STRANGE QUESTIONS ABOUT BRAIDS

Patrick DEHORNOY
SDAD ESA 6081
Département de mathématiques
Université Campus II, BP 5186, 14 032 Caen, France
dehornoy@math.unicaen.fr

ABSTRACT

The infinite braid group B_∞ admits a left self-distributive structure. In particular, it includes a free monogenerated left self-distributive system, and, therefore, it inherits all properties of the latter object. Here we discuss how such algebraic properties translate into the language of braids. We state new results about braids and propose a list of open questions.

Keywords: Braid groups, self-distributive law, ordered group.
AMS Subject Classification: 20F36

There exists a deep connection between the geometry of braids, described by Artin's braid group B_∞, and the geometry of the left self-distributivity identity $x(yz) = (xy)(xz)$, which turns out to be described by some extension of B_∞ [5]. One of the consequences of this connection is the existence of a left self-distributive operation on braids, called here braid exponentiation. This operation is highly non-trivial, and, in particular, every braid in B_∞ generates under exponentiation a free left self-distributive system—a free LD-system for short.

In recent years, a number of properties of LD-systems in general and of free LD-systems in particular have been established, either by a direct algebraic approach [5] [6] [15] [16] ..., or as an application of results about elementary embeddings in set theory [25] [26] [14]... Let us define a special braid to be a braid that can be generated from the unit braid using solely braid exponentiation. Then special braids form a free LD-system, and, therefore, they inherit all properties of such systems. So every algebraic result about free LD-systems must admit a counterpart in the language of braids. In this paper, we investigate such translations.

This study leads to new results about braid exponentiation, and about the linear ordering of braids introduced in [5] and reconstructed recently in [18]. The main new results we establish in this paper are: a complete study of left and right division in the system $(B_\infty, {}^\wedge)$; an intrinsic combinatorial characterization of special braids, which was missing up to now, and which results in an effective algorithm for recognizing special braids; a seemingly optimal compatibility result between the linear ordering of braids and their exponentiation, namely that $b < a{}^\wedge b$ holds for every b when a is positive or special; an explicit embedding of the extended braids defined in [12] into B_∞ and a characterization of its image.

Besides, we are naturally led to a number of new open questions. Typically, such questions arise when we consider the possible extension to arbitrary braids of those properties of special braids that come from self-distributive algebra. Most of these "strange" questions about braids seem to be non-trivial, and we hope that they can be of interest for topologists.

The paper comprises five sections. In Section 1, we investigate braid exponentiation and the associated division and iterated power operations. In Section 2, we concentrate on special braids, and their connection with the action of braids on self-distributive systems. In Section 3, we consider the linear ordering of braids and its compatibility with braid exponentiation. In Section 4, we discuss the possible projection of the previous properties onto quotients of the braid group B_∞. Finally, we consider in Section 5 the extended braids of [12], which leads to new questions about (ordinary) braids.

The author thanks M. Picantin for helpful comments, and R. Fenn for pointing out an inaccuracy.

1. Braid Exponentiation

We follow the standard notations of [1]: B_n denotes the group of n strand braids, which can be defined as the group generated by $n-1$ generators $\sigma_1, \ldots, \sigma_{n-1}$ submitted to the relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{for } |i-j| \geq 2, \qquad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}. \tag{1.1}$$

Here σ_i corresponds to the elementary braid where the $(i+1)$-th strand crosses over the i-th strand. The group B_∞ is the direct limit of the groups B_n with respect to the natural embedding of B_n into B_{n+1} that corresponds to adding a new strand on the right. In other words, B_∞ is the group generated by an infinite sequence of generators $\sigma_1, \sigma_2, \ldots$ indexed by the positive integers and submitted to (1.1). Positive braids are defined as those braids that admit at least one expression where no negative letter σ_i^{-1} occurs. The monoid of all positive braids is denoted by B_∞^+. It will be convenient to use the specific notation τ_p for the positive braid that lets the $p+1$-th strand cross over the strands 1 to p, *i.e.*, $\tau_p = \sigma_p \ldots \sigma_2\sigma_1$. We define τ_0 to be the unit braid 1.

Figure 1.1. The braid τ_p (here $p = 3$)

As was shown in [5], a new binary operation on B_∞ arises as the projection on B_∞ of a canonical operation on some extension of B_∞ that describes the geometry of the left self-distributive identity. This operation is the braid exponentiation defined by

$$a^\wedge b = a \cdot \mathrm{sh}(b) \cdot \sigma_1 \cdot \mathrm{sh}(a)^{-1},$$

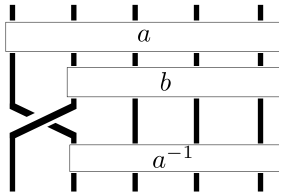


Figure 1.2. The braid $a\hat{}b$

(We recall that sh is the shift endomorphism of B_∞.)

The following result is proved in [5]:

Proposition 1.1. *Every braid in B_∞ generates a free LD-system under exponentiation.*

The result applies in particular to the unit braid 1 (the braid that is represented by a diagram with no crossing).

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

So, every special braid admits an expression involving only 1 and exponentiation. For instance, 1, σ_1, which is 1^1, $\sigma_2\sigma_1$, which is 1^(1^1), $\sigma_1^2\sigma_2^{-1}$, which is (1^1)^1, ... are special braids.

1.1. Left division

We consider first left division in the system $(B_\infty, \hat{}\,)$. Because the shift endomorphism of the group B_∞ is injective, braid exponentiation is left cancellative: $a\hat{}b = a\hat{}b'$ implies $b = b'$. It follows that, when we are given two braids a and c, there exists at most one braid b satisfying $a\hat{}b = c$. Here we study whether such a quotient actually exists. In the case of special braids, the answer is known.

Proposition 1.2. *Assume that a and c are special braids. Then the following are equivalent:*
(i) There exists a special braid b satisfying $a\hat{}b = c$;
(ii) The equality $a\hat{}c = (a\hat{}a)\hat{}c$ holds.

Proof. The fact that (i) implies (ii) does not use the hypothesis that a and b are special: it results from the equality $a\hat{}(a\hat{}b) = (a\hat{}a)\hat{}(a\hat{}b)$, which trivially holds in every LD-system. The converse implication is proved in [6] (in the context of abstract free LD-systems) using the existence of a unique normal form for the elements of a monogenerated free LD-system (a rather sophisticated result—using the normal form of [25] is also possible). ∎

The previous result suggests naturally that we look for a similar criterion in the case of arbitrary braids. We begin with an easy remark.

Lemma 1.3. *For b in B_∞, the following are equivalent:*
(i) The braids $\mathrm{sh}(b)$ *and* σ_1 *commute;*
(ii) The braid b belongs to $\mathrm{sh}(B_\infty)$.

Proof. It is clear that (ii) implies (i). Conversely, assume that b belongs to B_n. Then, using the "handle trick" of Figure 1.3, we have

$$\mathrm{sh}(b)^{-1}\,\sigma_1^{-1}\,\mathrm{sh}(b)\,\sigma_1 = \mathrm{sh}(b)^{-1}\,\sigma_2 \ldots \sigma_n\, b\, \sigma_n^{-1} \ldots \sigma_2^{-1}. \tag{1.2}$$

So, if $\mathrm{sh}(b)$ and σ_1 commute, we obtain

$$b = \sigma_n^{-1} \ldots \sigma_2^{-1}\,\mathrm{sh}(b)\,\sigma_2 \ldots \sigma_n,$$

and the latter expression belongs to $\mathrm{sh}(B_\infty)$ explicitely. ■

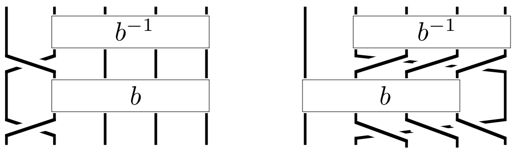


Figure 1.3: The handle trick

(See [19] for more general results about centralizers in B_∞.) We can easily prove the counterpart of Proposition 1.2.

Proposition 1.4. *Assume that a and c are braids. Then the following are equivalent:*
(i) There exists a braid b satisfying $a\hat{\ }b = c$;
(ii) The equality $a\hat{\ }c = (a\hat{\ }a)\hat{\ }c$ holds.

Proof. As above, (i) obviously implies (ii). Conversely, the equality $a\hat{\ }b = c$ develops into
$$\mathrm{sh}(b) = a^{-1}\,c\,\mathrm{sh}(a)\,\sigma_1^{-1},$$
so (i) is equivalent to the braid $a^{-1}\,c\,\mathrm{sh}(a)\,\sigma_1^{-1}$ belonging to $\mathrm{sh}(B_\infty)$. By Lemma 1.3, the latter condition is equivalent to the fact that $\mathrm{sh}(a^{-1}\,c\,\mathrm{sh}(a)\,\sigma_1^{-1})$ commutes with σ_1. Now, developing $a\hat{\ }c = (a\hat{\ }a)\hat{\ }c$ gives

$$\mathrm{sh}(c)\,\sigma_1 = \mathrm{sh}(a)\,\sigma_1\,\mathrm{sh}(a^{-1}\,c)\,\sigma_1\,\mathrm{sh}^2(a)\,\sigma_2^{-1}\,\mathrm{sh}^2(a^{-1}),$$

which is equivalent to

$$\mathrm{sh}(a^{-1} c\,\mathrm{sh}(a)\,\sigma_1^{-1}) = \sigma_1\,\mathrm{sh}(a^{-1}\,c\,\mathrm{sh}(a)\,\sigma_1^{-1})\,\sigma_1^{-1}.$$

This is precisely the above condition that $\mathrm{sh}(a^{-1}\,c\,\mathrm{sh}(a)\,\sigma_1^{-1})$ and σ_1 commute. So (ii) implies (i). ■

1.2. Right division

The case of right division is different, as no uniqueness can be expected in general: we just have seen above that, if c is equal to a^b, then a^c and $(a$^$a)$^c are equal, a result that holds in $(B_\infty,$ ^$)$ as well as in each LD-system. However, we can study right division rather easily. The following technical result will be used several times in the sequel.

Lemma 1.5. *Assume that b is a braid in B_∞, and n is a positive integer. The following are equivalent:*
(i) The braid b belongs to B_n;
(ii) The equality

$$\mathrm{sh}(b) = \tau_n^{-1}\, b\, \tau_n \tag{1.3}$$

holds.

Proof. The fact that (i) implies (ii) follows from Figure 1.4 below. For the converse implication, we assume $b \neq 1$. Let p be the least index such that b belongs to B_p. If $p > n$ holds, the braid $\tau_n^{-1}\, b\, \tau_n$ belongs to B_p, while $\mathrm{sh}(b)$ does not, so (1.3) is impossible. ■

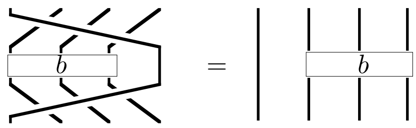


Figure 1.4: The shift in B_n

Lemma 1.6. *Assume that b belongs to B_n, and $p < n$ holds. Then the following are equivalent:*
(i) The braid b belongs to B_p;
(ii) The braid b commutes with $\sigma_n \ldots \sigma_{p+1}$.

Proof. By Lemma 1.5, b belongs to B_p if and only if $\mathrm{sh}(b)$ is equal to $\tau_p^{-1}\, b\, \tau_p$. Now, as b belongs to B_n, $\mathrm{sh}(b)$ is equal to $\tau_n^{-1}\, b\, \tau_n$. The equality $\tau_p^{-1}\, b\, \tau_p = \tau_n^{-1}\, b\, \tau_n$ amounts to b commuting with $\tau_n \tau_p^{-1}$. ■

We are now ready to describe right division in $(B_\infty,$ ^$)$. In the sequel, we say that two braids b, b' in B_∞ are *B_n-conjugate* if there exists some braid a in B_n such that $b' = aba^{-1}$ holds. The well-known solution by Garside of the conjugacy problem of B_n [21] does not solve the "partial conjugacy problem" of recognizing whether two braids in $B_{n'}$, $n' > n$, are B_n-conjugate. However, the argument showing that the conjugacy problem of a biautomatic group is solvable shows that the partial conjugacy problem associated with a parabolic subgroup is solvable as well, and this applies in particular to the parabolic subgroup B_n of $B_{n'}$ when $n' > n$ holds. Indeed, using the notations of [17, Th. 2.5.7], deciding whether b and b' are B_n-conjugate amounts to deciding whether the (effectively computable) automaton $M_{b'}^{b}$ accepts at least one word over the alphabet $\{\sigma_1, \ldots, \sigma_{n-1}\}$.

Proposition 1.7. *Assume that b, c are braids. Then the following are equivalent:*

(i) There exists a in B_n satisfying $a \wedge b = c$;

(ii) The braids $c\,\tau_n^{-1}$ and $\mathrm{sh}(b\tau_{n-1}^{-1})$ are B_n-conjugate.

