TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 345, Number 1, September 1994

BRAID GROUPS AND LEFT DISTRIBUTIVE OPERATIONS

PATRICK DEHORNOY

ABSTRACT. The decidability of the word problem for the free left distributive law is proved by introducing a structure group which describes the underlying identities. This group is closely connected with Artin's braid group B_∞. Braid colourings associated with free left distributive structures are used to show the existence of a unique ordering on the braids which is compatible with left translation and such that every generator σ_i is preponderant over all σ_k with $k > i$. This ordering is a linear ordering.

The first goal of the present paper is to give a proof of the following result, which had been conjectured for several years:

Theorem. *There is an effective algorithm for deciding whether a given identity is or is not a consequence of the left distributivity identity* $x(yz) = (xy)(xz)$.

Until recently this question has had a rather unusual status. Conditional solutions were given independently in [6] and [24], where the decision problem was reduced to a specific algebraic hypothesis, one which had been shown by Richard Laver to be a consequence of a very strong set-theoretical axiom, of a type which certainly cannot be derived from the usual axioms of set theory, namely, a large cardinal axiom. The question as to whether a strong axiom of this type was actually needed remained open. Opinions were in fact divided: a connection between large cardinals and a purely finitistic problem of this caliber would seem paradoxical, but it is well known that problems of a combinatorial type can embody surprisingly strong proof principles (see for instance [28]), and some work on free distributive structures has shown that they do give rise to intrinsically complex objects, typically nonprimitive recursive ones (cf. [12, 13]).

We will show that in the present case a solution which is purely algebraic in terms of the methods employed and the spirit of the argument can in fact be given. In particular, no unusual set-theoretical axioms are required for this argument. The decision method described in [6] was fully effective, but the proof of the *correctness* of the algorithm amounted to a direct invocation of this specific algebraic hypothesis which followed from a large cardinal axiom, with no hint of a direct proof. We shall refine this decision method below, introducing uniqueness at each step of the process, and the correctness will then be seen to follow very naturally.

Received by the editors February 5, 1993.
1991 *Mathematics Subject Classification*. Primary 20F36, 17A30, 17A50.
Key words and phrases. Braid group, word problem, nonassociative algebras, free algebras.

The main tools we use are "witnesses" for the left distributivity equivalences. These objects live in a big partial monoid $\mathscr{M}_{\mathrm{LD}}$ which is reminiscent of groupoids introduced in category theory (cf. [27, 3, 8]). The crucial point will be to guess a presentation of $\mathscr{M}_{\mathrm{LD}}$, and then to work with the group $\widetilde{B}_\infty$ admitting the same presentation. The main idea is that the relations used to define $\widetilde{B}_\infty$ should capture the essence of left distributivity, and hence $\widetilde{B}_\infty$ should resemble $\mathscr{M}_{\mathrm{LD}}$. In particular, the results proved for $\mathscr{M}_{\mathrm{LD}}$ using the geometry of left distributivity should have purely algebraic counterparts in $\widetilde{B}_\infty$; this happens to be true.

The group $\widetilde{B}_\infty$ is an extension of the infinite braid group B_∞, a fact which reflects a deep connection between braids and distributive operations. Actually $\widetilde{B}_\infty$ may be considered a 'ramified' version of B_∞ in which the linearly ordered sequence of integers is replaced by an infinite tree. The kernel of the natural map of $\widetilde{B}_\infty$ onto B_∞ is large, but both groups share very similar properties. In particular, the algebraic analysis developed by Garside for B_∞ in [17] can be extended to $\widetilde{B}_\infty$.

After applying properties of the group $\widetilde{B}_\infty$ to our decision algorithm for left distributivity equivalence, we will derive some consequences for its quotient B_∞ using convenient braid colourings. This leads to a new and more efficient algorithm for left distributivity equivalence and also to the realization of the free left distributive structure on one generator as a subset of B_∞. Braid colourings can also be used to transfer some order properties of free left distributive structures to B_∞, yielding

Theorem. *There is a unique partial ordering on the group B_∞ which is compatible with left translation and is such that every generator σ_i is infinitely large relative to all σ_k with $k > i$. This partial ordering is in fact a linear ordering which extends the partial ordering given by left divisibility. It is also effective, in the sense that there is an algorithm for comparing two braid words with respect to this ordering.*

After the first draft of this paper was circulated in the spring of 1992, David Larue gave a direct combinatorial argument in [22] for the property of braids which we use in our second algorithm and which we derive from an analysis of the group $\widetilde{B}_\infty$. Larue's argument gives a shorter proof for the decidability of left distributivity equivalence, but we would argue that the present proof is more natural. In particular, it seems difficult to justify the introduction of the "braid bracket", as well as the second algorithm itself, without reference to $\widetilde{B}_\infty$. Other results which use the methods and intuitions associated with $\widetilde{B}_\infty$, although their statements do not involve this group, are the existence of the linear ordering on B_∞ and the description in [11] of a quick algorithm for comparison of braid words.

The paper is organized as follows. The first comparison algorithm for left distributivity equivalence is presented in §1, and its correctness is reduced to obtaining an effective version for three basic properties of left distributivity. Sections 2, 3, and 4 successively treat the case of these three properties. Section 5 states some corollaries of the decidability result concerning the free left distributive structures. Section 6 studies the projection to B_∞ of the previous results and goes from braids to left distributive structures in order to define the second algorithm for left distributivity equivalence. Section 7 finally goes from left distributive structures to braids and constructs the linear ordering on B_∞.

