, and we find

$$N_R(\sigma_1\sigma_1^{-1}) = D_R(\sigma_1\sigma_1^{-1}) = \sigma_1, \quad N_R(\varepsilon) = D_R(\varepsilon) = \varepsilon,$$

which shows that $w \equiv w'$ does *not* implie $N_R(w) \equiv N_R(w')$ or $D_R(w) \equiv D_R(w')$. Nevertheless, there exists a connection between the numerators and denominators of equivalent braid words:

Lemma 2.3. *Assume that w and w' are equivalent braid words. Then there exist two positive braid words v, v' satisfying*

$$N_R(w)\ v \equiv N_R(w')\ v' \quad \text{and} \quad D_R(w)\ v \equiv D_R(w')\ v'. \tag{2.4}$$

By construction, the braid relations are symmetric, and everything we said so far about right word reversing can be transposed into a similar statement about *left* braid word reversing. We introduce the mapping θ_L of $\Sigma \times \Sigma$ into Σ^* by

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

and we see that the braid relations (1.1) also consist of the family of all relations

$$\theta_L(\sigma_i, \sigma_j)\ \sigma_j \equiv \theta_R(\sigma_j, \sigma_i)\ \sigma_i \tag{2.5}$$

for $i \neq j$. We observe now that (2.5) implies

$$\sigma_i\ \sigma_j^{-1} \equiv \theta_L(\sigma_j, \sigma_i)^{-1}\ \theta_L(\sigma_i, \sigma_j), \tag{2.6}$$

and we naturally define left braid word reversing by saying that w' is obtained from w by k steps of left word reversing if one can transform w into w' by successively replacing k factors of the type $\sigma_i\sigma_j^{-1}$ with the corresponding factor $\theta_L(\sigma_j, \sigma_i)^{-1}\ \theta_L(\sigma_i, \sigma_j)$. The counterpart of Proposition 2.2 is:

Proposition 2.4. *Assume that w is a braid word. Then there exist an integer $c_L(w)$ and two positive words $N_L(w)$, $D_L(w)$ such that every sequence of word reversing from w leads in $c_L(w)$ steps to the word $D_R(w)^{-1}N_L(w)$.*

The words $N_L(w)$ and $D_L(w)$ are called the left numerator and the left denominator of w. Of course, as for the functions N_R and D_R, the left functions N_L and D_L do not induce well-defined mappings on braids. However, let us mention here that, when a double, left and right, word reversing is used, then the resulting mappings induce well-defined mappings on braids (we shall not use this result in the sequel).

Proposition 2.5. *For w a braids word, define $N_{RL}(w) = N_L(N_R(w)D_R(w)^{-1})$ and $D_{RL}(w) = D_L(N_R(w)D_R(w)^{-1})$. Then the mappings N_{RL} and D_{RL} induce well-defined mappings on braids, i.e., $w \equiv w'$ implies $N_{RL}(w) \equiv N_{RL}(w')$ and $D_{RL}(w) \equiv D_{RL}(w')$.*

The construction of the words $N_{RL}(w)$ and $D_{RL}(w)$ is very simple: starting with w, we first reverse it to the right, obtaining the word $N_R(w)D_R(w)^{-1}$, and we then reverse the latter word to the left: the final word is a left fraction, which we call $D_{RL}(w)^{-1}N_{RL}(w)$. Observe that we obtain in this way a simple solution to the word problem of braids, *i.e.*, to the question of algorithmically recognizing whether a given braid word represents or not the unit braid.

Corollary 2.6. *Assume that w is a braid word. Then $w \equiv \varepsilon$ holds if and only if the words $N_{RL}(w)$ and $D_{RL}(w)$ are empty.*

Proof. As $N_{RL}(\varepsilon) = D_{RL}(\varepsilon) = \varepsilon$ trivially holds, applying Proposition 2.5 in the case $w \equiv \varepsilon$ gives $N_{RL}(w) \equiv D_{RL}(w) \equiv \varepsilon$. Now, for a positive braid word to be equivalent to the empty word implies being *equal* to the empty word. ■

Let us finally mention that, for every braid word w, the word $D_{RL}(w)^{-1}N_{RL}(w)$ happens to be the shortest left fraction equivalent to w, *i.e.*, the shortest word of the form $u^{-1}v$ with u, v in Σ^*. Using this remark and the normal form result of [1] for positive braids leads to a new construction of the greedy normal form of [10] and [9].