If the previous conditions are satisfied, the braids a in B_n satisfying $a \wedge b = c$ are those braids of the form $a_0 d$, where a_0 is an arbitrary braid satisfying $a_0 \wedge b = c$ and d is an arbitrary braid that commutes with $\mathrm{sh}(b\tau_{n-1}^{-1})$.

Proof. Assume that a belongs to B_n. Using (1.3), we obtain, for every b, the equality

$$a \wedge b = a\,\mathrm{sh}(b\tau_{n-1}^{-1})\,a^{-1}\,\tau_n. \tag{1.4}$$

Hence, $a \wedge b = c$ is equivalent to

$$c\,\tau_n^{-1} = a\,\mathrm{sh}(b\tau_{n-1}^{-1})\,a^{-1}. \tag{1.5}$$

Thus the equivalence of (i) and (ii) is proved. Assume now that $c = a_0 \wedge b$ holds. Then, by (1.5), $c = (a_0 d) \wedge b$ holds if and only if $\mathrm{sh}(b\tau_{n-1}^{-1})$ is equal to $d\,\mathrm{sh}(b\tau_{n-1}^{-1})\,d^{-1}$. ∎

Corollary 1.8. *For all braids a, a', and every positive integer p, the following are equivalent:*

(i) The equality $a \wedge \tau_{p-1} = a' \wedge \tau_{p-1}$ holds;

(ii) The braid $a^{-1}a'$ belongs to B_p.

Proof. Assume that a, a' belong to B_n, where $n \geq p$ holds. By the previous result, (i) holds if and only if the braid $a^{-1}a'$ commutes with $\mathrm{sh}(\tau_{p-1}\tau_{n-1}^{-1})$, which is $\sigma_{p+1}^{-1} \ldots \sigma_n^{-1}$, hence if and only if it commutes with $\sigma_n \ldots \sigma_{p+1}$. By Lemma 1.6, this means that $a^{-1}a'$ belongs to B_p. ∎

We see in particular that the mapping $a \mapsto a \wedge 1$ is injective on B_∞, a property that extends a similar result in every monogenerated free LD-system.

1.3. Right powers

We consider now the iterated powers of braids with respect to exponentiation. In the sequel, we use $x^{[m]}$ and $x_{[m]}$ to denote the m-th *right* and *left* powers of x defined inductively by

$$x^{[1]} = x_{[1]} = x, \quad x^{[m+1]} = x \wedge x^{[m]}, \quad x_{[m+1]} = x_{[m]} \wedge x.$$

For instance, an easy induction gives the formula

$$1^{[m]} = \tau_{m-1} \quad (= \sigma_{m-1} \ldots \sigma_2 \sigma_1). \tag{1.6}$$

In the case of special braids, precise results about right powers are known.

Definition. For b a special braid, the *height* $\mathrm{ht}(b)$ of b is defined as follows: $\mathrm{ht}(1)$ is 1, and, for $b \neq 1$, $\mathrm{ht}(b)$ is the least value of $\sup(\mathrm{ht}(b_1), \mathrm{ht}(b_2)) + 1$ when (b_1, b_2) ranges over all pairs such that b is $b_1 {}^\wedge b_2$.

For instance, the height of σ_1 is 2, the height of $\sigma_2\sigma_1$ (which is $1^{[3]}$) and $\sigma_1^2\sigma_2^{-1}$ (which is $1_{[3]}$) is 3, *etc.* The height of a special braid is the height of a minimal binary tree that expresses b in terms of 1 and $^\wedge$. We shall also use in the sequel the *exponent sum* $\varepsilon(b)$ of a braid b, where ε is the augmentation homomorphism of B_∞ to $\mathbb{Z}$ that maps every generator σ_i to 1.

Lemma 1.9. *Assume that b is a special braid.*
(i) The equality $b{}^\wedge\tau_{m-1} = \tau_m$ holds for $m \geq \mathrm{ht}(b)$.
(ii) The equality $b^{[m-\varepsilon(b)]} = 1^{[m]} = \tau_{m-1}$ holds for $m \geq \mathrm{ht}(b)$. In particular, we have $b^{[\mathrm{ht}(b)-\varepsilon(b)]} = \tau_{\mathrm{ht}(b)-1}$.

Proof. (i) We prove inductively on $p \geq 1$ that the property holds for $\mathrm{ht}(b) \leq p$. If p is 1, b must be 1, and the result follows from (1.6). Otherwise, there must exist special braids b_1 and b_2 such that b is $b_1{}^\wedge b_2$, and $\mathrm{ht}(b_1)$ and $\mathrm{ht}(b_2)$ are at most $p-1$. Assume $m \geq p$. Using the induction hypothesis, we find

$$b{}^\wedge\tau_{m-1} = (b_1{}^\wedge b_2){}^\wedge\tau_{m-1} = (b_1{}^\wedge b_2){}^\wedge(b_1{}^\wedge\tau_{m-2}) = b_1{}^\wedge(b_2{}^\wedge\tau_{m-2}) = b_1{}^\wedge\tau_{m-1} = \tau_m.$$

(ii) The argument is similar for the second formula. If p is 1, b is 1, $\varepsilon(b)$ is 0, and the result is obvious. Otherwise, assume $b = b_1{}^\wedge b_2$ with $\mathrm{ht}(b_1) < p$ and $\mathrm{ht}(b_2) < p$. We observe that $b^{[k]}$ is equal to $b_1{}^\wedge b_2^{[k]}$ for every k, and that $\varepsilon(b)$ is $\varepsilon(b_2) + 1$. So, using the induction hypothesis, we find for $m \geq p$

$$\begin{aligned} b^{[m-\varepsilon(b)]} &= b_1{}^\wedge b_2^{[m-\varepsilon(b)]} = b_1{}^\wedge b_2^{[m-1-\varepsilon(b_2)]} \\ &= b_1{}^\wedge 1^{[m-1]} = b_1{}^\wedge b_1^{[m-1-\varepsilon(b_1)]} = b_1^{[m-\varepsilon(b_1)]} = 1^{[m]}, \end{aligned}$$

which completes the proof. ∎

So it is natural to ask whether the relations of Lemma 1.9 extend to arbitrary braids or, in the contrary, characterize special braids. As for the first relation, it extends to the whole of B_∞.

Proposition 1.10. *Assume that b belongs to B_∞. Then the following are equivalent:*
(i) The braid b belongs to B_n;
(ii) The equality $b{}^\wedge\tau_{n-1} = \tau_n$ holds.

Proof. The explicit value of $b{}^\wedge\tau_{n-1}$ is $b\,\tau_n\,\mathrm{sh}(b^{-1})$. If b belongs to B_n, *i.e.*, if b can be expressed as a product of generators $\sigma_i^{\pm 1}$ with $i < n$, then $b\tau_n$ is equal to $\tau_n\mathrm{sh}(b)$, and (ii) holds.

Conversely, assume that b does not belong to B_n. Let m the least integer such that b belongs to B_{m+1}. By the results of [10], we know that b admits an expression where exactly one of σ_m, σ_m^{-1} occurs. It follows that $\mathrm{sh}(b)$ has an expression where exactly one of σ_{m+1}, σ_{m+1}^{-1} occurs, and the same holds for $b\tau_{n-1}\mathrm{sh}(b)^{-1}\tau_n^{-1}$. Hence, by the results of [5], the latter braid cannot be the unit braid. ∎

Corollary 1.11. *Assume that c is a special braid. Then, for every braid b, the equality b^$c^{[m]} = c^{[m+1]}$ holds for m large enough.*

Proof. Proposition 1.10 tell us that, for every braid b, the equality b^$1^{[m]} = 1^{[m+1]}$ holds for m large enough. The corollary follows, since, by Lemma 1.9, there exists p such that $c^{[m]}$ is $1^{[m+p]}$ for m large enough. ■

The previous result does not extend to the case of an arbitrary braid c. For instance, if c is σ_1^{-1}, then $c^{[m]}$ is $\sigma_m...\sigma_2\sigma_1^{-1}$, and 1^$c^{[m]}$, which is $\sigma_{m+1}...\sigma_3\sigma_2^{-1}\sigma_1$, is never equal to $c^{[m+1]}$, which is $\sigma_{m+1}...\sigma_3\sigma_2\sigma_1^{-1}$.

Similarly, Lemma 1.9(ii) does not extend to arbitrary braids: as was mentioned above, $\sigma_1^{-1[m]}$ is $\sigma_m...\sigma_2\sigma_1^{-1}$, and, therefore, no right power of σ_1^{-1} may be a right power of 1. We shall come back on the question in Section 4 below.

We finish this section with two open questions. It follows from Lemma 1.9 and Proposition 1.10 that, if b is a special braid of height n, then b belongs to B_n.

Question 1.12. *Is the converse implication true, i.e., is the height of every special braid that belongs to B_n bounded above by n?*

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

Question 1.13. *Does $(B_\infty, ^\wedge)$ include a free LD-system on two generators, i.e., do there exist two braids b_1, b_2 such that the closure of $\{b_1, b_2\}$ under exponentiation is a free LD-system based on $\{b_1, b_2\}$?*

We conjecture a negative answer. Observe that Corollary 1.11 implies that a possible free sub-LD-system of rank 2 of B_∞ contains no special braid. Indeed, if c is special, and b_1, b_2 are arbitrary braids, then Corollary 1.11 implies $b_1{}^\wedge c^{[m]} = b_2{}^\wedge c^{[m]}$ for m large enough. But, by the results of [4], no equality of the form $b_1{}^\wedge x = b_2{}^\wedge x$ may hold in a free LD-system based on the set $\{b_1, b_2\}$.

2. Special Braids

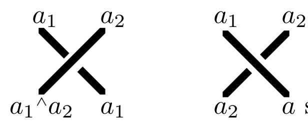
In this section, we give a combinatorial characterization of special braids by means of an action of braids on sequences of braids ("braid colorings"). This results in particular in an effective algorithm that recognizes whether a given braid word represents a special braid, and, if so, provides an explicit decomposition of this braid in terms of the unit braid and exponentiation.

2.1. The action of braids on LD-systems

Assume that $(\Sigma, {}^\wedge)$ is an LD-system where all left translations are bijections, *i.e.*, $(\Sigma, {}^\wedge)$ is an automorphic set in the sense of [2] or a rack in the sense of [20]—or, in a slightly different framework, a crystal in the sense of [22]. Then the formula

$$(a_1, \ldots, a_n)\sigma_i = (a_1, \ldots, a_{i-1}, a_i{}^\wedge a_{i+1}, a_i, a_{i+2}, \ldots, a_n) \tag{2.1}$$

defines an action of B_n on Σ^n. This action can be described in terms of colorings of the strands of a braid: for b a braid and $\vec{a}$ a sequence in Σ^n, the value of $(\vec{a})\, b$ is the sequence of output colors obtained when the input colors $\vec{a}$ are attributed to the top ends of the strands of b and the colors are propagated according to the rule



satisfying $a_2{}^\wedge a = a_1$.

However, the hypothesis that the translations of the LD-system $(\Sigma, {}^\wedge)$ are bijective can be relaxed into the hypothesis that these translations are injective, *i.e.*, the system $(\Sigma, {}^\wedge)$ is left cancellative, at the expense of considering a partial action [5]: $(\vec{a})\, b$ need no longer exist for every sequence $\vec{a}$ in Σ^n, but it remains true that, for every braid word w, there exists a sequence $\vec{a}$ such that $(\vec{a})w$ exists, and that, if w, w' are braid words representing the same braid b, and $\vec{a}$ is a sequence such that both $(\vec{a})w$ and $(\vec{a})w'$ exist, then the latter sequences are equal, and $(\vec{a})\, b$ can be unambiguously defined to be $(\vec{a})w$.

As B_∞ equipped with exponentiation is a left cancellative LD-system, it is eligible for the previous partial action. So (2.1) defines a partial action of B_n on B_∞^n for every n, hence a partial action of B_∞ on the set of all sequences from B_∞ indexed by positive integers. Observe that the restriction of the action to B_∞^+ is everywhere defined, for problems with division occur only at negative crossings. .

The following argument is easy, but it relies upon deep results about free LD-systems.