1. The comparison method

We consider terms constructed using variables from a set Σ and a binary operator and ask whether two terms P, Q become equivalent when the left distributivity identity is assumed. The product of P and Q will be denoted by $P[Q]$, so that left distributivity is expressed as the identity

$$x[y[z]] = x[y][x[z]].$$

The set of all terms constructed using the elements of Σ and bracket is denoted $\mathcal{T}_\Sigma$. We also fix an element a of Σ and write $\mathcal{T}_a$ for the set of all terms involving only a. The question we investigate is the decidability of the congruence $=_{\mathrm{LD}}$ on $\mathcal{T}_\Sigma$ generated by the pairs $(P[Q[R]], P[Q][P[R]])$. Two terms P, Q satisfying $P =_{\mathrm{LD}} Q$ will be called LD-*equivalent.* Since the quotient structure $\mathcal{T}_\Sigma / =_{\mathrm{LD}}$ is the free left distributive structure generated by Σ, the above question is simply the word problem for free left-distributive structures. We shall at first consider the special case of one variable, i.e. the restriction of $=_{\mathrm{LD}}$ to $\mathcal{T}_a$.

In order to sketch the term comparison process we need some notation. The *right powers* of the term a are the terms $a^{[n]}$ inductively defined by $a^{[1]} = a$ and $a^{[n+1]} = a[a^{[n]}]$. Then we introduce a refinement of the relation $=_{\mathrm{LD}}$ as follows. Two terms P, Q are LD-equivalent if P can be transformed into Q by applying a finite sequence of elementary transformations, each of which consists either in replacing some subterm $R[S[T]]$ by the corresponding subterm $R[S][R[T]]$ or in replacing some subterm $R[S][R[T]]$ by the corresponding subterm $R[S[T]]$. We say that Q is an *expansion* of P if only the first type of elementary transformations is used in some sequence leading from P to Q. Finally for any term P which is not the atomic term a we denote by $l(P)$ the left subterm of P. The following results about the equivalence relation $=_{\mathrm{LD}}$ are established in [5] and [6].

Property A. *For any term P in $\mathcal{T}_a$, the terms $a^{[n+1]}$ and $P[a^{[n]}]$ and LD-equivalent for n large enough.*

Property B. *Two LD-equivalent terms have a common expansion.*

Property C. *If R is an expansion of P and P is not a, then for some integer r the term $l^r(R)$ is an expansion of $l(P)$.*

The following three facts immediately follow. Let P, Q be arbitrary terms in $\mathcal{T}_a$.

Fact A. *For some integer n, the terms $P[a^{[n]}]$ and $Q[a^{[n]}]$ are LD-equivalent.*

Fact B. *For some integer n and some term R, the terms $P[a^{[n]}]$ and $Q[a^{[n]}]$ admit R as a common expansion.*

Fact C. *For some term R and some integers p, q the term $l^p(R)$ is an expansion of P and the term $l^q(R)$ is an expansion of Q.*

The idea is to decide the LD-equivalence of the terms P and Q by comparing the integers p and q obtained in Fact C. One direction is trivial. Indeed, if p and q are equal, then P and Q must be LD-equivalent since both of them are LD-equivalent to $l^p(R)$.

There are now two ways for completing the scheme in order to obtain an effective decision method. In the first approach we observe that objects R, p, q satisfying the conclusion of Fact C can always be found by an exhaustive enumeration of all expansion of the initial terms P and Q. (Of course, these objects need not be unique.) Write $R \sqsubset S$ if the term R is an iterated left subterm of the term S, i.e., if R is $l^r(S)$ for some $r \geq 1$, and denote by $\sqsubset_{\mathrm{LD}}$ the $=_{\mathrm{LD}}$-saturation of the relation $\sqsubset$. If the integers p, q in the conclusion of Fact C are not equal, then either $l^p(R) \sqsubset l^q(R)$ or $l^q(R) \sqsubset l^p(R)$ holds, and therefore $P \sqsubset_{\mathrm{LD}} Q$ or $Q \sqsubset_{\mathrm{LD}} P$ holds. Assume that the relation $\sqsubset_{\mathrm{LD}}$ is known to be antireflexive, i.e., that $P \sqsubset_{\mathrm{LD}} P$ never holds; then we can conclude that P and Q are not LD-equivalent. So we have the following partial result:

Proposition 1 [6]. *If the relation $\sqsubset_{\mathrm{LD}}$ is antireflexive, the relation $=_{\mathrm{LD}}$ is decidable in the case of one variable.*

It is remarkable that Richard Laver in [24] obtains the same result using a completely different method. A major argument in favor of the antireflexivity of the relation $\sqsubset_{\mathrm{LD}}$ is another result of Laver in [24]:

Theorem 2 [24]. *Assume the existence of an n-huge cardinal for every integer n. Then the relation $\sqsubset_{\mathrm{LD}}$ on $\mathscr{T}_a$ is antireflexive.*

Let us say that a set endowed with a left distributive bracket is an LD-*system* and that an LD-system $\mathfrak{g}$ is *antireflexive* if no equality of the form

$$x = x[y_1] \cdots [y_k]$$

may hold in $\mathfrak{g}$. Laver constructs from the elementary embeddings associated with the large cardinals whose existence is assumed an antireflexive LD-system. It then follows that the free LD-system with one generator is itself antiflexive, which exactly means that the relation $\sqsubset_{\mathrm{LD}}$ is antireflexive on $\mathscr{T}_a$. This is the way a very strong logical assumption was connected with the decidability of the relation $=_{\mathrm{LD}}$.