3. Action of braids on left cancellative LD-systems

We have described in Section 1 a natural action of the braid monoid B_n^+ on the n-th power of every LD-system by means of braid colourings, and observed that the action can be extended to the whole braid group B_n when the considered LD-system admits bijective left translations, *i.e.*, when it is what we have called an LD-quasigroup. In this section, we show how to extend the result to LD-systems where left translations are only suppoed to be injective, at the expense of obtaining a partial action only. The existence and uniqueness of this partial action relies on using the braid word reversing technique of Section 2.

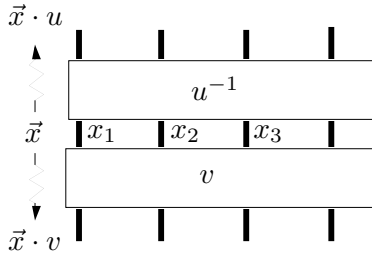
Definition. Assume that $(S, *)$ is an LD-system and w is an n-strand braid word, $n \leq \infty$. We say that a pair of sequences $(\vec{a}, \vec{c})$ in S^n is an *S-colouring* for w if colours from S can be attributed to each segment in the canonical diagram associated with w in such a way that $\vec{a}$ are the input (top) colours, $\vec{c}$ are the output (bottom) colours, and the rules

are obeyed at each crossing.

If w is a positive braid word, we know that, for every sequence $\vec{a}$ in S^n, the pair $(\vec{a}, \vec{a} \cdot w)$ is a colouring of w, and, if S is an LD-quasigroup, the same holds for every braid word. The point is that, even if the LD-system we consider is not an LD-quasigroup, S-colourings exist for every braid word.

Lemma 3.1. *Assume that $(S, *)$ is an LD-system and u, v are positive n-strand braid words. Then, for every sequence $\vec{x}$ in S^n, the pair $(\vec{x} \cdot u, \vec{x} \cdot v)$ is an S-colouring for $u^{-1}v$.*

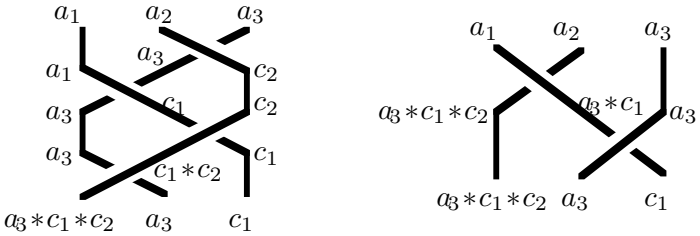
Proof. (See figure below) We apply the colours $\vec{x}$ in the middle of the diagram associated with $u^{-1}v$ and propagate them upwards through u^{-1} and downwards through v. So we obtain $\vec{x} \cdot u$ on the top of the diagram, and $\vec{x} \cdot v$ on the bottom. By construction, the rules of colouring are obeyed in each part of the diagram. ∎



We know that every braid can be represented by a braid word of the form $u^{-1}v$ with u, v positive braid words, *i.e.*, every braid word w is equivalent to a word of the form above. This, however, is *not* sufficient for concluding that there exists an S-colouring for w: indeed, an S-colouring for a braid word w need not be an S-colouring for every braid word w' that is equivalent to w. Now, the results of Section 2 can be applied.

Lemma 3.2. *Assume that $(S,*)$ is an LD-system. Assume that the braid word w is L-reversible to w', and that $(\vec{a},\vec{c})$ is an S-colouring for w'. Then $(\vec{a},\vec{c})$ is an S-colouring for w as well. In particular, if $(\vec{a},\vec{c})$ is an S-colouring for $D_{\text{L}}^{-1}(w)N_{\text{L}}(w)$, it is an S-colouring for w as well.*

Proof. It suffices to prove the result when w is L-reversible to w' in one step. If w' has been obtained from w by deleting some factor $\sigma_i\sigma_i^{-1}$, or replacing $\sigma_i\sigma_j^{-1}$ with $\sigma_j^{-1}\sigma_i$ with $|j-i|\geq 2$, the result is obvious. Assume that w' has been obtained from w by replacing some factor $\sigma_i\sigma_j^{-1}$ with $|j-i|=1$ by $\sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i$. Assume for instance $i=1$ and $j=2$. So we start with a colouring of $\sigma_2^{-1}\sigma_1^{-1}\sigma_2\sigma_1$, and we wish to construct a colouring of $\sigma_1\sigma_2^{-1}$ with the same end colours. Let a_1, a_2, a_3 be the initial colours. The hypothesis that the rules of colouring are obeyed at the first crossing implies that there exists c_2 in S such that $a_2 = a_3 * c_2$ holds. Similarly, there exists c_1 in S such that $a_1 = a_3 * c_1$ holds. Then the colouring must be as displayed on the figure below, and, then, the colouring displayed on the right answers the question. ■



A similar argument gives the following result, whose proof is left to the reader.