Lemma 2.1. *Assume that $\vec{a}$ is a sequence of special braids and $(\vec{a})\, b$ exists. Then the latter sequence consists of special braids.*

Proof. It suffices to show that each elementary step in the action introduces only special braids. Now, by definition, if a and b are special braids, so is $a{}^\wedge b$, and the case of positive crossings is trivial. On the other hand, assume that a and c are special braids, and b is a braid satisfying $a{}^\wedge b = c$. By the trivial part of Proposition 1.4, the equality $a{}^\wedge c = (a{}^\wedge a){}^\wedge c$ holds in B_∞, hence in B_∞^{sp}. Now, by the non-trivial part of Proposition 1.2, this implies that there exists b' in B_∞^{sp} that satisfies $a{}^\wedge b' = c$. Finally, by left cancellativity, b must be equal to b', *i.e.*, b must be a special braid. So the action of negative crossings introduces special braids only. ∎

We characterize special braids as follows:

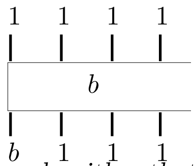
Proposition 2.2. *Let b be an arbitrary braid. Then the following are equivalent:*
(i) The braid b is special;
(ii) The sequence $(1, 1, 1, \dots)\, b$ exists, and it is equal to $(b, 1, 1, \dots)$.

Proof. First we prove that (i) implies (ii) using induction on the length of a braid word that represents b. It is clear that (ii) holds when b is 1. Assume that b is b_1^b_2, and b_1, b_2 satisfy (ii). Then we find

$$\begin{aligned}(1, 1, \dots)\, b &= ((((1, 1, \dots)\, b_1)\, \mathrm{sh}(b_2))\, \sigma_1)\, \mathrm{sh}(b_1^{-1})\\ &= (((b_1, 1, 1, \dots)\, \mathrm{sh}(b_2))\, \sigma_1)\, \mathrm{sh}(b_1^{-1})\\ &= ((b_1, b_2, 1, 1, \dots)\, \sigma_1)\, \mathrm{sh}(b_1^{-1})\\ &= (b, b_1, 1, 1, \dots)\, \mathrm{sh}(b_1^{-1})\\ &= (b, 1, 1, 1, \dots).\end{aligned}$$

Indeed, for the last step, the hypothesis on b_1 implies that $(b_1, 1, 1, \dots)\, b_1^{-1}$ is defined and equal to $(1, 1, \dots)$, and, similarly, $(b, b_1, 1, 1, \dots)\, \mathrm{sh}(b_1^{-1})$ is defined and equal to $(b, 1, 1, \dots)$. Conversely, assume that b satisfies (ii). The braid 1 is special, so Lemma 2.1 tells us that b is special. ■

Thus, a special braid is a braid that produces itself using braid coloring and starting from unit braids, according to the scheme



Proposition 2.3. *There exists an algorithm that recognizes whether a given braid word represents a special braid, and, if so, gives an expression of this braid in terms of the unit braid and exponentiation.*

Proof. Let w be an arbitrary braid word. We decide whether w represents a special braid as follows: first, we reverse w into an equivalent braid word uv^{-1} with u, v positive using the method of [7]; then, we compute $(1, 1, 1, \dots)\, uv^{-1}$. By [5], it is known that, if $(\vec{a})\, w'$ is defined for at least one braid word w' equivalent to w, then $(\vec{a})\, uv^{-1}$ must be defined. Then w represents a special braid if and only if the previous computation is successful and it ends with a sequence of the form $(b, 1, 1, \dots)$, *i.e.*, all components from the second are trivial. The latter point can be effectively tested using one of the many algorithms that solve the word problem of braids. Moreover, there exists an effective left division algorithm in free monogenerated LD-systems [6]. Hence, we can obtain an effective expression of the special braids involved in $(1, 1, 1, \dots)\, uv^{-1}$ in terms of 1 and exponentiation. ■

Example 2.4. Let w be the braid word $\sigma_2^{-1}\sigma_1^{-1}\sigma_2^2\sigma_1$. We first reverse w into the equivalent word $\sigma_1^2\sigma_2^{-1}$. Then we compute $(1, 1, 1)\, \sigma_1^2\sigma_2^{-1}$: thus u is here σ_1^2, and v is σ_2. The value of $(1, 1, 1)\, \sigma_1^2$ is ((1^1)^1, 1^1, 1). Then, in order to apply v, we have to divide 1^1 by 1 on the left. In the present case, the result is obvious: division is possible and the quotient is 1. So we see that $(1, 1, 1)\, \sigma_1^2\sigma_2^{-1}$ is ((1^1)^1, 1, 1), and, finally, we conclude that w represents the special braid (1^1)^1, *i.e.*, $1_{[3]}$.

2.2. Special decompositions

The previous results allow us to express every braid in terms of special braids, in an effective way.

Definition. Assume that b is a braid and $(b_1, b_2, \ldots)$ is a finite sequence of special braids—or an infinite sequence eventually equal to 1. We say that $(b_1, b_2, \ldots)$ is a *special decomposition* for b if the equality

$$b = b_1 \cdot \mathrm{sh}(b_2) \cdot \mathrm{sh}^2(b_3) \cdot \ldots \tag{2.2}$$

holds.

Proposition 2.5. *Let b be an arbitrary braid. Then the following are equivalent:*
(i) The braid b admits a special decomposition;
(ii) The sequence $(1, 1, 1, \ldots)\, b$ is defined.
In this case, the special decomposition of b is unique, and it is equal to $(1, 1, 1, \ldots)\, b$.

Proof. Assume that $(a_1, a_2, \ldots)$ is a sequence of braids eventually equal to 1, and that $(a_1, a_2, \ldots)\, b$ is equal to $(b_1, b_2, \ldots)$. Then, an easy induction on the length of b gives the equality

$$b_1\, \mathrm{sh}(b_2)\, \mathrm{sh}^2(b_3) \ldots \;=\; a_1\, \mathrm{sh}(a_2)\, \mathrm{sh}^2(a_3) \ldots\, b. \tag{2.3}$$

In particular, if $(1, 1, \ldots)\, b$ is equal to $(b_1, b_2, \ldots)$, we obtain $b = b_1\, \mathrm{sh}(b_2)\, \mathrm{sh}^2(b_3) \ldots$ As the braid 1 is special, we are sure that all braids b_i are special. So (ii) implies (i).

Conversely, assume $b = b_1\, \mathrm{sh}(b_2)\, \mathrm{sh}^2(b_3) \ldots$ with b_1, b_2, $\ldots$ special. Then we obtain successively

$$\begin{aligned}(1, 1, \ldots)\, b &= (1, 1, \ldots)\, b_1\, \mathrm{sh}(b_2)\, \mathrm{sh}^2(b_3) \ldots \\ &= (b_1, 1, 1, \ldots)\, \mathrm{sh}(b_2)\, \mathrm{sh}^2(b_3) \ldots \\ &= (b_1, b_2, 1, 1, \ldots)\, \mathrm{sh}^2(b_3) \ldots = \ldots = (b_1, b_2, b_3, \ldots).\end{aligned}$$

This proves that (i) implies (ii) and, in addition, that the special decomposition is unique when it exists. ∎

Corollary 2.6. *Every positive braid admits a unique special decomposition.*

Proof. If b belongs to B_∞^+, then, by construction, the sequence $(1, 1, \ldots)\, b$ is defined since possible obstructions occur only with negative crossings. ∎

Notice that the algorithm of Proposition 2.3 allows us to effectively obtain the possible special decomposition of a braid.

If we consider positive braids with a fixed number of strands, we can say a little more. Indeed, if b lies in B_n^+, the special decomposition of b contains n factors only, *i.e.*, we have $b = b_1 \mathrm{sh}(b_2) \ldots \mathrm{sh}^{n-1}(b_n)$ for some special braids b_1, …, b_n. However, it must be noticed that the braids b_i involved in the decomposition need not belong to B_n—and, actually, they do not in general: for instance the special decomposition of σ_1^2, which lies in B_2, is $(\sigma_1^2 \sigma_2^{-1})\, \mathrm{sh}(\sigma_1)$, and $\sigma_1^2 \sigma_2^{-1}$ does not belong to B_2.

Proposition 2.7. *The positive braids that are special are exactly the braids* $1^{[m]}$*, i.e., those braids of the form* $\sigma_{m-1}\ldots\sigma_2\sigma_1$.

Proof. We use induction on the length of (a positive expression of) b. The result is obviously true for the unit braid 1. Now assume that b is positive and $b\sigma_i$ is special. Since b is positive, $(1,1,\ldots)\,b$ exists. Let $(b_1,b_2,\ldots)$ be the latter sequence. If i is not equal to 1, the i-th component of $(1,1,\ldots)\,b\sigma_i$ is equal to $b_i{}^\wedge b_{i+1}$, which cannot be 1. Thus i must be 1. The hypothesis that $b\sigma_1$ is special then implies $b_1 = b_3 = b_4 = \ldots = 1$, *i.e.*, $(1,1,\ldots)\,b = (1,b_2,1,1,\ldots)$. Applying (2.2), we see that b is equal to $\mathrm{sh}(b_2)$. Now, by construction, b_2 is positive, and it is special, as $(1,1,\ldots)\,b_2$ is equal to $(b_2,1,1,\ldots)$. By induction hypothesis, b_2 is $1^{[m]}$ for some m, and, then, b is $1^{[m+1]}$. ■

It is then easy to characterize those braids for which the decomposition of (2.2) involves only positive braids.

Proposition 2.8. *Let b be an arbitrary braid. Then the following are equivalent:*
(i) The braid b admits a special decomposition consisting of positive braids;
(ii) The braid b is a positive simple braid, i.e., there exists an integer n such that b divides Garside's fundamental braid Δ_n.

Proof. Assume that $(1,1,1,\ldots)\,b$ is $(b_1,b_2,\ldots)$. By Proposition 2.5, the braids b_i are special. If we assume in addition that b_i is positive, then, by Proposition 2.7, there must exist an integer m_i such that b_i is $\sigma_{m_i-1}\ldots\sigma_1$. If this occurs for every i, we obtain

$$b = (\sigma_{m_1-1}\ldots\sigma_1)(\sigma_{m_2-1}\ldots\sigma_2)\ldots, \tag{2.4}$$

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

Conversely, if b is a positive simple braid, then it is well-known that it admits a decomposition of the form (2.4), where m_i is the initial position of the strand that finishes at position i in b. By uniqueness, we know that this decomposition coincides with the one associated with $(1,1,1,\ldots)\,b$. So (i) holds. ■

In particular, the special decomposition of Δ_n is

$$\Delta_n = (\sigma_{n-1}\ldots\sigma_1)\,\mathrm{sh}(\sigma_{n-2}\ldots\sigma_1)\;\ldots\;\mathrm{sh}^{n-2}(\sigma_1).$$

3. The Linear Ordering of Braids

One of the most important properties of free LD-systems is the existence of canonical linear orderings. In particular, there exists on every monogenerated free LD-system a unique linear ordering such that the inequality $a < a^\wedge b$ holds for all a, b. So, as special braids form a free monogenerated LD-system, there exists a unique linear ordering of special braids that satisfies the previous inequality. We consider now an extension of this ordering to arbitrary braids. The existence of special decompositions enables us to first define a linear ordering on positive braids: if b and b' are positive braids—or, more generally, two braids that admit special decompositions—we say that $b < b'$ holds if, letting $(b_1, b_2, \ldots)$ and $(b'_1, b'_2, \ldots)$ be their special decompositions, the sequence $(b_1, b_2, \ldots)$ precedes the sequence $(b'_1, b'_2, \ldots)$ with respect to the lexicographical extension of the ordering on special braids: $(b_1, b_2, \ldots) < (b'_1, b'_2, \ldots)$ holds if $b_1 < b'_1$ holds, or if $b_1 = b'_1$ and $b_2 < b'_2$ hold, *etc.* Finally, we extend the linear ordering to the whole of B_∞ by using the fact that every braid is the quotient of two positive braids: for b an arbitrary braid, we say that $b > 1$ if b is equal to $b_1^{-1} b_2$ where b_1 and b_2 are positive braids satisfying $b_1 < b_2$. One verifies [5] that this definition is non-ambiguous, and that the braid ordering extends the ordering of special braids.

Definition. The braid b is *σ_1-positive* (*resp.* *σ_1-negative*, *resp.* *σ_1-neutral*) if it admits at least one expression where σ_1 occurs, but σ_1^{-1} does not (*resp.* σ_1^{-1} occurs, but σ_1 does not, *resp.* neither σ_1 nor σ_1^{-1} occurs).

In particular, a braid is σ_1-neutral if and only if it belongs to the image of the shift endomorphism.

Proposition 3.1. [5], [10] *(i) Let b_1, b_2 be special braids. Then $b_1 < b_2$ holds if and only if the braid $b_1^{-1} b_2$ is σ_1-positive.*
(ii) Let b_1, b_2 be arbitrary braids. Then $b_1 < b_2$ holds if and only if there exists a nonnegative integer k and a σ_1-positive braid b such that $b_1^{-1} b_2$ is $\mathrm{sh}^k(b)$.