A second approach for comparing terms by means of the scheme above is to show by a direct computation that the final integers p, q must be equal if the initial terms P, Q are LD-equivalent. Such a computation is made difficult by the lack of uniqueness at each step of the process. Our natural idea therefore will be to refine the method by selecting at each step *canonical witnesses* so that the effective computation can be carried out. The final algorithm will therefore keep the general structure described above and look like the following:

Comparison algorithm. Let P, Q be two terms in $\mathscr{T}_a$.

Step A. Determine a witness $\varphi(P, Q)$ for the LD-equivalence of the terms $P[a^{[n]}]$ and $Q[a^{[n]}]$ for n large enough.

Step B. Deduce witnesses $F(P, Q)$ and $G(P, Q)$ for the existence of a common expansion R for the terms $P[a^{[n]}]$ and $Q[a^{[n]}]$.

Step C. Deduce integers $f(P, Q)$ and $g(P, Q)$ such that the term $l^{f(P,Q)}(R)$ is an expansion of P and the term $l^{g(P,Q)}(R)$ is an expansion of Q. Then P and Q are LD-equivalent if and only if the integers $f(P, Q)$ and $g(P, Q)$ are equal.

Since each step in the comparison originates in the corresponding Property A, B, or C, our task will be to establish an *effective version* of these properties comprising an existence result (to be used in order to define the canonical objects) and a uniqueness result (to be used in order to propagate the initial assumption $P =_{\mathrm{LD}} Q$ toward the final equality $f(P, Q) = g(P, Q)$).

2. Effective version of Property A: The group $\widetilde{B}_\infty$

The point is to introduce adequate "witnesses" for describing LD-equivalence of terms. These witnesses will live in some big structure endowed with a partial associative operation. This structure can also be described as the set of all consequences of the left distributivity identity endowed with a convenient product.

As we already observed, two terms P, Q are LD-equivalent if and only if there exists a composition of finitely many elementary transformations which maps P to Q, each elementary transformation consisting in applying the left distributivity identity to some subterm. Let us denote by Ω the partial operator on $\mathscr{T}_\Sigma$ which maps any term of the form $R[S[T]]$ to the corresponding term $R[S][R[T]]$. We also have to introduce the translated copies of Ω associated with the various points where Ω could be applied. First we need notation for the subterms of a given term. We use the geometrical intuition of binary trees for representing terms and finite sequences of 0's and 1's for addressing the points in such trees.

Definition. (i) The monoid $\mathbb{S}$ is the set of all finite sequences of 0's and 1's endowed with concatenation. The empty sequence of $\mathbb{S}$ is denote by Λ.

(ii) For P in $\mathscr{T}_\Sigma$ and w in $\mathbb{S}$ short enough, $P_{(w)}$ is the subterm of P "with root at w", i.e., $P_{(w)}$ is determined by the inductive clauses: $P_{(\Lambda)}$ is P is any case, and if P is $Q[R]$, then $P_{(0w)}$ is $Q_{(w)}$ and $P_{(1w)}$ is $R_{(w)}$.

We denote by Ω_w the w-translated copy of Ω: applying Ω_w to P consists of replacing the subterm $P_{(w)}$, which is $P_{(w0)}[P_{(w10)}[P_{(w11)}]]$, by

$$P_{(w0)}[P_{(w10)}][P_{(w0)}[P_{(w11)}]].$$

We consider the monoid generated by all (partial) operators Ω_w and Ω_w^{-1} under reverse composition and denote by $\mathscr{M}_{\mathrm{LD}}$ the subset of this monoid made by excluding the empty operator. It should be clear that two terms P, Q are LD-equivalent if and only if some operator in $\mathscr{M}_{\mathrm{LD}}$ maps P to Q. So the elements of $\mathscr{M}_{\mathrm{LD}}$ are witnesses for LD-equivalences. For effective computations we shall use the following notation.

Definition. (i) The monoid $\mathscr{S}^+$ is the free monoid generated by $\mathbb{S}$, and the monoid $\mathscr{S}$ is the free monoid generated by $\mathbb{S}$ and a disjoint copy $\overline{\mathbb{S}}$ of $\mathbb{S}$. The empty sequence of $\mathscr{S}$ is denoted by ε.

(ii) For $\overline{w}$ in $\overline{\mathbb{S}}$, $\Omega_{\overline{w}}$ is Ω_w^{-1} and the notation Ω_ξ is extended to ξ in $\mathscr{S}$ so that $\Omega_{\xi_1 \bullet \xi_2}$ is $\Omega_{\xi_2} \circ \Omega_{\xi_1}$.