Lemma 3.3. *Assume that $(S,*)$ is an LD-system. Assume that the braid word w is R-reversible to w', and that $(\vec{a},\vec{c})$ is an S-colouring for w. Then $(\vec{a},\vec{c})$ is an S-colouring for w' as well. In particular, if $(\vec{a},\vec{c})$ is an S-colouring for w, it is an S-colouring for $N_{\text{R}}(w)D_{\text{R}}(w)^{-1}$ as well.*

Definition. Assume that $(S,*)$ is an LD-system. For $\vec{a}$ in S^∞ and w a braid word, we say that $\vec{a}$ is *admissible* for w if there exists at least one sequence $\vec{c}$ such that $(\vec{a},\vec{c})$ is an S-colouring of w.

It follows from Lemmas 3.1 and 3.2 that, for every LD-system S and every braid word w, there exists at least one sequence in S^∞ that is admissible for w. We can extend this result to the case of several braid words simultaneously.

Lemma 3.4. *Assume that $(S,*)$ is an LD-system. Let w_1, …, w_n a finite family of braid words. Then there exists a sequence in S^∞ that is admisible for each w_i.*

Proof. Lemma 3.2 implies that every sequence of the form $\vec{x}\cdot uD_{\text{L}}(w)$ with u a positive word is admissible for w. We can find positive words u_1, …, u_n satisfying

$$u_1D_{\text{L}}(w_1) \equiv \ldots \equiv u_nD_{\text{L}}(w_n) :$$

we choose $u_1, \ldots, u_n$ so that $u_i D_L(w_i)$ represents the left lcm of the positive braids represented by $D_L(w_1), \ldots, D_L(w_n)$, which is known to exist in the braid monoid B_∞^+. Then, for every initial choice $\vec{x}$, the common value of the sequences $\vec{x} \cdot u_i D_L(w_i)$ is admissible for w_i. ■

Proposition 3.5. *Assume that $(S, *)$ is a left cancellative LD-system, and w, w' are equivalent braid words. Then, for each sequence $\vec{a}$ in S^∞ that is admissible both for w and w', there exists exactly one sequence $\vec{c}$ such that $(\vec{a}, \vec{c})$ is both an S-colouring of w and w'.*

Proof. Assume that $(\vec{a}, \vec{c})$ is an S-colouring of w, and $(\vec{a}, \vec{c}')$ is a colouring of w'. As w and w' are equivalent, by Lemma 2.3, there exist positive words v, v' satisfying

$$N_R(w)v \equiv N_R(w')v', \qquad D_R(w)v \equiv D_R(w')v'.$$

By Lemma 3.3, $(\vec{a}, \vec{c})$ is also an S-colouring of the word $N_R(w)D_R(w)^{-1}$, and, therefore, it is an S-colouring of $N_R(w)vv^{-1}D_R(w)^{-1}$ too. By construction, we have

$$\vec{a} \cdot N_R(w)v = \vec{c} \cdot D_R(w)v.$$

The same argument gives $\vec{a} \cdot N_R(w')v' = \vec{c}' \cdot D_R(w')v'$, and, therefore, we have

$$\vec{c} \cdot D_R(w)v = \vec{c}' \cdot D_R(w')v' = \vec{c}' \cdot D_R(w)v.$$

This implies $\vec{c} = \vec{c}'$. Indeed, it suffices for an induction to show that $\vec{x} \cdot \sigma_i = \vec{x}\,' \cdot \sigma_i$ implies $\vec{x} = \vec{x}\,'$. The hypothesis implies $x_i = x_i'$ and $x_i * x_{i+1} = x_i' * x_{i+1}'$, hence $x_{i+1} = x_{i+1}'$ provided $(S, *)$ admits left cancellation. ■

The previous result applies in particular to the case when the words w and w' coincide, and it tells us that there exists at most one colouring of w with a given initial sequence of colours. It follows that the following definition makes sense:

Definition. Assume that $(S, *)$ is a left cancellative LD-system. For w a braid word and $\vec{a}$ a sequence in S^∞, $\vec{a} \cdot w$ is defined to be the unique sequence $\vec{c}$ such that $(\vec{a}, \vec{c})$ is an S-colouring of w, if it exists. If b is a braid, $\vec{a} \cdot b$ is defined to be the sequence $\vec{a} \cdot w$, where w is an arbitrary expression of b such that $\vec{a} \cdot w$ exists, if such an expression exists.