Observe in particular that (i) implies that the quotient of two special braids is never σ_1-neutral except if it is trivial, *i.e.*, if the considered special braids are equal. The existence of the linear ordering of braids implies, and, actually, is equivalent to the following trichotomy property:

Corollary 3.2. *Let b be an arbitrary braid. Then exactly one of the following cases occurs:*
(i) The braid b is σ_1-positive;
(ii) The braid b is σ_1-negative;
(iii) The braid b is σ_1-neutral.

An alternative approach to the linear ordering $<$ based on the connection of braids with homeomorphisms of a punctured disk has been developed recently in [18].

3.1. Compatibility with exponentiation

As we mentioned, the inequality $a < a\hat{}b$ holds for all special braids a, b. The extension to arbitrary braids is straightforward.

Proposition 3.3. *The inequality $a < a\hat{}b$ holds for all braids a, b.*

Proof. Obvious: $a^{-1}(a\hat{}b)$ is equal to $\mathrm{sh}(b)\sigma_1\mathrm{sh}(a^{-1})$, an explicitely σ_1-positive braid. ∎

On the other hand, a deep property of the linear ordering on monogenerated free LD-systems is that the inequality $b < a\hat{}b$ also holds [6] [25]. It follows that, if a, b are special braids, then $b < a\hat{}b$ holds. This leads us immediately to

Question 3.4. *Does the inequality $b < a\hat{}b$ hold for all braids a, b?*

It is easy to give a negative answer. For instance, we have $1 > \sigma_1^{-2}\hat{}1$, and $\sigma_2\sigma_1 > (\sigma_1\sigma_3^{-2})\hat{}(\sigma_2\sigma_1)$: in the latter case, the quotient $(\sigma_2\sigma_1)^{-1}(\sigma_1\sigma_3^{-2})\hat{}(\sigma_2\sigma_1)$ is equal to $\sigma_2\sigma_3^{-1}\sigma_2\sigma_1^{-1}\sigma_2^{-1}\sigma_3\sigma_2^{-1}\sigma_4^2$, hence is a σ_1-negative braid. The latter example shows that even the hypothesis that a is σ_1-positive is not sufficient to guarantee that the inequality holds for every b.

We establish positive (partial) answers to Question 3.4. According to the previous remarks, these results seem to be optimal.

Lemma 3.5. *Let b be an arbitrary braid. Then the braid $b^{-1}\,\mathrm{sh}(b)\,\sigma_1$ is σ_1-positive.*

Proof. Let us denote by $[x, y]$ the commutator of x and y, *i.e.*, $xyx^{-1}y^{-1}$. Let c be $b^{-1}\,\mathrm{sh}(b)\,\sigma_1$. We can write c as $c'c''$, where c' is $[b^{-1}, \sigma_2 \ldots \sigma_n]$ and c'' is $[\sigma_2 \ldots \sigma_n, b^{-1}]b^{-1}\,\mathrm{sh}(b)\,\sigma_1$. Now we have

$$c' = (b^{-1}\,\sigma_2 \ldots \sigma_n\, b)\,\sigma_n^{-1} \ldots \sigma_2^{-1}.$$

The first term is a conjugate of the positive braid $\sigma_2 \ldots \sigma_n$. Hence, by the results of [27] (or of [3], or of [31]), the inequality $b^{-1}\,\sigma_2 \ldots \sigma_n\, b > 1$ holds, and, therefore, the braid $b^{-1}\,\sigma_2 \ldots \sigma_n\, b$ is either σ_1-positive, or σ_1-neutral. As the braid $\sigma_n^{-1} \ldots \sigma_2^{-1}$ is σ_1-neutral, we conclude that c' is either σ_1-positive, or σ_1-neutral (we do *not* claim that $c' \geq 1$ holds).

On the other hand, we find

$$c'' = \sigma_2 \ldots \sigma_n\, b^{-1}\, \sigma_n^{-1} \ldots \sigma_2^{-1}\,\mathrm{sh}(b)\,\sigma_1.$$

Using the handle trick of Figure 2.1, we obtain

$$c'' = \sigma_1^{-1}\,\mathrm{sh}(b^{-1})\,\sigma_1\,\mathrm{sh}(b)\,\sigma_1.$$

Now, the latter expression shows that c'' is a conjugate of the positive braid σ_1, hence, always by [27], $c'' > 1$ holds. We deduce that c'' is either σ_1-positive, or σ_1-neutral, and so is $c'c''$, *i.e.*, c.

It remains to show that c cannot be σ_1-neutral, which is easy. Indeed, let f be the permutation of the integers associated with b. Then the origin of the strand that finishes at position 1 in c is $f^{-1}(f(1) + 1)$, hence it cannot be 1, as it is the case for every σ_1-neutral braid. ∎

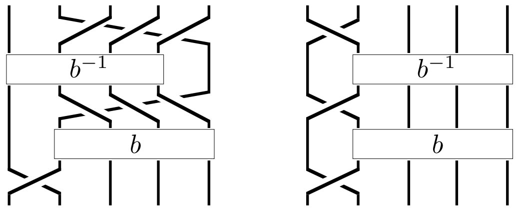


Figure 2.1: The handle trick again

Proposition 3.6. *Assume that the braid a can be expressed as $a'a''\mathrm{sh}(a'^{-1})$ where a'' is a positive braid. Then the inequality $b < a\hat{}b$ holds for every braid b.*

Proof. Let d be $a'^{-1}b$. Then we have

$$\begin{aligned} b^{-1}(a\hat{}b) &= d^{-1}\, a''\, \mathrm{sh}(d)\, \sigma_1\, \mathrm{sh}(a^{-1}) \\ &= (d^{-1}\, \mathrm{sh}(d)\, \sigma_1) \cdot (\sigma_1^{-1}\, \mathrm{sh}(d^{-1})\, a''\, \mathrm{sh}(d)\, \sigma_1) \cdot \mathrm{sh}(a^{-1}). \end{aligned}$$

By Lemma 3.5, the first braid in the latter decomposition is σ_1-positive. The second one is a conjugate of a positive braid, so $\sigma_1^{-1}\, \mathrm{sh}(d^{-1})\, a''\, \mathrm{sh}(d)\, \sigma_1 > 1$ holds, and, therefore, the braid $\sigma_1^{-1}\, \mathrm{sh}(d^{-1})\, a''\, \mathrm{sh}(d)\, \sigma_1$ is either σ_1-positive or σ_1-neutral. Finally, the last factor is σ_1-neutral. Hence the braid $b^{-1}(a\hat{}b)$ is σ_1-positive. ■

Corollary 3.7. *Assume that the braid a is positive or special. Then the inequality $b < a\hat{}b$ holds for every braid b.*

Proof. If a is positive, we apply the previous result with $a' = 1$. On the other hand, an immediate induction shows that, if a is special, it is either 1, and we apply Lemma 3.5, or it can be expressed as $a_1\hat{}\ldots\hat{}a_p\hat{}1$, where $a_1, \ldots, a_p$ are themselves special. Now, in this case, a is $a'\tau_p\mathrm{sh}(a'^{-1})$ with $a' = a_1\mathrm{sh}(a_2)\ldots\mathrm{sh}^{p-1}(a_p)$. ■

Observe that the previous result gives a new proof that the inequality $b < a\hat{}b$ holds in every monogenerated LD-system.

3.2. Laver's conjecture

Neither the linear ordering of B_∞ nor its restriction to B_∞^+ is a well-ordering, since the sequence $\sigma_1, \sigma_2, \ldots$ is strictly decreasing. On the other hand, Laver has proved in [27] that the restriction of the linear ordering to B_n^+ is a well-ordering, and Burckel has shown in [3] that the ordertype of this restriction is the ordinal $\omega^{\omega^{n-2}}$: for instance, the order-type of B_2^+ is ω, the ordertype of the natural numbers—which is obvious—while the order-type of B_3^+ is ω^ω.

Definition. For $(b_1, \ldots, b_n)$ a given sequence of braids, $D(b_1, \ldots, b_n)$ is the subset of B_n consisting of those braids b such that the sequence $(b_1, \ldots, b_n)\, b$ is defined.

For instance, $D(1, \ldots, 1)$ consists of all braids in B_n that admit a special decomposition—so it contains all positive braids in B_n.

Question 3.8. *Let $(b_1, \ldots, b_n)$ be a finite sequence of braids. Is the set $D(b_1, \ldots, b_n)$ well-ordered by the linear ordering of braids?*

The question is implicit at the end of [27], and Laver conjectures a positive answer. This question—together with some variants involving free LD-systems on more than one generator—seems to be one of the major open questions in the area. A positive solution would imply a number of consequences in the study of free LD-systems.

Restricting to finite sequences is necessary: the set $D(1, 1, \ldots)$ (infinite sequence) includes B_∞^+, which is not well-ordered. However, we could easily modify the construction of the linear ordering so that the sequence $\sigma_1, \sigma_2, \ldots$ becomes increasing. In this case we could obtain a well-ordering on B_∞^+ (with order type ω^{ω^ω}). But, even so, $D(1, 1, \ldots)$ would not be well-ordered, as it contains all special braids, and the latter are not well-ordered, as shows the infinite descending sequence

$$1_{[1]}{}^\wedge 1_{[2]} > 1_{[2]}{}^\wedge 1_{[2]} > 1_{[3]}{}^\wedge 1_{[2]} > \ldots$$

To mention a partial result connected with Laver's conjecture, let Λ_k denote the free LD-system on k generators $x_1, \ldots, x_k$. So, in particular, Λ_1 is isomorphic to $(B_\infty^{sp}, {}^\wedge)$. It is known that Λ_k is left cancellative, so it is eligible for braid colorings. In other words, Formula (2.1) defines for every n and k a partial action of B_n on Λ_k^n. Then we can consider for every sequence $(a_1, \ldots, a_n)$ in Λ_k^n the set $D(a_1, \ldots, a_n)$ consisting of those braids such that $(a_1, \ldots, a_n)\, b$ is defined. Larue has shown in [24] that the set $D(x_1, \ldots, x_k)$ coincides with B_n^+, and, therefore, Laver's conjecture is true in this particular case. Let us observe that using the free LD-system Λ_k is not really leaving the framework of braids. Indeed, in the same way as Λ_1 can be realized as a subsystem of B_∞ equipped with braid exponentiation, Λ_k can be realized as a subsystem of CB_∞ equipped with braid exponentiation, where CB_∞ is the extension of B_∞ obtained by adding a sequence of pairwise commuting new generators $\rho_1, \rho_2, \ldots$ submitted to the relations $\sigma_i \rho_j = \rho_j \sigma_i$ for $j < i$ and $j > i+1$, and $\sigma_i \rho_{i+1} \rho_i = \rho_i \rho_{i+1} \sigma_i$. The elements of CB_∞ can be interpreted as braids where the strands wear some integer charges [9].

3.3. Decompositions

The fact that the braid ordering is linear together with the characterization of Proposition 3.1 imply that every braid which does not belong to $\mathrm{sh}(B_\infty)$, *i.e.*, which is not σ_1-neutral, admits an expression where exactly one of σ_1, σ_1^{-1} occurs. Moreover, the results of [24], [10], and [18] give three different proofs of the more precise result that every braid in B_n admits in B_n a decomposition of the previous type.

Several questions arise about the possible numbers of letters σ_1 in a σ_1-positive expression of a given braid. Determining the minimal such number is connected with the following question.

Question 3.9. *Assume that the braid $\sigma_1 \mathrm{sh}(b) \sigma_1$ has a σ_1-positive decomposition with only one σ_1. Is the same true for b?*

The previous condition is obviously sufficient: if b is $\mathrm{sh}(b_0)\sigma_1\mathrm{sh}(b_1)$, then $\sigma_1\mathrm{sh}(b)\sigma_1$ is equal to $\mathrm{sh}^2(b_0)\sigma_2\sigma_1\sigma_2\mathrm{sh}^2(b_1)$. Whether the condition is necessary is open.

As shows the trivial equality $\sigma_2\sigma_1 = \sigma_1^k\sigma_2\sigma_1\sigma_2^{-k}$, there is no upper bound in general on the number of σ_1's in a σ_1-positive decomposition of a braid. However, it would be interesting to obtain upper bounds for the maximal number of σ_1's when the expression is to be chosen in some fixed set of braid words. In order to state a precise question, let $\sim$ denote the least congruence on braid words that contains all pairs $(\sigma_i\sigma_j\sigma_i, \sigma_j\sigma_i\sigma_j)$, $(\sigma_i^{-1}\sigma_j^{-1}\sigma_i^{-1}, \sigma_j^{-1}\sigma_i^{-1}\sigma_j^{-1})$, $(\sigma_i\sigma_j^{-1}, \sigma_j^{-1}\sigma_i^{-1}\sigma_j\sigma_i)$, $(\sigma_i^{-1}\sigma_j, \sigma_j\sigma_i\sigma_j^{-1}\sigma_i^{-1})$ for $|i-j| = 1$, and $(\sigma_i\sigma_j, \sigma_j\sigma_i)$, $(\sigma_i^{-1}\sigma_j^{-1}, \sigma_j^{-1}\sigma_i^{-1})$, $(\sigma_i\sigma_j^{-1}, \sigma_j^{-1}\sigma_i)$, $(\sigma_i^{-1}\sigma_j, \sigma_j\sigma_i^{-1})$ for $|i-j| \geq 2$. Thus, $\sim$ is included in the usual braid word equivalence, but we do not allow the equivalences $\sigma_i^{\pm 1}\sigma_i^{\mp 1} \equiv \varepsilon$ (where ε denotes the empty word) which may create *ex nihilo* new factors $\sigma_i^{\pm 1}\sigma_i^{\mp 1}$.