For instance, if a, b, c, d are any variables in Σ, the operator $\Omega_{\overline{1} \bullet \Lambda}$ maps the term $a[b[c][b[d]]]$ to the (LD-equivalent) term $a[b][a[c[d]]]$. Observe that if we extend the "bar" notation so that for ξ in $\mathscr{S}$ the sequence ξ is obtained from ξ by reversing the ordering of the factors and exchanging w and $\overline{w}$, then $\Omega_{\overline{\xi}}$ is exactly the inverse mapping of Ω_ξ. Also observe that Ω_ξ may be empty: for geometrical reasons no term in the image of $\Omega_{\Lambda\bullet 1}$ may belong to the image of Ω_Λ and therefore $\Omega_{\Lambda\bullet 1\bullet\overline{\Lambda}}$ is empty. We have immediately

Lemma 1. (i) *Two terms P, Q in $\mathscr{T}_\Sigma$ are LD-equivalent if and only if there exists a sequence ξ in $\mathscr{S}$ such that Ω_ξ maps P to Q.*

(ii) *The term Q is an expansion of the term P if and only if there exists a sequence X in $\mathscr{S}^+$ such that Ω_X maps P to Q.*

We turn to Property A, which is proved in [6] by induction on the size of the term P in $\mathscr{T}_a$. Indeed, if P is a, the equivalence is an equality for every n. Now assume $P = Q[R]$, and

$$\begin{cases} a^{[n+1]} =_{\mathrm{LD}} Q[a^{[n]}] & \text{for } n \geq q, \\ a^{[n+1]} =_{\mathrm{LD}} R[a^{[n]}] & \text{for } n \geq r. \end{cases}$$

If n is greater than $q+1$ and $r+1$, the sequence of equivalences

$$a^{[n+1]} =_{\mathrm{LD}} Q[a^{[n]}] =_{\mathrm{LD}} Q[R[a^{[n-1]}]] =_{\mathrm{LD}} Q[R][Q[a^{[n-1]}]] =_{\mathrm{LD}} Q[R][a^{[n]}]$$

gives $a^{[n+1]} =_{\mathrm{LD}} P[a^{[n]}]$ and the induction goes on. So the equivalence $a^{[n+1]} =_{\mathrm{LD}} P[a^{[n]}]$ holds for $n \geq h(P)$, where $h(P)$ is the geometrical parameter defined by

$$h(P) = \begin{cases} 1 & \text{if } P \text{ is } a, \\ \sup(h(Q), h(R)) + 1 & \text{if } P \text{ is } Q[R] \end{cases}$$

($h(P)$ is the height of P viewed as a tree).

In order to obtain an effective witness for the above equivalences, we just have to translate in the language of the Ω-operators the inductive argument. Assume again $P = Q[R]$ and

$$\begin{cases} \Omega_\eta : a^{[n+1]} \mapsto Q[a^{[n]}] & \text{for } n \geq h(Q), \\ \Omega_\zeta : a^{[n+1]} \mapsto R[a^{[n]}] & \text{for } n \geq h(R). \end{cases}$$

If 1ζ is the sequence obtained from ζ by adding a 1 at the beginning of each factor and if n is at least $h(R)+1$, the operator $\Omega_{1\zeta}$ maps the term $Q[a^{[n]}]$ to the term $Q[R[a^{[n-1]}]]$ (as well as any term $S[a^{[n]}]$ to the corresponding term $S[R[a^{[n-1]}]]$). Similarly the operator $\Omega_{1\eta}$ maps the term $Q[R][a^{[n]}]$ to the term $Q[R][Q[a^{[n-1]}]]$. Hence the above sequence of equivalence translates into the following sequence:

$$a^{[n+1]} \overset{\Omega_\eta}{\mapsto} Q[a^{[n]}] \overset{\Omega_{1\zeta}}{\mapsto} Q[R[a^{[n-1]}]] \overset{\Omega_\Lambda}{\mapsto} Q[R][Q[a^{[n-1]}]] \overset{\Omega_{\overline{1\eta}}}{\mapsto} Q[R][a^{[n]}],$$

and we conclude that if ξ is the sequence $\eta \bullet 1\zeta \bullet \Lambda \bullet \overline{1\eta}$, the operator Ω_ξ maps $a^{[n+1]}$ to $P[a^{[n]}]$.

Definition. A bracket operation is defined on $\mathscr{S}$ by

$$\eta[\zeta] = \eta \bullet 1\eta \bullet \Lambda \bullet \overline{1\eta}.$$

Then χ is the bracket-preserving homomorphism of $\mathscr{T}_a$ to $\mathscr{S}$ which maps a to the empty sequence ε.

We have obtained

Proposition 2 (Effective Property A, existence part). *For any term P in $\mathcal{T}_a$ and any integer $n \geq h(P)$ the operator $\Omega_{\chi(P)}$ maps $a^{[n+1]}$ to $P[a^{[n]}]$.*

It follows that for any two terms P, Q in $\mathcal{T}_a$, the operator $\Omega_{\overline{\chi(P)}\bullet\chi(Q)}$ maps the term $P[a^{[n]}]$ to the term $Q[a^{[n]}]$ provided that n is at least the supremum of $h(P)$ and $h(Q)$. Assume that P and Q are LD-equivalent. By Lemma 1 there must exist a sequence ξ such that the operator Ω_ξ maps P to Q, and therefore the operator $\Omega_{0\xi}$ maps the term $P[a^{[n]}]$ to the term $Q[a^{[n]}]$ for any integer n, as well as the operator $\Omega_{\overline{\chi(P)}\bullet\chi(Q)}$.