We thus have extended the action of braids to all left cancallative LD-systems, at the expense of having in general a partial action, *i.e.*, one that need not be defined everywhere. In the case of a left cancellative LD-system that is not an LD-quasigroup, the hypothesis that the sequence $\vec{a} \cdot b$ exists does not imply that $\vec{a} \cdot w$ exists for every braid word w that represents b. The important fact is that, yet the action is partial, there always exist sequences that are admissible for a given braid. More precisely, we deduce from Lemma 3.4 the follwing result:

Proposition 3.6. *Assume that $(S, *)$ is a left cancellative LD-system. Then, for every finite family of braids $b_1, \ldots, b_m$ in B_n, there exists at least one sequence $\vec{a}$ in S^n such that $\vec{a} \cdot b_i$ is defined for every i.*

We are thus led to looking for new examples of LD-systems, namely left cancellative LD-systems that need not be LD-quasigroups, *i.e.*, where left division need not be always possible.

Example 3.7. (free LD-systems) It is known [5] that free LD-systems of any rank are left cancellative. Thus they are eligible for the partial action of braids. We shall not investigate this action directly here.

Example 3.8. (injection bracket) The injection bracket of Example 1.13 is left cancellative. Indeed, assume that f, g, g' are (non-surjective) injections of $\mathbf{N}$ into itself satisfying $f[g] = f[g']$. For every nonnegative integer p, $f[g](f(p)) = f[g'](f(p))$ expands into $f(g(p)) = f(g(p'))$, which implies $g(p) = g'(p)$ as f is injective. Hence $(I_\infty, [\,])$ is eligible for the partial braid action.

Example 3.9. (braid exponentiation) Let sh denote the shift endomorphism of the group B_∞ that maps σ_i to σ_{i+1} for every i. Let us define a new binary operation $*$ on B_∞ using the formula

$$a * b = a\ \mathrm{sh}(b)\ \sigma_1\ \mathrm{sh}(a^{-1}). \tag{3.1}$$

The motivation for introducing (3.1) (called braid exponentiation in recent references) is provided by the general theory of left self-distributivity [5]. It is easy to verify that the operation $*$ is left self-distributive, and that the LD-system $(B_\infty, *)$ is left cancellative (the latter point follows from the injectivity of the endomorphism sh). Hence $(B_\infty, *)$ is eligible for the partial braid action.

4. The action of braids on braids

In the sequel, we shall concentrate on the latter action, *i.e.*, the action of braids on braids equipped with the self-distributive operation of (3.1). Here we shall see how this action naturally leads to introducing a linear order of the braids, as an application of general results about LD-systems.

The first technically significant fact is that the action of braids on braids can be connected with a multiplication on the right in B_∞, a property that is reminiscent of Formulas 1.7, 1.9, and 1.12.

Definition. We denote by $B_\infty^{(\infty)}$ the set of all sequences in B_∞^∞ with only finitely many entries not equal to 1, and, for $\vec{x}$ in $B_\infty^{(\infty)}$, we define

$$\mathrm{sh}\Pi(\vec{x}) = \prod_{k=1}^{\infty} \mathrm{sh}^{k-1}(x_k) = x_1\ \mathrm{sh}(x_2)\ \mathrm{sh}^2(x_3)\ldots \tag{4.1}$$

Lemma 4.1. *Assume $\vec{a} \in B_\infty^{(\infty)}$, $b \in B_\infty$, and $\vec{a} \cdot b$ exists. Then we have*

$$\mathrm{sh}\Pi(\vec{a} \cdot b) = \mathrm{sh}\Pi(\vec{a})\ b. \tag{4.2}$$

Proof. We use induction on the minimal length of a braid word w representing b and such that $\vec{a} \cdot w$ exists. If w is empty, everything is clear. The result is true when w is empty.