Question 3.10. *Is it true that, for every braid word w, there exists a constant c depending only on the number of strands in w such that the length of every freely reduced word that is $\sim$-equivalent to w is bounded by c times the length of w?*

A positive answer to the question would improve dramatically the complexity bounds of the algorithm described in [10]. The question is most presumably connected with the automatic structure of the braid groups [17] [11].

4. Equivalence Relations and Quotients

New questions arise when we consider equivalence relations. On the one hand, some quotients of the braid groups are known, and we can investigate the possible self-distributive operations induced by braid exponentiation on these quotients. We shall consider here the case of permutations and of Burau matrices.

On the other hand, as special braids make a free monogenerated LD-system, every monogenerated LD-system is a quotient of $(B_\infty^{sp}, {}^\wedge)$. In other words, for every monogenerated LD-system Σ, there must exist an equivalence relation $\equiv_\Sigma$ on B_∞^{sp} that is compatible with exponentiation and such that the quotient-structure $B_\infty^{sp}/{\equiv_\Sigma}$ is isomorphic to Σ. Looking for a geometric construction of the relation $\equiv_\Sigma$ and for a possible extension of this relation from special braids to arbitrary braids is a very natural task.

4.1. Exponentiation of permutations

We denote by π the surjective homomorphism of the group B_∞ onto the symmetric group S_∞ consisting of those permutations of the positive integers that eventually coincide with identity. For b a braid and p a positive integer, $\pi(b)(p)$ is the initial position of the strand that finishes at position p in b.

Proposition 4.1. *Braid exponentiation induces a well-defined left self-distributive operation on the symmetric group S_∞.*

The result is obvious, as braid exponentiation is defined by means of braid product and shift, and the projection π is a homomorphism with respect to these operations. Thus, for f, g in S_∞, the permutation $f^\wedge g$ is defined by

$$f^\wedge g = f \circ \mathrm{sh}(g) \circ s_1 \circ \mathrm{sh}(f^{-1}), \tag{4.1}$$

where $\mathrm{sh}(h)$ is defined by $\mathrm{sh}(h)(1) = 1$, $\mathrm{sh}(h)(p+1) = h(p) + 1$, and s_i denotes the transposition that exchanges i and $i+1$. Observe that (4.1) also defines a left self-distributive operation on the full symmetric group consisting of all permutations of the positive integers.

As in the case of braids, we have the natural notion of a *special permutation*, defined as one that can be generated from the identity mapping using exclusively exponentiation.

Question 4.2. *Give a combinatorial characterization of special permutations.*

The characterization of special braids given in Section 1 cannot be used. Actually, it is not clear that the technique of strand colorings can be used in the case of permutations. Indeed, if we try to let the symmetric group S_n act on sequences of colors, we must assume that the colors are equipped with a left self-distributive operation, but the compatibility with the relation $s_i^2 = \mathrm{id}$ requires that the color exponentiation satisfies the additional relations $a^\wedge b = b$, in which case coloring gives nothing more than the considered permutation.

Similarly, special decompositions of permutations exist, but they are trivial. Indeed, it is obvious that an arbitrary permutation f can be decomposed, in a unique way, as

$$f = \mathrm{id}^{[f(1)]} \circ \mathrm{sh}(\mathrm{id}^{[f(2)-1]}) \circ \mathrm{sh}^2(\mathrm{id}^{[f(3)-1]}) \circ \dots$$

Projecting Lemma 1.9 on S_∞ gives some necessary conditions that every special permutation has to satisfy. Projecting the first relation shows that, for every special permutation f, the equality

$$f^\wedge \mathrm{id}^{[m]} = \mathrm{id}^{[m+1]}$$

holds for $m \geq \mathrm{ht}(f)$, where $\mathrm{ht}(f)$ is defined to be 1 if f is the identity mapping, and to be the minimal value of $\sup(\mathrm{ht}(f_1), \mathrm{ht}(f_2)) + 1$ where (f_1, f_2) ranges on the pairs that satisfy $f = f_1{}^\wedge f_2$ otherwise. . However, as in the case of braids, this equality holds more generally for every permutation f such that $f(k) = k$ holds for $k > m$, and, actually, it characterizes such permutations.

The second relation in Lemma 1.9 is more interesting. We cannot project it directly, as the exponent sum of braids does not induce a well-defined mapping on permutations. However, we can use instead another integer parameter that behaves similarly.

Definition. For f in S_∞, the integer $\nu(f)$ is defined by

$$\nu(f) = \mathrm{card}\{p\ ;\ f(p+1) = p\}.$$

Lemma 4.3. *For f, g in S_∞, $\nu(f^\wedge g)$ is $\nu(g) + 1$.*

Proof. Denote by $S(f)$ the set $\{p\ ;\ f(p+1)=p\}$. We claim that the equality

$$S(f\hat{}g) = \{f(1)\} \cup f(S(g)) \tag{4.2}$$

holds. It clearly implies the desired relation $\nu(f\hat{}g) = \nu(g)+1$. The verification is an easy computation. For $p = f(1)$, we find $f\hat{}g(p+1) = p$, while, for $p \neq f(1)$, we find $f\hat{}g(p+1) = f(g(f^{-1}(p)+1))$. The latter is equal to p if and only if $g(f^{-1}(p)+1)$ is equal to $f^{-1}(p)$, *i.e.*, if and only if $f^{-1}(p)$ belongs to $S(g)$. ∎

Proposition 4.4. *Assume that f is a special permutation. Then the equality*

$$f^{[m-\nu(f)]} = \mathrm{id}^{[m]} = s_{m-1} \circ \ldots \circ s_2 \circ s_1$$

holds for $m \geq \mathrm{ht}(f)$.

Proof. Use the same inductive argument as for Lemma 1.9(ii). ∎

The previous condition can be used to prove that a given permutation is not special. Let us for instance consider the permutation $f = s_1 s_2 s_1$. An easy induction gives $f^{[m]} = s_1 \circ \mathrm{id}^{[m+1]}$. As $\nu(f)$ is 0, this is enough to conclude that f is not special. However the necessary condition of Proposition 4.4 is not sufficient: the permutation $f = s_1 \circ s_2$ satisfies $\nu(f) = 0$ and $f^{[3]} = \mathrm{id}^{[3]}$, but it follows from Proposition 4.9 below that it is not special.

The LD-system $(S_\infty^{sp}, \hat{}\,)$ consisting of all special permutations is not free: for instance, one can check in S_∞ the equality

$$\mathrm{id}_{[3]}\hat{}\mathrm{id}^{[2]} = \mathrm{id}^{[3]}\hat{}\mathrm{id}^{[2]} = s_1 \circ s_3,$$

while, in B_∞, we have

$$1_{[3]}\hat{}1^{[2]} = \sigma_1^3\sigma_3\sigma_2^{-2} \neq 1^{[3]}\hat{}1^{[2]} = \sigma_2^2\sigma_1\sigma_3^{-1}.$$

Question 4.5. *Give a presentation of the free LD-system $(S_\infty^{sp}, \hat{}\,)$, i.e., describe all relations that connect special permutations.*

4.2. Linear representations

Braid groups admit several linear representations. Here we consider briefly the case of the classical Burau representation. We write $\mathrm{GL}_\infty(\mathbb{Z}[t,t^{-1}])$ for the direct limit of the linear groups $\mathrm{GL}_n(\mathbb{Z}[t,t^{-1}])$ with respect to the embeddings

$$i_{n,n+1} : M \longmapsto \begin{pmatrix} & & & 0 \\ & M & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then the (unreduced) Burau representation ρ of B_∞ in $\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}])$ is defined by the conditions $\rho(\sigma_1) = \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix}$ and $\rho(\mathrm{sh}(b)) = \mathrm{sh}(\rho(b))$, where sh also denotes the shift endomorphism of $\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}])$

$$M \longmapsto \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M & \\ 0 & & & \end{pmatrix}.$$

As in the case of permutations, braid exponentiation induces a well-defined exponentiation on the image of ρ. The latter is a proper subgroup of $\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}])$, but it is obvious to verify that the formula

$$A\hat{\ }B = A\,\mathrm{sh}(B)\,\rho(\sigma_1)\,\mathrm{sh}(A^{-1})$$

specifies a well-defined left self-distributive operation on the whole of $\mathrm{GL}_\infty(\mathbb{Z}[t, t^{-1}])$. It is well-known [29], [28] that the Burau representation is not faithful.

Question 4.6. *Is the Burau representation faithful on special braids?*

The only partial result about this question is the remark that, if for b a braid $\rho_1(b)$ denotes the first column of the matrix $\rho(b)$, then the mapping ρ_1 cannot be injective on special braids. Indeed, the existence of the special decomposition of every positive braid as a product of shifted special braids given by Corollary 2.6 implies that, if ρ_1 were injective on B_∞^{sp}, then ρ would be injective on B_∞^+, hence on the whole of B_∞, and this is false. The previous argument leaves open the question of effectively constructing two special braids b_1, b_2 such that the first columns of the Burau images of b_1 and b_2 coincide. This can be done by starting with explicit positive braids whose Burau matrices have the same first column and using braid colorings to obtain special decompositions. In this way, it can be shown that the first columns (and, therefore, the first rows) of the Burau matrices of the special braids

$$\begin{aligned}&(((1^{[5]}\hat{\ }1^{[3]})\hat{\ }(1^{[5]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }((1^{[5]}\hat{\ }1^{[3]})\hat{\ }(1^{[5]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }1^{[5]}\hat{\ }1^{[3]})\hat{\ }(1^{[5]}\hat{\ }1^{[3]})\hat{\ }\\ &\quad(((1^{[5]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }((1^{[5]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }(((1^{[3]}\hat{\ }1)\hat{\ }1^{[3]})\hat{\ }1^{[3]}\hat{\ }1)\hat{\ }(1^{[3]}\hat{\ }1)\hat{\ }1^{[3]})\hat{\ }(1^{[5]}\hat{\ }1^{[3]})\hat{\ }1\end{aligned}$$

and

$$\begin{aligned}&(((1^{[4]}\hat{\ }1^{[3]})\hat{\ }(1^{[4]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }((1^{[4]}\hat{\ }1^{[3]})\hat{\ }(1^{[4]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }1^{[4]}\hat{\ }1^{[3]})\hat{\ }(1^{[4]}\hat{\ }1^{[3]})\hat{\ }\\ &\quad(((1^{[4]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }((1^{[4]}\hat{\ }1^{[3]})\hat{\ }1)\hat{\ }(((1^{[2]}\hat{\ }1)\hat{\ }1^{[2]})\hat{\ }1^{[2]}\hat{\ }1)\hat{\ }(1^{[2]}\hat{\ }1)\hat{\ }1^{[2]})\hat{\ }(1^{[4]}\hat{\ }1^{[3]})\hat{\ }1\end{aligned}$$

coincide—here $a\hat{\ }b\hat{\ }c$ stands for $a\hat{\ }(b\hat{\ }c)$. However, the rest of the matrices do not coincide.

4.3. Monogenerated LD-systems

Instead of considering the already known quotients of the braid groups, we can also start from free LD-systems. By definition of a free system, every monogenerated LD-system is a quotient of $(B_\infty^{sp}, {}^\wedge)$. Thus we can consider a given monogenerated LD-system Σ, and look for a geometrical definition of the congruence on B_∞^{sp} that yields Σ as the associated quotient, or, equivalently, for a geometrical definition of a homomorphism of $(B_\infty, {}^\wedge)$ onto Σ.

We begin with an easy example. A rather trivial monogenerated LD-system consists of $\mathbf{N}$ equipped with the exponentiation

$$x^\wedge y = y + 1. \tag{4.3}$$

The corresponding question is to construct on B_∞^{sp}, and, possibly, on B_∞, a mapping say φ such that $\varphi(b_1{}^\wedge b_2)$ is $\varphi(b_2) + 1$. The question is easy: we have already found two such mappings, namely the augmentation mapping ε, and the mapping $b \mapsto \nu(\pi(b))$. These mappings take equal values on special braids, but not on arbitrary braids, which reflects the fact that $(B_\infty, {}^\wedge)$ is not a free monogenerated LD-system.