Definition. For ξ, η in $\mathcal{S}$, the operators Ω_ξ and Ω_η are *compatible* (resp. *strongly compatible*) if there exists a term P such that the images of P under Ω_ξ and Ω_η exist and coincide (resp. if for any term P which belongs to the domains of Ω_ξ and Ω_η the images of P under Ω_ξ and Ω_η coincide).

So if the terms P and Q are equivalent, there exists a sequence ξ' in $\mathcal{S}$ such that the operators $\Omega_{\chi(P)\bullet\chi(Q)}$ and $\Omega_{0\xi'}$ are compatible. Both notions of compatibility and strong compatibility are strong properties which will be seen in §5 to coincide nearly with equality. But presently it is very uneasy to work directly with them for the double reason that compatibility is not clearly a transitive relation and no exhaustive set of generating pairs is known. The strategy will consist in introducing some refinement $\equiv$ of the compatibility relations and using it instead of compatibility. The definition of $\equiv$ will be made by using some pairs (ξ, η) such that the corresponding operators Ω_ξ and Ω_η are known to be strongly compatible and even equal.

Definition. (i) The *LD-pairs* are all pairs in $\mathcal{S}^+ \times \mathcal{S}^+$ of the following five types:

$$\begin{gathered}(u \bullet u1 \bullet u,\ u1 \bullet u \bullet u1 \bullet u0),\\ (u \bullet u11w,\ u11w \bullet u),\\ (u \bullet u01w,\ u10w \bullet u),\\ (u \bullet 10w \bullet u00w,\ u0w \bullet u),\\ (u0v \bullet u1w,\ u1w \bullet u0v),\end{gathered}$$

where u, v, and w range over $\mathbb{S}$.

(ii) The relation $\equiv^+$ is the congruence on the monoid $\mathcal{S}^+$ generated by all LD-pairs. The relation $\equiv$ is the congruence on the monoid $\mathcal{S}$ generated by all LD-pairs together with all pairs $(u \bullet \overline{u}, \varepsilon)$ and $(\overline{u} \bullet u, \varepsilon)$ for u in $\mathbb{S}$. The monoid $\mathcal{S}^+/\equiv^+$ is denoted by $\widetilde{B}_\infty^+$, and the group $\mathcal{S}/\equiv$ is denoted by $\widetilde{B}_\infty$.

An easy verification gives

Lemma 3. (i) *For X, Y in $\mathcal{S}^+$, $X \equiv^+ Y$ implies $\Omega_X = \Omega_Y$.*

(ii) *For ξ, η in $\mathcal{S}$, $\xi \equiv \eta$ implies that the operators Ω_ξ and Ω_η are strongly compatible.*

Geometrical intuition suggests that any equality or compatibility relation between the operators Ω_ξ follows from the relations given by LD-pairs, i.e., that LD-pairs give to some extent a complete description of the geometry of left distributivity. If this intuition is true, all geometric features arising from the action of the operators Ω_ξ on terms should have a purely algebraic counterpart involving only the relation $\equiv$. This approach consists of replacing the "bad" structure $\mathscr{M}_{\mathrm{LD}}$ (bad because the product is not defined everywhere and because the exact presentation is not known) by the "good" structure $\widetilde{B}_\infty$ (a true group with a perfectly known presentation).

There exists a close connection between the group $\widetilde{B}_\infty$ and Artin's braid group B_∞ (whence our notation). Its existence is connected with a deep relation between left distributivity and braids. For the moment this connection is important because it suggests to extend to $\widetilde{B}_\infty$ the algebraic tools which have been developed for B_∞, in particular by Garside in [17]. Recall that B_∞ is the group generated by an infinite sequence of generators $\sigma_1, \sigma_2, \ldots$ submitted to the relations

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

Lemma 4. *The mapping ψ of $\mathbb{S}$ to B_∞ which maps w to 1 if there is at least one 0 in w and maps 1^i to σ_{i+1} induces a surjective homomorphism of $\widetilde{B}_\infty$ onto B_∞.*

Proof. The existence of the morphism is immediate from the particular form of the LD-pairs. □

By construction $\psi(0w)$ is 1 for any w in $\mathbb{S}$, so the normal subgroup N_0 of $\widetilde{B}_\infty$ generated by all length 1 sequences $0w$ is included in the kernel of ψ. Actually the results of §3 could be applied to prove that the kernel of ψ is exactly the subgroup N_0.

Now the following result is natural if the conjecture that the congruence $\equiv$ resembles the compatibility relation is true.

Proposition 5 (Effective version of Property A, uniqueness part). *Assume that the operator Ω_ξ maps the term P to the term Q. Then one has*

$$\overline{\chi(P)} \bullet \chi(Q) \equiv 0\xi.$$

Proof. An explicit computation using the definition of the bracket on $\mathscr{S}$ shows the following equivalences for any sequences $\xi, \xi', \eta, \eta', \zeta$ in $\mathscr{S}$:

$$\xi[\eta][\xi[\zeta]] \equiv \xi[\eta[\zeta]] \bullet 0, \tag{1}$$
$$(\xi \bullet 0\xi')[\eta \bullet 0\eta'] \equiv \xi[\eta] \bullet 00\xi' \bullet 01\eta'. \tag{2}$$