Assume now $w = \sigma_i w_0$. Let b_0 be the braid represented by w_0. By hypothesis, $\vec{a} \cdot \sigma_i$ and $(\vec{a} \cdot \sigma_i) \cdot b_0$ exist. We find first

$$\begin{aligned}
\mathrm{sh}\Pi(\vec{a} \cdot \sigma_i) &= \mathrm{sh}\Pi((a_1, \dots, a_i * a_{i+1}, a_i, \dots)) \\
&= a_1\ \mathrm{sh}(a_2)\ \dots\ \mathrm{sh}^{i-1}(a_i * a_{i+1})\ \mathrm{sh}^i(a_i)\ \mathrm{sh}^{i+1}(a_{i+2}) \dots \\
&= a_1\ \mathrm{sh}(a_2)\ \dots\ \mathrm{sh}^{i-1}(a_i)\ \mathrm{sh}^i(a_{i+1})\ \sigma_i\ \mathrm{sh}^i(a_i)^{-1}\ \mathrm{sh}^i(a_i)\ \mathrm{sh}^{i+1}(a_{i+2}) \dots \\
&= a_1\ \mathrm{sh}(a_2)\ \dots\ \mathrm{sh}^{i-1}(a_i)\ \mathrm{sh}^i(a_{i+1})\ \sigma_i\ \mathrm{sh}^{i+1}(a_{i+2}) \dots \\
&= a_1\ \mathrm{sh}(a_2)\ \dots\ \mathrm{sh}^{i-1}(a_i)\ \mathrm{sh}^i(a_{i+1})\ \mathrm{sh}^{i+1}(a_{i+2}) \dots\ \sigma_i = \mathrm{sh}\Pi(\vec{a})\ \sigma_i,
\end{aligned}$$

as σ_i commutes with every braid in the image of sh^k with $k \geq i+1$. Applying the induction hypothesis, we deduce $\mathrm{sh}\Pi(\vec{a} \cdot b) = \mathrm{sh}\Pi(\mathrm{sh}\Pi(\vec{a} \cdot \sigma_i))\ b_0 = \mathrm{sh}\Pi(\vec{a})\ \sigma_i\ b_0 = \mathrm{sh}\Pi(\vec{a})\ b$. ■

It follows that the action of B_∞ on $B_\infty^{(\infty)}$ is strongly faithful:

Proposition 4.2. *Assume that b and b' are braids in B_∞ and there exists at least one sequence $\vec{a}$ in $B_\infty^{(\infty)}$ such that $\vec{a} \cdot b$ and $\vec{a} \cdot b'$ are defined and equal. Then b and b' are equal.*

Proof. By Lemma 4.1, $\vec{a} \cdot b = \vec{a} \cdot b' = \vec{c}$ implies $b = \mathrm{sh}\Pi(\vec{c})\ \mathrm{sh}\Pi(\vec{a})^{-1} = b'$. ■

We shall now use the partial action of braids on braids to construct a linear ordering on B_∞. To this end, we introduce a certain subset of B_∞. For every braid b, there exists a least sub-LD-system of $(B_\infty, *)$ that contains b, namely the closure of the singleton $\{b\}$ under operation $*$. A significant rôle is played by the closure of $\{1\}$ in the sequel.

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

By construction, every special braid has an expression involving the trivial braid 1 and operation $*$ exclusively. Thus, for instance, 1, $1 * 1$, which is σ_1, $(1 * 1) * 1$, which is $\sigma_1^2 \sigma_2^{-1}$, $1 * (1 * 1)$, which is $\sigma_2 \sigma_1$, are special braids.

By definition, special braids equipped with operation $*$ form a left cancellative LD-system, and, therefore, we can use them to colour the strands of the braids. In particular, restating Proposition 3.6 in this case yields:

Proposition 4.3. *For every finite family of braids $b_1, \dots, b_m$ in B_n, there exists at least one sequence $\vec{a}$ of special braids such that $\vec{a} \cdot b_i$ is defined and consists of special braids for every i.*

Applying Formula (4.2) in the case of special braids leads to a decomposition of every braid in terms of special braids.

Definition. Assume that b is a braid.We say that $\vec{c}$ is a *special decomposition* for b if $\vec{c}$ is a sequence of special braids satisfying $b = \mathrm{sh}\Pi(\vec{c})$.

Lemma 4.4. *Every positive braid admits a special decomposition.*

Proof. For $b \in B_\infty^+$, the sequence $(1, 1, \dots) \cdot b$ is always defined, since possible obstructions occur only with negative crossings. It consists of special braids, as special braids are closed under $*$. ■

As every braid is the quotient of two positive braids, we deduce:

Corollary 4.5. *Every braid can be expressed under the form*

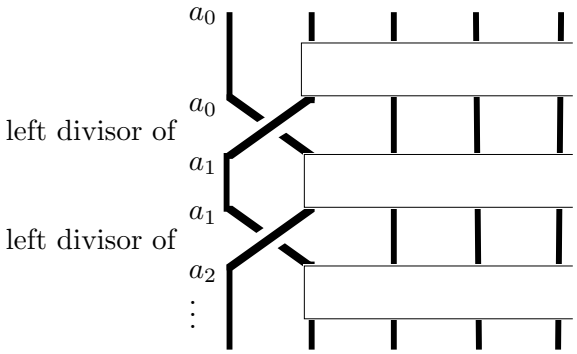
$$\dots\ \mathrm{sh}^{i-1}(a_i)^{-1}\ \dots\ \mathrm{sh}(a_2)^{-1}\ a_1^{-1}\ c_1\ \mathrm{sh}(c_2)\ \dots\ \mathrm{sh}^{i-1}(c_i)\ \dots$$

where a_1, a_2, ..., c_1, c_2, ... are special braids.

In order to go further, we shall use without proof two results of self-distributive algebra. The first deals with operation $*$ on B_∞.

Proposition 4.6. *Left division in the LD-system $(B_\infty, *)$ has no cycle.*

This result was first proved in [5]. A simpler proof appears in [15]. It can be observed that the result is straightforward once at least one example of a left cancellative LD-system where left division has no cycle is known (and one can prove that a free LD-system is such an example). Indeed, using the explicit definition of the operation $*$, we see that a possible cycle for left division in $(B_\infty, *)$ would give a braid word w representing the unit braid, and such that σ_1 occurs in w, but σ_1^{-1} does not. Assume that $(S, *)$ is a left cancellative LD-system where left division has no cycle, and that w is an n-strand braid word as above. We let w act on S^n: there exists at least one sequence $\vec{a}$ in S^n such that $\vec{a}\cdot w$ exists. Now, by definition, the successive colours on the leftmost strand make a strictly increasing sequence with respect to left division in S. As left division is supposed to have no cycle, this implies that the final colour of the leftmost strand does not coincide with the initial colour of the leftmost strand, and, therefore, w cannot represent the unit braid.



The second result we shall use without proof is a general property of monognerated LD-systems, which also appears in [5]. For $(S, *)$ a binary system, and a, b in S, we say that a is an *iterated left divisor* of b, and write $a \sqsubset b$, if there exists some positive integer p, and some elements b_1, ..., b_p in S satisfying

$$b = (\dots((a * b_1) * b_2 \dots) * b_p. \tag{4.3}$$

Proposition 4.7. *Assume that $(S, *)$ is a monogenerated LD-system. Then any two elements of S are comparable with respect to the iterated left divisibility relation, i.e., for all a, b in S, at least one of $a \sqsubset b$, $a = b$, $a \sqsupset b$ holds.*

Applying this result to the LD-system of special braids, we deduce:

Proposition 4.8. *The relation $\sqsubseteq$ on special braids is a linear ordering that extends the left divisibility relation of $*$, i.e., $a \sqsubset a * b$ holds for all a, b.*

For instance, the sequence 1, $1*1$, $(1*1)*1$, $((1*1)*1)*1$, ... is increasing in $(B_\infty^{sp}, \sqsubset)$, which corresponds to the explicit inequalities

$$1 \sqsubset \sigma_1 \sqsubset \sigma_1^2\sigma_2^{-1} \sqsubset \sigma_1^2\sigma_2^{-1}\sigma_1\sigma_3\sigma_2^{-2} \sqsubset \dots$$

A crucial property of the order $\sqsubseteq$ on B_∞^{sp} is that it can be characterized explicitly in terms of occurrences of the generator σ_1.

Lemma 4.9. *Assume that a, b are special braids; Then the following are equivalent:*
(i) The relation $a \sqsubset b$ holds;
(ii) The braid $a^{-1}b$ admits an expression where σ_1 occurs, but σ_1^{-1} does not.

Proof. Assume $a \sqsubset b$. By construction, this means that there exists special braids b_1, ..., b_p satisfying (3.4). Expanding the latter expression gives

$$b = a\ \mathrm{sh}(b_1)\ \sigma_1\ \mathrm{sh}(c_1)\ \sigma_1\ \dots\ \sigma_1\ \mathrm{sh}(c_p),$$

with $c_k = ((\dots((a*b_1)*b_2)\dots)*b_k)^{-1}b_{k+1}$. Hence the braid $a^{-1}b$ admits an expression where σ_1 occurs p times and σ_1^{-1} does not occur.