Much deeper questions appear when we consider finite monogenerated LD-systems, and, in particular, the so-called systems A_n.

Proposition 4.7. (Laver [26], Drápal [15]) *For every positive integer n, there exists a unique LD-system A_n whose domain is the set $\{1, 2, \ldots, 2^n\}$ and that satisfies $p^\wedge 1 = p + 1$ for $p < 2^n$ and $2^n{}^\wedge 1 = 1$.*

The LD-systems A_n play a fundamental role in self-distributive algebra. In [27], Laver constructs them as natural quotients of a certain LD-system that arises in set theory from an unprovable large cardinal hypothesis, and he shows under that hypothesis that the projective limit of the A_n's includes a free LD-system—a result of which no proof in usual logic is known to date, *cf.* [14]. In [16], Drápal shows that every finite monogenerated LD-system can be constructed from the A_n's using simple operations. As the LD-system $(B_\infty^{sp}, {}^\wedge)$ is free, there must exist for every n a congruence relation $\equiv_n$ on special braids such that the quotient of B_∞^{sp} under $\equiv_n$ is A_n.

Question 4.8. *Does a geometrical description of $\equiv_n$ exist? Does $\equiv_n$ extend to the whole of B_∞ in some way?*

These questions are probably very difficult. In the LD-system A_n, the left power $1_{[2^n+1]}$ is equal to 1—actually A_n is the LD-system with presentation $\langle x \; ; \; x_{[2^n+1]} = x \rangle$. Hence, in B_∞, we must have $1_{[m]} \not\equiv_n 1$ for $m \leq 2^n$ and $1_{[2^n+1]} \equiv_n 1$. As the left powers $1_{[m]}$ in B_∞ are complicated objects, the congruence $\equiv_n$ is likely to be complicated as well. The only result we have now deals with the case $n = 1$.

Proposition 4.9. *If f is a special permutation, then $f^{-1}(1)$ is 1 or 2. The relation $f^{-1}(1) = f'^{-1}(1)$ is a congruence on $(S_\infty^{sp}, {}^\wedge)$, and the associated quotient is A_1.*

Proof. Developing the definition shows that $(f^\wedge g)^{-1}(1)$ is 2 when $f^{-1}(1)$ is 1, or when $f^{-1}(1)$ is 2 and $g^{-1}(1)$ is 2, and that $(f^\wedge g)^{-1}(1)$ is 1 when $f^{-1}(1)$ is 2 and $g^{-1}(1)$ is 1. ■

Corollary 4.10. *If b is a special braid, then $\pi(b)^{-1}(1)$ is 1 or 2. The relation $\pi(b)^{-1}(1) = \pi(b')^{-1}(1)$ is a congruence on $(B_\infty^{sp}, {}^\wedge)$, and the associated quotient is A_1.*

The argument of Proposition 4.9 extends to the sub-LD-system of $(S_\infty, {}^\wedge)$ consisting of those permutations f such that $f^{-1}(1)$ is either 1 or 2. But it does not extend to the whole of the symmetric group S_∞ as, in general, the value of $(f^\wedge g)^{-1}(1)$ does not depend only on the values of $f^{-1}(1)$ and $g^{-1}(1)$. Similarly, it is easy to see that looking for a possible quotient A_2 by considering the values of $f^{-1}(1)$ and $f^{-1}(2)$ does not work. Actually, nothing is known about the following problem:

Question 4.11. *Assume $n \geq 2$. Is the finite LD-systems A_n a quotient of $(S_\infty^{sp}, {}^\wedge)$?*

To finish this paragraph with another seemingly difficult problem, let us briefly mention the index function on free LD-systems. In [6], a normal form is defined on the free LD-system on one generator: each element of Λ_1 is represented by a unique term involving variables from an infinite sequence $x_1, x_2, \ldots$. Define the *index* of a as the index of the last variable occurring in the normal form of a. For instance, the index of $1^{[m]}$ is m, while the index of $1_{[m]}$ is 1 for $m \geq 3$. As special braids make a copy of Λ_1, the index of a special braid is well-defined.

Question 4.12. *Does the index of a special braid admit a geometrical definition—and possibly extend to arbitrary braids?*

We conjecture that there exists a connection between the index of a braid and its colorings using colors from a free LD-system on infinitely many generators. Similar questions can be raised for the alternative normal forms considered in [25] or [27].

5. Extended Braids

Further questions about (ordinary) braids arise when we consider the monoid EB_∞ of extended braids. The latter is introduced in [12] as a (partial) completion of the braid group B_∞ with respect to the topology associated with the linear ordering. The point here is that EB_∞ itself is equipped with two left self-distributive operations, one that extends braid exponentiation and one quite new, which makes it natural to consider for these operations the counterpart of those questions we discussed above in the case of B_∞.

Several constructions of EB_∞ are possible. Here, we define it as a disjoint sum

$$EB_\infty = \coprod_{p\geq 0} B_\infty / B_p,$$

so that the elements of EB_∞ are equivalence classes of pairs (b, q), b in B_∞, q a non negative integer, with respect to the relation $\equiv$ such that $(b, q) \equiv (b', q')$ holds if and only if q and q' are equal and $b^{-1}b'$ belongs to B_q. We shall denote by $[b, q]$ the equivalence class of (b, q). Here B_0 and B_1 are trivial groups, so, in particular, the mappings $a \mapsto [a, 0]$ and $a \mapsto [a, 1]$ define two injections of B_∞ into EB_∞.

It is shown in [12] that the extended braid $[b, q]$ is the limit of the increasing Cauchy sequence $(b\tau_{q,n}\ ;\ n \geq 0)$, where $\tau_{q,n}$ denotes the braid $\tau_q\,\mathrm{sh}(\tau_q)\ldots\mathrm{sh}^{n-1}(\tau_q)$, and that $[b, q]$ can be thought of as the braid b followed by an infinite series of positive crossings letting the leftmost q strands vanish at the right end of the diagram.

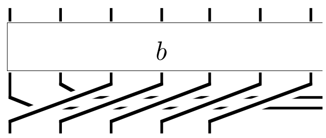


Figure 5.1. The extended braid $[b, q]$

The set EB_∞ is equipped with the associative product

$$[a, p] \cdot [b, q] = [a\ \mathrm{sh}^p(b), p + q],$$

and with two left self-distributive operations

$$[a, p]^\wedge[b, q] = [a\ \mathrm{sh}^p(b)\ \tau_{p,q}\ \mathrm{sh}^q(a)^{-1}, q],$$
$$[a, p] * [b, q] = [a\ \tau_p\ \mathrm{sh}(a^{-1}\ b), q + 1],$$

The first self-distributive operation is a rather direct extension of braid exponentiation—observe that the mapping $b \mapsto [b, 1]$ defines an embedding of $(B_\infty, {}^\wedge)$ into $(EB_\infty, {}^\wedge)$. In the sequel, we shall consider the second one exclusively.

As for ordinary braids, our starting point is a result stating that EB_∞ includes copies of the free monogenerated LD-system.

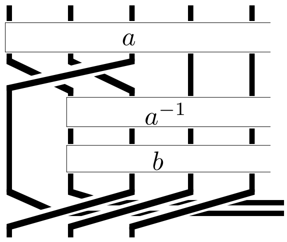


Figure 5.2. The extended braid $[a, 2] * [b, 1]$

Proposition 5.1. [12] *Every extended braid generates under operation $*$ a free LD-system.*

In particular, those extended braids that can be obtained from the unit $[1, 0]$ using exclusively $*$ form a free LD-system. They will be called naturally *special* extended braids.

5.1. Powers

Lemma 5.2. *Let $[b, q]$ be an extended braid. Then the equalities*

$$[b, q]^{[m]} = [b, q + m - 1], \quad [b, q]_{[m]} = [b\,\mathrm{sh}^q(1_{[m-1]}), q + 1]$$

hold for every positive m.

Proof. Use induction on $m \geq 1$. Everything is obvious for $m = 1$, so assume $m \geq 2$. For the right power, we find

$$[b, q]^{[m]} = [b, q] * [b, q]^{[m-1]} = [b, q] * [b, q + m - 2] = [b\tau_q, q + m - 1].$$

Now τ_q belongs to B_{q+1}, so the class $[b\tau_q, q + m - 1]$ is also $[b, q + m - 1]$.

For the left power, the result holds for $m = 2$ by the previous computation. Assume $m \geq 3$. By using the induction hypothesis, the equality

$$\mathrm{sh}^q(c)\,\tau_{q+1}\,\mathrm{sh}^{q+1}(c^{-1}) = \mathrm{sh}^q(c\sigma_1\mathrm{sh}(c^{-1}))\,\tau_q,$$

and the fact that τ_q belongs to B_{q+1}, we find

$$\begin{aligned}[b, q]_{[m]} &= [b, q]_{[m-1]} * [b, q]\\ &= [b\,\mathrm{sh}^q(1_{[m-2]})\,\tau_{q+1}\,\mathrm{sh}^{q+1}(1_{[m-2]}^{-1}), q + 1]\\ &= [b\,\mathrm{sh}^q(1_{[m-2]}\,\sigma_1\,\mathrm{sh}(1_{[m-2]})^{-1}))\,\tau_q, q + 1] = [b\,\mathrm{sh}^q(1_{[m-1]}), q + 1],\end{aligned}$$

as was claimed. ∎

Proposition 5.3. *For every extended braid $[b, q]$ with b in B_n, the equality*

$$[b, q]^{[m-q]} = [1, 0]^{[m]} \tag{5.1}$$

holds for $m > n$.

Proof. By the previous lemma, $[b,q]^{[m-q]}$ is equal to $[b, m-1]$. For $m > n$, b belongs to B_{m-1}, hence $[b, m-1]$ is also $[1, m-1]$, which is $[1,0]^{[m]}$. ■

Corollary 5.4. *The LD-system* $(EB_\infty, *)$ *includes no free LD-system on two generators.*

Proof. Assume that $[b_1, q_1]$ and $[b_2, q_2]$ are two extended braids. Then, by Proposition 5.3, there exist two integers m_1 and m_2 such that the right powers $[b_1, q_1]^{[m_1]}$ and $[b_2, q_2]^{[m_2]}$ are equal. Now, it is easily verified that, if Λ_2 is a free LD-system based on $\{x_1, x_2\}$, no power of x_1 may be equal to a power of x_2. ■

Another consequence of Lemma 5.2 is that square roots are easily determined in $(EB_\infty, *)$.

Proposition 5.5. *Let* $[b,q]$ *be an extended braid. Then those extended braid* $[a,p]$ *that satisfy* $[a,p]^{[2]} = [b,q]$ *are exactly those of the form* $[bc, q-1]$ *with* c *in* B_q.

5.2. Embedding of EB_∞ into B_∞

By uniqueness of the free monogenerated LD-system, there exists an isomorphism of the subsystem of $(EB_\infty, *)$ generated by $[1,0]$ onto the subsystem of $(B_\infty, {}^\wedge)$ generated by 1, *i.e.*, onto the system of special braids. We prove now that this isomorphism extends into an embedding of the whole of $(EB_\infty, *)$ into $(B_\infty, {}^\wedge)$.

Definition. For $p \geq 0$ and a a braid in B_∞, $I_p(a)$ is the braid $a\,\tau_p\,\mathrm{sh}(a^{-1})$.

Lemma 5.6. *Assume* $p, p' \geq 0$ *and* $a, a' \in B_\infty$. *Then the following are equivalent:*
(i) The braids $I_p(a)$ *and* $I_{p'}(a')$ *are equal;*
(ii) The integers p *and* p' *are equal and* $a^{-1}a'$ *belongs to* B_p.

Proof. As the exponent sum of $I_p(a)$ is p, $I_p(a)$ and $I_{p'}(a')$ may be equal only if p and p' are equal. Then, letting c be $a^{-1}a'$, $I_p(a) = I_{p'}(a')$ is equivalent to $\mathrm{sh}(c) = \tau_p^{-1}\, c\tau_p$, hence, by Lemma 1.5, to c belonging to B_p. ■

Definition. For α an extended braid, say $\alpha = [a,p]$, we let $I(\alpha)$ be the braid $I_p(a)$.