Now for proving the proposition, we may assume that the sequence ξ has length 1, i.e., reduces to a unique factor w or $\overline{w}$. An induction will then finish the proof. Now by symmetry we may assume that ξ is w. We now use induction of the length of w (as a sequence of 0's and 1's). If w is Λ, the hypothesis that Ω_Λ maps the term P to the term Q means that Q is $P_{(0)}[P_{(10)}][P_{(0)}[P_{(11)}]]$, and therefore one has

$$\chi(P) = \xi[\eta[\zeta]] \quad \text{and} \quad \chi(Q) = \xi[\eta][\xi[\zeta]]$$

where $\xi = \chi(P_{(0)})$, $\eta = \chi(P_{(10)})$, and $\zeta = \chi(P_{(11)})$. Formula (1) gives the conclusion. Now assume that w is $0w'$. Since $\Omega_{0w'}$ maps P to Q, P cannot be a, so P is $P'[P'']$ for some terms P', P''. Then Q must be $Q'[P'']$ where Q' is the image of P' under $\Omega_{w'}$. By induction hypothesis, one has

$$\chi(Q') \equiv \chi(Q) \bullet 0w',$$

and therefore using (2) one obtains

$$\chi(Q) = \chi(Q')[\chi(P'')] = (\chi(P')\bullet 0w')[\chi(P'')] = \chi(P')[\chi(P'')]\bullet 00w' = \chi(P)\bullet 0w.$$

The argument is similar if w is $1w'$ for some w'. □

Definition. For P, Q in $\mathcal{T}_a$, $\varphi(P, Q)$ is the sequence $\overline{\chi(P)}\bullet\chi(Q)$.

The effective version of Property A yields at once

Fact A (Effective version). *Let P, Q be two terms in $\mathcal{T}_a$ and n be any integer at least equal to* $\sup(h(P), h(Q))$.

(i) *The operator $\Omega_{\varphi(P,Q)}$ maps $P[a^{[n]}]$ to $Q[a^{[n]}]$.*

(ii) *If P and Q are LD-equivalent, then $\varphi(P, Q) \equiv 0\xi'$ holds for some ξ' in $\mathcal{S}$.*

So according to the scheme of §1 it is natural to take the

Comparison algorithm. (Input: two terms P, Q in $\mathcal{T}_a$.)

Step A. Determine $\varphi(P, Q)$.

Example. Let P be the term $a[a][a[a[a]]]$ and Q be the term $a[a[a][a[a]]]$. Applying the inductive construction of χ, one obtains

$$\chi(P) = \Lambda\bullet 11\bullet 1\bullet\Lambda\bullet\overline{1}$$

and

$$\chi(Q) = 1\bullet 11\bullet 1\bullet\overline{11}\bullet\Lambda$$

and therefore

$$\varphi(P, Q) = \overline{\chi(P)}\bullet\chi(Q) = 1\bullet\overline{\Lambda}\bullet\overline{1}\bullet\overline{11}\bullet\overline{\Lambda}\bullet 1\bullet 11\bullet 1\bullet\overline{11}\bullet\Lambda.$$

Remark. The introduction of the monoid $\mathcal{M}_{\mathrm{LD}}$ (and therefore of its "improved version" $\widetilde{B}_\infty$) can be seen as the construction of a product on the left distributivity identities themselves. An identity, i.e. a pair of terms (P, Q), is a consequence of left distributivity just if $P =_{\mathrm{LD}} Q$ holds. Let us say that a term P' is a *substitute* of the term P if there exists a substitution Σ, i.e., a mapping of Σ to $\mathcal{T}_\Sigma$, such that P' is the term P^σ obtained from P by replacing every variable x by its image under σ. Similarly say that an identity (P', Q') is an *instance* of the identity (P, Q) if for some σ as above P' is P^σ and Q' is Q^σ. Assuming that Σ is an infinite set and a sequence $a_1, a_2, \ldots$ in Σ, has been fixed, we can define the *canonical* terms to be those terms P such that the leftmost occurrences of the variables occurring in P make an initial segment of $(a_1, a_2, \ldots)$.

By an inductive argument one verifies that for every ξ in $\mathcal{S}$ such that the mapping Ω_ξ is not empty, there exist unique canonical terms K_ξ and $\overline{K}_\xi$ such that the domain of Ω_ξ is exactly the set of all substitutes of K_ξ, the image of Ω_ξ is exactly the set of all substitutes of $\overline{K}(\xi)$, and for any substitution σ, Ω_ξ maps $(K_\xi)^\sigma$ to $(\overline{K}_\xi)^\sigma$. For instance, the term K_Λ is $a_1[a_2[a_3]]$ while the term $\overline{K}_\Lambda$ is $a_1[a_2][a_1[a_3]]$. The term K_ξ coincides with the term $\overline{K}_{\overline{\xi}}$. So Lemma 1 means that every consequence of left distributivity is an instance of some (nonunique) canonical identity of the form $(K_\xi, \overline{K}_\xi)$, and the monoid

$\mathscr{M}_{\mathrm{LD}}$ can be seen as being associated with a product on (canonical) identities. This product can easily be described in terms of substitutions by means of the unification formalism (see [8] for some remarks on this approach, which is essentially equivalent to the categorical point of view of [27]).