Conversely, assume that $a \sqsubset b$ does not hold. Then either we have $a = b$, hence $a^{-1}b = 1$, or $b \sqsubset a$ holds, and, by the previous argument, $b^{-1}a$ admits an expression where σ_1 occurs, but σ_1^{-1} does not, hence $a^{-1}b$ admits an expression where σ_1^{-1} occurs, but σ_1 does not. In both cases, Proposition 4.6 implies that $a^{-1}b$ cannot admit an expression where σ_1 occurs, but σ_1^{-1} does not. ∎

Assume that b and b' are arbitrary braids. By Proposition 3.12, we know that there exists at least one sequence of special braids $\vec{a}$ such that both $\vec{a}\cdot b$ and $\vec{a}\cdot b'$ exist and consist of special braids. Now special braids are equipped with a linear order, and there exists a natural lexicographical extension of this ordering into a linear ordering of special sequences: for $\vec{a}$, $\vec{a}'$ special sequences, say $\vec{a} = (a_1, a_2, \dots)$, $\vec{a}' = (a'_1, a'_2, \dots)$, we say that $\vec{a} \sqsubset^{Lex} \vec{a}'$ is true if $a_k \sqsubset a'_k$ holds for the first index k satisfying $a_k \neq a'_k$. The obvious idea is to define the braid b to be smaller than the braid b' if the sequence $\vec{a}\cdot b$ is smaller than $\vec{a}\cdot b'$ with respect to $\sqsubset^{Lex}$.

In order to make the intuition rigorous, we have to verify that the previous comparison of b and b' does not depend on the choice of the special sequence $\vec{a}$. Verification is easy, because the order admits another equivalent intrinsic definition.

Definition. Let b be a braid. We say that b is *σ_1-positive* (*resp. σ_1-negative*) if it admits at least one expression where the letter σ_1 occurs, but σ_1^{-1} does not (*resp.* σ_i^{-1} occurs but σ_i does not). We say that b is *σ-positive* (*resp. σ-negative*) if there exists a nonnegative integer k such that b is the image under sh^k of a σ_1-positive braid (*resp.* of a σ_1-negative braid).

With these notions, Proposition 4.6 states that a σ_1-positive braid is never trivial, and Lemma 4.9 states that, if a and b are special braids, then $a \sqsubset b$ holds if and only if $a^{-1}b$ is σ_1-positive.

Lemma 4.10. *Assume that b is a σ-positive braid. Then b is neither the unit braid, nor a σ-negative braid.*

Proof. Assume that b is both $\mathrm{sh}^i(b_1)$ and $\mathrm{sh}^j(b_2^{-1})$ where b_1 is σ_1-positive and b_2 is σ_1-positive or equal to 1. Assume $i \leq j$. Then $b_1\ \mathrm{sh}^{j-i}(b_2)$ is a σ_1-positive braid, contradicting Proposition 4.6. ∎

Lemma 4.11. *Assume that b, b' are braids. Then the following are equivalent:*

(i) There exists a sequence $\vec{a}$ of special braids such that $\vec{a} \cdot b$ and $\vec{a} \cdot b'$ exist, consist of special braids, and $\vec{a} \cdot b \sqsubset^{Lex} \vec{a} \cdot b'$ holds;

(ii) The braid $b^{-1}b'$ is σ-positive.

Proof. Assume (i). Let $\vec{c}$ and $\vec{c}'$ denote respectively the sequences $\vec{a} \cdot b$ and $\vec{a} \cdot b'$. By Lemma 4.1, we have $\mathrm{sh}\Pi(\vec{c}) = \mathrm{sh}\Pi(\vec{a})\ b$, and $\mathrm{sh}\Pi(\vec{c'}) = \mathrm{sh}\Pi(\vec{a})\ b'$. So we deduce

$$b^{-1}\ b' = \mathrm{sh}\Pi(\vec{c})^{-1}\ \mathrm{sh}\Pi(\vec{c}'). \tag{4.4}$$

By definition, there exists an integer i such that $c_k = c'_k$ holds for $k < i$, and $c_i \sqsubset c'_i$ holds. Thus (4.4) takes the form

$$b^{-1}\ b' = \mathrm{sh}^i(\mathrm{sh}(c^{-1})\ c_i^{-1}\ c'_i\ \mathrm{sh}(c'))$$

for some c, c'. By Lemma 4.9, the braid $c_i^{-1}\ c'_i$ is σ_1-positive, and so is the braid $\mathrm{sh}(c^{-1})\ c_i^{-1}\ c'_i\ \mathrm{sh}(c')$. Hence the braid $b^{-1}b'$ is σ-positive, as it admits a decomposition where σ_i occurs, and neither σ_i^{-1} nor any $\sigma_k^{\pm 1}$ with $k < i$ occurs.