Proposition 5.7. *(i) The mapping* I *is an embedding of* $(EB_\infty, *)$ *into* $(B_\infty, {}^\wedge)$.
(ii) Assume that b *belongs to* B_n *and* $\varepsilon(b)$ *is* p. *Then* b *belongs to the image of* I *if and only if it belongs to the image of* I_p, *if and only if the braids* $b\tau_n^{-1}$ *and* $\sigma_{p+1}^{-1} \ldots \sigma_n^{-1}$ *are* B_n*-conjugate.*

Proof. (i) First, Lemma 5.6 guarantees that I is a well-defined mapping, and that it is injective. Then, assume $[c,r] = [a,p] * [b,q]$. We find

$$\begin{aligned} I([a,p])^\wedge I([b,q]) &= a\,\tau_p\,\mathrm{sh}(a^{-1})\,\mathrm{sh}(b)\,\mathrm{sh}(\tau_q)\,\mathrm{sh}^2(b^{-1})\,\sigma_1\,\mathrm{sh}^2(a)\,\mathrm{sh}(\tau_p^{-1})\,\mathrm{sh}(a^{-1}) \\ &= a\,\tau_p\,\mathrm{sh}(a^{-1}b)\,\tau_{q+1}\,\mathrm{sh}^2(b^{-1}a)\,\mathrm{sh}(\tau_p^{-1})\,\mathrm{sh}(a^{-1}) \\ &= c\,\tau_r\,\mathrm{sh}(c^{-1}) = I([c,r]), \end{aligned}$$

which shows that I is a homomorphism.

(ii) By construction, $I_p(a)$ is equal to $a^\wedge\tau_{p-1}$. We then apply Proposition 1.6. ■

Observe that every special braid except 1 belongs to the image of I. Indeed, such a special braid can always be expressed as $b_1{}^\wedge\ldots{}^\wedge b_p{}^\wedge 1$ for some special braids $b_1, \ldots, b_p$. The explicit value of the latter braid is $I_p(b)$, where b is $b_1\mathrm{sh}(b_2)\ldots\mathrm{sh}^{p-1}(b_p))$, *i.e.*, b is a braid that admits a special decomposition of length p.

We extend now to the whole image of I two properties that we know hold for special braids.

Proposition 5.8. *Assume that b belongs to the image of I. Then the exponent sum $\varepsilon(b)$ and the integer $\nu(\pi(b))$ are equal.*

Proof. Assume that b is $I_p(a)$. Then $\varepsilon(b)$ is p. Let f be the permutation $\pi(a)$. Then $\pi(b)$ is $f \circ s_{p-1} \circ \ldots \circ s_1 \circ \mathrm{sh}(f^{-1})$. Let k be a positive integer. Then $\pi(b)(k+1)$ is $f(s_{p-1}(\ldots(s_1(f^{-1}(k)+1))\ldots))$. If $f^{-1}(k)$ belongs to $\{1,\ldots,p\}$, $s_{p-1}(\ldots(s_1(f^{-1}(k)+1))\ldots)$ is $f^{-1}(k)$, and $\pi(b)(k+1)$ is k. Otherwise, $s_{p-1}(\ldots(s_1(f^{-1}(k)+1))\ldots)$ is $f^{-1}(k)+1$, and $\pi(b)(k+1)$ cannot be k. So there exist exactly p numbers satisfying $\pi(b)(k+1) = k$. ∎

Proposition 5.9. *Assume that b is a braid in B_n that belongs to the image of I_p. Then $b^{[n-p]}$ is equal to $1^{[n]}$, i.e., to τ_{n-1}.*

Proof. Assume that b is $I_p(a)$, *i.e.*, $b = a\,\tau_p\,\mathrm{sh}(a^{-1})$. As we assume that b belongs to B_n, the permutation $\pi(b)$ moves at most n integers, and, therefore, $\nu(\pi(b))$, which is p by the previous result, is at most $n-1$. We claim now that a must belong to B_{n-1}. Indeed, assume that the least index m such that a belongs to B_m is at least n. Then a has an expression where exactly one of σ_m, σ_m^{-1} occurs, and $\mathrm{sh}(a^{-1})$ has an expression where exactly one of σ_{m+1}, σ_{m+1}^{-1} occurs. As $\sigma_{m+1}^{\pm 1}$ does not occur in τ_p, we conclude that $a\tau_p\mathrm{sh}(a^{-1})$ does not belong to B_m, contradicting the hypothesis that b belongs to B_n. Now Proposition 5.3 tells us that $[a,p]^{[n-p]}$ is equal to $[1,0]^{[n]}$ in $(EB_\infty, *)$. Applying the homomorphism I, we deduce that $b^{[n-p]}$ is equal to $1^{[n]}$ in $(B_\infty, {}^\wedge)$. ∎

Instead of using EB_∞ and Proposition 5.3 in the previous proof, we could also resort to the formula

$$(a\,\tau_p\,\mathrm{sh}(a^{-1}))^{[m]} = a\,\tau_{p+m}\,\mathrm{sh}(a^{-1}).$$

Question 5.10. *Are the necessary conditions of Propositions 5.8 and 5.9 sufficient for a braid b to lie in the image of I?*

A very weak partial result is as follows.

Proposition 5.11. *For a positive braid b, the necessary condition of Proposition 5.8 is sufficient for b to lie in the image of I.*

Proof. For b a positive braid b, the value of $\nu(\pi(b))$ is equal to its exponent sum if and only if b admits an expression of the form $\sigma_{i_1}\ldots\sigma_{i_p}$ with $i_1 > \ldots > i_p$. Now, the formula

$$I(\tau_{1,i_1-1}^{-1}\ldots\tau_{1,i_p-1}^{-1}, p) = \sigma_{i_p}\ldots\sigma_{i_1}$$

can be checked directly in this case. ∎

5.3. Special extended braids

The action of braids on sequences of elements from a left cancellative LD-system $(\Sigma, \wedge)$ can be generalized to extended braids. In order to define the action of $[b, q]$ on a sequence $\vec{a}$, we refer to the interpretation of $[b, q]$ given in Figure 4.1. For the braid part, we use the standard rule, and it only remains to specify the rule for the final pattern where the q first strands vanish at the right end. Owing to the fact that $[1, q]$ is the limit of the braids $\tau_{q,n}$ when n goes to infinity, we define

$$(a_1, a_2, \ldots)[1, q] = (a'_{q+1}, a'_{q+2}, \ldots),$$

where a'_i is $a_1{}^\wedge\ldots{}^\wedge a_q{}^\wedge a_i$ for $i > q$—we recall that $a^\wedge b^\wedge c$ stands for $a^\wedge(b^\wedge c)$. The hypothesis that the operation $^\wedge$ is left self-distributive guarantees that the definition is sound: replacing $[1, q]$ with $[b, q]$ for some b in B_q may change the values of $a_1, \ldots, a_q$, but not the value of the expressions $a_1{}^\wedge\ldots{}^\wedge a_q{}^\wedge a_i$.

Lemma 5.12. *Assume that $\vec{a}$ is a sequence of braids eventually equal to 1. Then, when it is defined, the value of $(\vec{a})\,\beta$ determines the extended braid β.*

Proof. Assume that $(\vec{a})\,[b, q]$ and $(\vec{a})\,[b', q']$ coincide. By construction, $(\vec{a})\,b$ exists and is some sequence $(b_1, b_2, \ldots)$, and $(\vec{a})\,b'$ is some sequence $(b'_1, b'_2, \ldots)$. Then, by definition, the i-th component of $(\vec{a})\,[b, q]$ is $b_1{}^\wedge\ldots{}^\wedge b_q{}^\wedge b_{i+q}$. Now, for n large enough, b and b' belong to B_{n-1} and the n-th term a_n of $\vec{a}$ is 1. Hence both b_n and b'_n are 1. So the hypothesis $(\vec{a})\,[b, q] = (\vec{a})\,[b', q']$ together with the previous computation implie

$$b_1{}^\wedge\ldots{}^\wedge b_q{}^\wedge 1 = b'_1{}^\wedge\ldots{}^\wedge b'_{q'}{}^\wedge 1. \tag{5.2}$$

The equality of the exponent sums implies $q = q'$. Then, by left self-distributivity, (5.2) inductively implies $b_1{}^\wedge\ldots{}^\wedge b_q{}^\wedge a = b'_1{}^\wedge\ldots{}^\wedge b'_q{}^\wedge a$ for every special braid a. By left cancellation in $(B_\infty, {}^\wedge)$, we deduce in turn that b_{i+q} and b'_{i+q} are equal for every positive i. Finally, (5.2) means that the braids $I(b_1\mathrm{sh}(b_2)\ldots\mathrm{sh}^{q-1}(b_q), q)$ and $I(b'_1\mathrm{sh}(b'_2)\ldots\mathrm{sh}^{q-1}(b'_q), q)$ are equal. By Lemma 5.6, this implies that there exists a braid c in B_q such that $b'_1\mathrm{sh}(b'_2)\ldots\mathrm{sh}^{q-1}(b'_q)$ is equal to $b_1\mathrm{sh}(b_2)\ldots\mathrm{sh}^{q-1}(b_q)\,c$. Now c commutes with every element in $\mathrm{sh}^q(B_\infty)$, so, using Formula (2.3), we conclude that b' is bc. Hence the pairs (b, q) and (b', q') represent the same extended braid. ■

We recall that the mapping I of the previous subsection induces an isomorphism of special extended braids onto special braids which maps $[1, 0]$ to 1. On the shape of Proposition 2.2, we have the following intrinsic characterization of special extended braids in terms of colorings by braids.

Proposition 5.13. *Let β be an arbitrary extended braid. Then the following are equivalent:*

(i) The extended braid β is special;

(ii) The sequence $(1, 1, 1, \ldots)\,\beta$ exists and it has the form $(b, b, b, \ldots)$ for some braid b.

If the above conditions hold, the braid b of (ii) is equal to $I(\beta)$.

Proof. It is clear that (ii) holds when β is $[1,0]$. So, for proving that (i) implies (ii), it suffices to show that (ii) holds for β when β is $\beta_1 * \beta_2$ and β_1, β_2 satisfy (ii). Assume that β_i is the class of (b_i, q_i). By hypothesis, the sequence $(1,1,\ldots)\,\beta_1$ exists and it is equal to $(I(\beta_1), I(\beta_1), \ldots)$. Hence $(1,1,\ldots)\,b_1$ must exist as well, and it has the form $(a_1, \ldots, a_q, a, a, \ldots)$, where the braid a is satisfies $a_1{}^\wedge \ldots {}^\wedge a_q{}^\wedge a = I(\beta_1)$. Hence, we have

$$(1,1,\ldots)\,b_1\,\tau_{q_1} = (I(\beta_1), a_1, \ldots, a_q, a, a, \ldots),$$

and, therefore,

$$\begin{aligned}(1,1,1,\ldots)\,\beta &= (I(\beta_1), a_1, \ldots, a_q, a, a, \ldots)\,\mathrm{sh}(b_1^{-1}\,b_2)\,[1, q_2+1]\\ &= (I(\beta_1), 1, 1, \ldots)\,\mathrm{sh}(\beta_2)\,[1,0]\\ &= (I(\beta_1), I(\beta_2), I(\beta_2), \ldots)\,[1,0]\\ &= (I(\beta), I(\beta), I(\beta), \ldots).\end{aligned}$$

Conversely, we observe as in Section 1 that 1 is a special braid, so that, if the sequence $(1,1,\ldots)\,\beta$ exists, it consists of special braids. So (ii) implies that $(1,1,1,\ldots)\,\beta$ has the form $(I(\beta'), I(\beta'), \ldots)$ for some special extended braid β'. Now the latter sequence is the value of $(1,1,1,\ldots)\,\beta'$ as well, so Lemma 5.12 implies $\beta' = \beta$. ■

As an application, we deduce:

Proposition 5.14. *The extended braid $[b,q]$ is special if and only if there exist special braids $b_1, \ldots, b_q$ such that b is equal to $b_1\,\mathrm{sh}(b_2)\ldots\mathrm{sh}^{q-1}(b_q)$.*

Proof. Assume that $[b,q]$ is special and b belongs to B_n. We assume $n \geq q$. By Proposition 5.13, the sequence $(1, \ldots, 1)\,b$ ($n{+}1$ times 1) exists. Let $(b_1, \ldots, b_n, 1)$ be its value. Always by Proposition 5.13, we have $I_q(b) = b_1{}^\wedge \ldots {}^\wedge b_q{}^\wedge b_i$ for every $i > q$. Hence, in particular, we have $I_q(b) = b_1{}^\wedge \ldots {}^\wedge b_q{}^\wedge 1$, and, because $(B_\infty, {}^\wedge)$ admits left cancellation, $b_i = 1$ for $i > q$. Applying Formula (2.3), we deduce that b admits the decomposition $b_1\,\mathrm{sh}(b_2)\ldots\mathrm{sh}^{q-1}(b_q)$. Conversely, if b has the previous form, a direct computation shows that the sequence $(1,1,\ldots)\,[b,q]$ exists and it the constant sequence with value $b_1{}^\wedge \ldots {}^\wedge b_q{}^\wedge 1$. By Proposition 5.13, we conclude that $[b,q]$ is special—and that the value of $I([b,q])$ is $b_1{}^\wedge \ldots {}^\wedge b_q{}^\wedge 1$. ■

We have seen in Proposition 5.5 that computing square roots in $(EB_\infty, *)$ is easy. Computing square roots in free LD-systems is a much more difficult task. Let us for instance consider the equation $x^{[2]} = [1,0]^{[4]}$. As $[1,0]^{[4]}$ is $[1,3]$, we know by Proposition 5.5 that the solutions in EB_∞ are all extended braids $[b,2]$ with b in B_3. Solving the equation in the monogenerated free LD-system amounts to finding among the previous solutions those that are special. By Proposition 5.14, this is equivalent to finding the pairs (b_1, b_2) of special braids such that $b_1\mathrm{sh}(b_2)$ belongs to B_3. It is easy to check that the four pairs $(1,1)$, $(1,\sigma_1)$, (σ_1,σ_1) and $(\sigma_1^2\sigma_2^{-1}, 1)$ work, this leading to four distinct solutions of $x^{[2]} = [1,3]$ in EB_∞, namely $[1,2](= [1,0]^{[3]})$, $[\sigma_2, 2](= [1,0]^{[3]} * [1,0]^{[2]})$, $[\sigma_1\sigma_2, 2](= ([1,0]^{[3]} * [1,0]_{[3]})$

and $[\sigma_1^2\sigma_2^{-1}, 2](= [1,0]_{[3]} * [1,0]^{[2]})$. But we have no proof that there are no other special solution. As we mentioned above, a positive answer to Question 1.12 would imply that there are at most 2^n special braids in B_n and lead to a systematic way for solving equations like the one considered here.