3. Effective version of Property B: decomposition as fractions in $\widetilde{B}_\infty$

In terms of the operators Ω_ξ, the fact that two LD-equivalent terms must have a common extension implies that for any sequence ξ in $\mathscr{S}$ (such that the domain of Ω_ξ is not empty), there exist *positive* sequences X, Y in $\mathscr{S}^+$ such that the operators Ω_ξ and $\Omega_{X\bullet\overline{Y}}$ are compatible. So it is natural to conjecture that any sequence ξ is $\equiv$-equivalent to a "(right) fraction" of the form $X\bullet\overline{Y}$ with X, Y positive sequences (i.e., sequences in $\mathscr{S}^+$). This would clearly be a convenient version of Property B.

We are thus led to study the expression of the elements of the group $\widetilde{B}_\infty$ as quotients of positive elements. The proof of the above conjecture will be a little long, but it is very natural because it refines and extends classical constructions used for the braid group B_∞. The details are given in [11] in a general setting and in the particular case of braids, so we shall be a little sketchy here and only emphasize the really specific points. The proof of Property B given in [5] cannot be transferred directly because it makes a crucial use of the terms and of the meaning of Ω_ξ as operators on terms. Here we need a purely syntactic proof using only the particular form of the LD-pairs.

The starting point is the observation that for any distinct u, v in $\mathbb{S}$ there exists exactly one LD-pair (X, Y) such that X begins with u and Y begins with v or conversely. Precisely, let C be the mapping of $\mathbb{S}\times\mathbb{S}$ into $\mathscr{S}^+$ defined by

$$C(u, v) = \begin{cases} v & \text{if } v \text{ is not a prefix of } u1 \text{ or } v11 \text{ is a prefix of } u, \\ u\bullet v\bullet u0 & \text{if } u1 = v, \\ \varepsilon & \text{if } u = v, \\ v10w\bullet v00w & \text{if } u = v0w, \\ v01w & \text{if } u = v10w, \\ u\bullet v & \text{if } u = v1 \end{cases}$$

(say that x is a prefix of y if y is xz for some z). Then all pairs $(u\bullet C(v, u), v\bullet C(u, v))$ are LD-pairs, and therefore one has, for any u, v in $\mathbb{S}$,

$$\overline{u}\bullet v \equiv C(v, u)\bullet\overline{C(u, v)}.$$

This is enough to transform any length 2 sequence into an $\equiv$-equivalent (right) quotient of positive sequences. For transforming similarly sequences with arbitrary length, we can easily iterate the previous method.

Definition. The sequence ξ *reduces* to the sequence η (with respect to the mapping C) if one can transform ξ to η by a finite composition of elementary transformations, each of which consists in replacing some subsequence $\overline{u}\bullet v$ by the corresponding subsequence $C(v, u)\bullet\overline{C(u, v)}$.

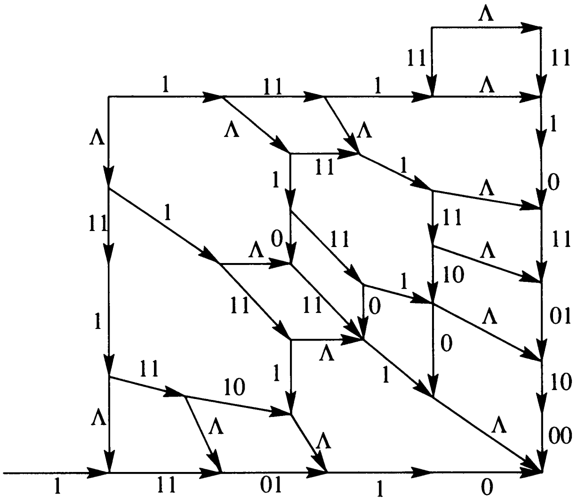


Figure 1

The irreducible sequences are the sequences $X \bullet \overline{Y}$ with X, Y positive. It is not obvious that any sequence should reduce to such an irreducible sequence, but an easy argument shows that if some reduction of ξ leads to $X \bullet \overline{Y}$, then any reduction of ξ leads to $X \bullet \overline{Y}$ and uses the same number of elementary steps. So the following notions make sense.

Definition. (i) For ξ in $\mathcal{S}$, the *numerator* $N(\xi)$ and the *denominator* $D(\xi)$ of x are the unique positive sequences X, Y such that ξ reduces to $X \bullet \overline{Y}$, if they exist.

(ii) For X, Y in $\mathcal{S}^+$, the *complement* $C(X, Y)$ of X in Y is the numerator of the sequence $\overline{Y} \bullet X$, if it exists.

There is no problem in the above notation for the complement: for u, v in $\mathbb{S}$, the numerator of $\overline{v} \bullet u$ exists and is $C(u, v)$ in any case. Reduction can be adequately illustrated in the Cayley graph of the group $\widetilde{B}_\infty$. It consists in "closing" the patterns made of two arrows which have the same origin but are not yet the initial segments of convergent paths. The number of elementary transformations used in the reduction is exactly the number of closed domains in the associated graph. Figure 1 illustrates the reduction of the sequence

$$1 \bullet \overline{\Lambda} \bullet \overline{1} \bullet \overline{11} \bullet \overline{\Lambda} \bullet 1 \bullet 11 \bullet 1 \bullet \overline{11} \bullet \Lambda$$

(the one obtained in the example at the end of §2) and shows that the numerator and denominator of this sequence do exist and respectively are

$$1 \bullet 11 \bullet 01 \bullet 1 \bullet 0 \quad \text{and} \quad 11 \bullet 1 \bullet 0 \bullet 11 \bullet 01 \bullet 10 \bullet 00.$$

By construction, we have

Lemma 1. *Assume that the numerator and the denominator of the sequence ξ exist. Then the equivalence*

$$\xi \equiv N(\xi) \bullet \overline{D(\xi)}$$

holds, and moreover the operator $\Omega_{N(\xi) \bullet \overline{D(\xi)}}$ includes the operator Ω_ξ (as a set of pairs).