Conversely, assume that the braid $b^{-1}b'$ is σ-positive. Let $\vec{a}$ an arbitrary sequence of special braids such that both $\vec{a} \cdot b$ and $\vec{a} \cdot b'$ exist and consist of special braids. As $\sqsubset^{Lex}$ is a linear order on sequences of special braids, it suffices that we show that both $\vec{a} \cdot b = \vec{a} \cdot b'$ and $\vec{a} \cdot b' \sqsubset^{Lex} \vec{a} \cdot b$ are impossible. Now, the first relation implies $b = b'$, hence $b^{-1}b' = 1$. The second relation implies that the braid $b^{-1}b'$ is σ-negative. Both are incompatible with the hypothesis of $b^{-1}b'$ being σ-positive. ∎

Definition. Assume that b, b' are braids. We say that $b <_L b'$ is true if one of the equivalent conditions of Lemma 4.11 holds.

Proposition 4.12. *(i) Every braid b, $b \neq 1$, is either σ-positive or σ-negative.*

(ii) The relation $\leq_L$ is a linear ordering on B_∞ that extends the ordering $\sqsubseteq$ of special braids. It is compatible with multiplication on the left.

Proof. Point (i) follows from the previous lemma, as the lexicographical ordering on special sequences is, by construction, a linear ordering. For (ii), the product of two σ-positive braids is a σ-positive braids, hence the relation $\leq_L$ is transitive. Moreover $b <_L b$ is impossible, as the unit braid 1 is not σ-positive. Hence $\leq_L$ is an ordering. It extends the previously defined order on B_∞^{sp} as a σ_1-positive braid is σ-positive by definition. ∎

It is easy to prove that $\leq_L$ is the unique ordering on B_∞ that is compatible with multiplication on the left and shift, and satisfies $1 <_L \mathrm{sh}(b)\sigma_1\mathrm{sh}(b')$ for all b, b'.

The main property of this order known to date is the following result of Laver [16], as improved by Burckel [3]:

Proposition 4.13. *For every integer, the restriction of the linear order $\leq_L$ to positive n-strand braids is a well-ordering whose type is the ordinal $\omega^{\omega^{n-2}}$.*

The braid ordering plays a crucial rôle in the quick algorithm for the word problem of braids described in [8]. Let us finally mention that new definitions $\leq_L$ in terms of mapping class groups and of hyperbolic geometry have been given recently in [11] and [19] respectively.

References

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

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

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

[4] P. Dehornoy, *Algebraic properties of the shift mapping*, Proc. Amer. Math. Soc. **106-3** (1989) 617–623.

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

[6] —, *Groups with a complemented presentation*, J. Pure Appl. Algebra **116** (1997) 115–137.

[7] —, *From large cardinals to braids via distributive algebra*, J. Knot Theory & Ramifications **4-1** (1995) 33–79.

[8] —, *A fast method for comparing braids*, Advances in Math. **125** (1997) 200–235.

[9] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford **45-2** (1994) 479–497.

[10] D. Epstein & *al.*, *Word Processing in Groups*, Jones & Barlett Publ. (1992).

[11] R. Fenn, M.T. Greene, D. Rolfsen, C. Rourke & B. Wiest, *Ordering the braid groups*, Pacific J. of Math., to appear.

[12] R. Fenn & C. P. Rourke, *Racks and links in codimension 2*, J. of Knot Theory and its Ramifications (1992) 343–406;

[13] F. A. Garside, *The braid group and other groups*, Quart. J. Math. Oxford **20** No.78 (1969) 235–254.

[14] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. of Pure and Appl. Algebra **23** (1982) 37–65;

[15] D.M. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994) 104–112.

[16] R. Laver, *Braid group actions on left distributive structures and well-orderings in the braid group*, J. Pure Appl. Algebra **108-1** (1996) 81–98.

[17] S. V. Matveev, *Distributive Groupoids in Knot Theory*, Math. Sbornik **119, 1-2** (1982) 73–83.

[18] Prasolov, V.V. & A.B. Sossinsky, *Knots, links, braids, and 3-manifolds (in Russian)*, MCCME (1997).

[19] H. Short & B. Wiest, *Ordering the mapping class groups after Thurston*, preprint.

Laboratoire SDAD, ESA 6081 CNRS
Mathématiques, BP 5186
Université Campus II, 14 032 Caen, France

dehornoy@math.unicaen.fr
http://www.math.unicaen.fr/∼dehornoy/