5.4. Division

By Proposition 1.2, we know that, for $[a,p]$, $[c,r]$ special extended braids, there exists a special extended braid $[b,q]$ satisfying $[a,p] * [b,q] = [c,r]$ if and only if $[a,p] * [c,r]$ is equal to $[a,p]^{[2]} * [c,r]$. Let us consider the question of whether this characterization holds for arbitrary extended braids.

Lemma 5.15. *Let $[a,p]$ and $[c,r]$ be arbitrary extended braids. Let d be the braid $\tau_p^{-1}a^{-1}c$.*

(i) There exists an extended braid $[b,q]$ such that $[a,p] * [b,q]$ is equal to $[c,r]$ if and only if r is at least 1 and the braid d belongs to $\mathrm{sh}(B_\infty) \cdot B_r$.

(ii) The equality $[a,p] * [c,r] = [a,p]^{[2]} * [c,r]$ holds if and only if the braid $\mathrm{sh}(d^{-1})\sigma_1\mathrm{sh}(d)$ belongs to B_{r+1}.

Proof. (i) By definition, the equality $[a,p] * [b,q] = [c,r]$ is equivalent to the conjunction of $q+1=r$ and of $c^{-1}\,a\,\tau_p\,\mathrm{sh}(a^{-1}b) \in B_r$. Assume that these conditions hold. Then $\mathrm{sh}(b^{-1}\,a)d$ belongs to B_r, hence there exists a braid e in B_r such that $\mathrm{sh}(a)de$ belongs to $\mathrm{sh}(B_\infty)$. As $\mathrm{sh}(a)$ belongs to $\mathrm{sh}(B_\infty)$, this implies that de belongs to $\mathrm{sh}(B_\infty)$, and, therefore, that d belongs to $\mathrm{sh}(B_\infty) \cdot B_r$. Conversely, assume $r \geq 1$ and $d = \mathrm{sh}(f)e^{-1}$ for some e in B_r. Define b and q by $b = af$ and $q = r-1$. Then $c^{-1}\,a\,\tau_p\,\mathrm{sh}(a^{-1}\,b)$ belongs to B_r, and $[a,p] * [b,q] = [c,r]$ holds. Observe that the previous condition defines a unique extended braid, for replacing the braid e with another braid e' in B_r amounts to replacing b with b' such that $b^{-1}b'$ belongs to B_{r-1}: this means that the pairs (b,q) and (b',q) represent the same extended braid.

(ii) First $[a,p]^{[2]}$ is equal to $[a\tau_p, p+1]$. So, using the equality $\tau_p\tau_{p+1}\mathrm{sh}(\tau_p^{-1}) = \tau_{p+1}$, we obtain the explicit values

$$[a,p] * [c,r] = [a\ \tau_p\ \mathrm{sh}(a^{-1}\ c), r+1]$$
$$[a,p]^{[2]} * [c,r] = [a\ \tau_{p+1}\ \mathrm{sh}(a^{-1}\ c), r+1].$$

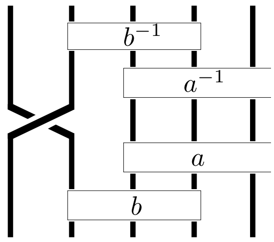
The previous extended braids are equal if and only if the quotient braid

$$(a\ \tau_p\ \mathrm{sh}(a^{-1}\ c))^{-1}\ (a\ \tau_{p+1}\ \mathrm{sh}(a^{-1}\ c)) \tag{5.3}$$

belongs to B_{r+1}. Using the equality $\tau_p^{-1}\ \tau_{p+1} = \mathrm{sh}(\tau_p)\,\sigma_1\ \mathrm{sh}(\tau_p^{-1})$, we see that the braid in (5.3) is equal to $\mathrm{sh}(d^{-1})\ \sigma_1\ \mathrm{sh}(d)$, which gives the desired condition. ∎

As is obvious on figure below, if the braid d belongs to $\mathrm{sh}(B_\infty) \cdot B_r$, the braid

$\mathrm{sh}(d^{-1})\sigma_1\mathrm{sh}(d)$ belongs to B_{r+1}.



Question 5.16. *Assume that b is a braid in B_∞ such that $\mathrm{sh}(b^{-1})\sigma_1\mathrm{sh}(b)$ belongs to B_{n+1}. Does b belong necessarily to $\mathrm{sh}(B_\infty) \cdot B_n$?*

A positive answer to the question would give for the LD-system $(EB_\infty, *)$ a complete description of left division. A (very weak) partial result in this direction is

Proposition 5.17. *The answer to Question 5.16 is positive in the case $n = 1$.*

Proof. We assume that the braid b satisfies $\mathrm{sh}(b^{-1})\sigma_1\mathrm{sh}(b) = \sigma_1^m$ for some integer m, and we wish to deduce that b belongs to $\mathrm{sh}(B_\infty)$. First we claim that m must be 1. Indeed, $m \leq 0$ is impossible as a σ_1-positive braid cannot be σ_1-negative. Then, let f be the standard image of b in the group $\mathrm{Aut}(F_\infty)$, where F_∞ is the free group based on the sequence $(x_1, x_2, \ldots)$. By construction, $f(x_1)$ has the form $x_1 w x_1^{-1}$, where w is a freely reduced word not involving x_1. On the other hand, for $m \geq 2$, if g is the image of σ_1^m in $\mathrm{Aut}(F_\infty)$, $g(x_1)$ is $x_1 x_2 x_1 \ldots x_1^{-1} x_2^{-1} x_1^{-1}$, $m+1$ positive letters, m negative letters. Thus the only possibility is $m = 1$. Then the result follows from Lemma 1.3—or from the fact that w above must be x_2, which is possible only if $\mathrm{sh}(b)$ has an expression where $\sigma_2^{\pm 1}$ does not occur. ∎

The case of right division is easy. Developing the definition gives:

Proposition 5.18. *Assume that $[b, q]$ and $[c, r]$ are extended braids. Then there exists an extended braid $[a, p]$ satisfying $[c, r] = [a, p] * [b, q]$ if and only if r is $q + 1$ and $c\,\mathrm{sh}(b^{-1})$ belongs to the image of I_p.*

5.5. The order on EB_∞

Let $<$ be the relation on EB_∞ such that $[a, p] < [b, q]$ holds if and only if the inequality $a\tau_{p,n} < b\tau_{q,n}$ holds in B_∞ for n large enough. Then $<$ is a linear ordering on EB_∞ that extends the braid ordering (with respect to the embedding $b \mapsto [b, 0]$ of B_∞ into EB_∞), and $[b, q]$ is the limit of the increasing sequence $(b\tau_{q,n}; n \geq 0)$.

As in the case of braids, we know that the inequalities $\alpha < \alpha * \beta$ and $\beta < \alpha * \beta$ hold when α and β are special extended braids. This leads to the question of whether these inequalities hold for arbitrary extended braids.

Proposition 5.19. *The inequalities $\alpha < \alpha * \beta$ and $\beta < \alpha * \beta$ hold for all extended braids α, β.*

Proof. The first inequality is obvious, so we consider the second one. Assume that (a, p) represents α and (b, q) represents β. Developing the expressions and letting c be $a^{-1}b\,\tau_{q,n}$, we see that $\beta < \alpha * \beta$ holds in EB_∞ if and only if

$$1 < c^{-1}\ \tau_p\ \mathrm{sh}(c)\,\tau_{1,n} \tag{5.4}$$

holds in B_∞ for n large enough. Now, by Lemma 3.5, we know that $c^{-1}\ \mathrm{sh}(c)\,\sigma_1$ is σ_1-positive. By [27], inserting positive generators in a σ_1-positive braids preserves its σ_1-positivity. So it is clear that the braid $c^{-1}\ \tau_p\ \mathrm{sh}(c)\,\tau_{1,n}$ is σ_1-positive for every p, and for $n \geq 1$. ■

Finally, let us briefly mention that the alternative operation ^ on EB_∞ does not behave nicely with respect to the ordering. The main reason is that the embedding $b \mapsto [b, 0]$ of B_∞ into EB_∞ is increasing, but the embedding $b \mapsto [b, 1]$ is not: for instance, $\sigma_1 > \sigma_2$ holds in B_∞, while $[\sigma_1, 1] < [\sigma_2, 1]$ holds in EB_∞. This implies that even the inequality $\alpha < \alpha$^β does not hold in general in EB_∞: for instance $[\sigma_1, 1] > [\sigma_1, 1]$^$[\sigma_1^{-2}, 1]$ holds in EB_∞.

The previous results may suggest that, as far as the self-distributive structure is concerned, the system $(EB_\infty, *)$ of extended braids behaves better than the larger system $(B_\infty,$ ^$)$ of ordinary braids. In particular, answering the questions of Section 4 about possible quotients could turn to be easier in the framework of extended braids.

References

[1] J. Birman, *Braids, Links, and Mapping Class Groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

[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, *A canonical ordering for free LD systems*, Proc. Amer. Math. Soc. **122-1** (1994) 31–37.

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

[6] —, *A normal form for the free left distributive law*, Int. J. for Algebra & Computation **4-4** (1994) 499–528.

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

[8] —, *Weak faithfulness properties for the Burau representation*, Topology and its Applic **69** (1996) 121–143.

[9] —, *Construction of left distributive operations*, Preprint.

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

[11] —, *Three-dimensional realizations of braids*, J. London Math. Soc., to appear.

[12] —, *Transfinite braids and left distributive operations*, Math. Zeitschr. **228** (1998) 405–433.

[13] R. Dougherty, *Critical points in an algebra of elementary embeddings*, Ann. P. Appl. Logic **65** (1993) 211–241.

[14] R. Dougherty & T. Jech, *Finite left-distributive algebras and embedding algebras*, Advances in Math., to appear.

[15] A. Drápal, *Homomorphisms of primitive left distributive groupoids*, Comm. in Algebra **22-7** (1994) 2579–2592.

[16] —, *Finite left distributive groupoids with one generator*, Int. J. for Algebra Computation, to appear.

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

[18] R. Fenn, M. Greene, D. Rolfsen, C. Rourke & B. Wiest, *Ordering the braid groups*, Preprint (1998).

[19] R. Fenn, D. Rolfsen & J. Zhu, *Centralisers in the braid group and singular braid monoid*, L'Enseignement Mathematique **42** (1996) 75–96.

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

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

[22] L. Kauffman, *Knots and Physics*, World Scientific (1991).

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

[24] —, *Left-distributive and left-distributive idempotent algebras*, Ph D Thesis, University of Colorado, Boulder (1994).

[25] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91-2** (1992) 209–231.

[26] —, *On the algebra of elementary embeddings of a rank into itself*, Advances in Math. **110** (1995) 334–346.

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

[28] D. Long & M. Paton, *The Burau representation is not faithful for $n \geq 6$*, Topology **32-2** (1993) 439–447.

[29] J. Moody, *The Burau representation of the group B_n is unfaithful for large n*, Bull. Americ. Math. Soc. **25-2** (1991) 379–384.

[30] D. Rolfsen & J. Zhu, *Braids, orderings and zero divisors*, Proc. Amer. Math. Soc., to appear.

[31] B. Wiest, *Dehornoy's ordering of the braid groups extends the subword ordering*, Preprint (1998).