So C-reduction gives (in an effective way) the wished decomposition when it terminates. The latter point, however, is quite problematic because the elementary complements $C(u, v)$ for u, v in $\mathbb{S}$ have length strictly greater than 1 in some cases.

In order to solve the problem, the idea is to introduce a subset $\widehat{\mathbb{S}}$ of $\mathscr{S}^+$ which strictly includes $\mathbb{S}$ and to construct a new complement mapping $\widehat{C}$ so that for X, Y in $\widehat{\mathbb{S}}$ the complement $\widehat{C}(X, Y)$ still lies in $\widehat{\mathbb{S}}$. It will then be clear that the reductions using $\widehat{C}$ have to terminate and more precisely that the determination of the $\widehat{C}$-numerator and denominator of a sequence ξ which is written as a product of p sequences in $\widehat{\mathbb{S}}$ and q inverses of sequences in $\widehat{\mathbb{S}}$ will require at most pq calls to the $\widehat{C}$ mapping.

For the definition of a convenient set $\widehat{\mathbb{S}}$, we use the geometry of left distributivity and the proof of Property B in [5]. We can also use the intuition given by the projection on braids (see the remark at the end of this section). The main point in the proof of Property B is the existence, for every term P in $\mathscr{T}_\Sigma$, of a "big" term ∂P such that ∂P is an expansion of every 1-expansion of P, where Q is said to be a 1-expansion of P when some operator Ω_w maps P to Q, i.e., Q is obtained from P by exactly one step of distribution. A close examination of the positive sequences X such that the operator Ω_X maps a term P to a term of which ∂P is an expansion suggests the following inductive construction.

Definition. (i) For w in $\mathbb{S}$ and k a nonnegative integer, $w_{(k)}$ is the empty sequence ε if k is 0 and is the sequence $w1^{k-1} \bullet w1^{k-2} \bullet \cdots \bullet w1 \bullet w$ otherwise.

(ii) The set $\widehat{\mathbb{S}}$ is the closure of $\{\varepsilon\}$ under all operations

$$(X, Y) \mapsto \Lambda_{(k)} \bullet 1X \bullet 0Y.$$

An easy induction shows that any sequence in $\widehat{\mathbb{S}}$ has a unique decomposition as $\prod^{\triangleright}_{w\in\mathbb{S}} w_{(k_w)}$ where $\langle k_w\,;\, w \in \mathbb{S}\rangle$ is a sequence of integers with only finitely many positive values and $\triangleright$ is the linear ordering on $\mathbb{S}$ such that $u \triangleright v$ holds if and only if either u is a strict prefix of v or there exists w such that $w1$ is a prefix of u and $w0$ is a prefix of v. Indeed it suffices to show the uniqueness of the initial factor $\Lambda_{(k_\Lambda)}$. To this end observe that Λ occurs at most once in any element of $\widehat{\mathbb{S}}$ and that k_Λ is the rank of this unique occurrence in the sequence (where rank 0 means no occurrence). The integer k_w will be called the *index* of w in X and will be denoted by $\operatorname{ind}(w, X)$. Notice that $\mathbb{S}$ is included in $\widehat{\mathbb{S}}$, for Λ clearly belongs to $\widehat{\mathbb{S}}$, and for every w in $\mathbb{S}$ the sequence wX is in $\widehat{\mathbb{S}}$ if (and only if) X is in $\widehat{\mathbb{S}}$.

Lemma 2. *Assume that X belongs to $\widehat{\mathbb{S}}$ and that the inequality*

$$l + \operatorname{ind}(1^l, X) < i + \operatorname{ind}(1^i, X)$$

holds for every $l < i$. Then the sequence $X \bullet \Lambda_{(i)}$ is $\equiv^+$-equivalent to a sequence X' in $\widehat{\mathbb{S}}$ such that $\operatorname{ind}(\Lambda, X')$ *is* $i + \operatorname{ind}(1^i, X)$.

Proof. The result is easily deduced from the following formulas, which hold for any integer p, k, i and any sequence Y in $\mathscr{S}^+$

$$1^p{}_{(k)} \bullet \Lambda_{(i)} \begin{cases} \equiv^+ \Lambda_{(i)} \bullet 1^p{}_{(k)} & \text{if } i < p, \\ = \Lambda_{(k+i)} & \text{if } i = p, \\ \equiv^+ \Lambda_{(i)} \bullet 1^{p+1}{}_{(k)} \bullet 01^p{}_{(k)} & \text{if } i > p + k. \end{cases}$$

$$1^p 0Y \bullet \Lambda_{(i)} \equiv^+ \begin{cases} \Lambda_{(i)} \bullet 1^p 0Y & \text{if } i < p, \\ \Lambda_{(i)} \bullet 01^p Y & \text{if } i = p, \\ \Lambda_{(i)} \bullet 1^{p+1}0Y \bullet 01^p 0Y & \text{if } i > p. \end{cases}$$

The first two cases in the first formula are easy, as well as the particular case $k = 0$. For the third case, denote by $\mathcal{F}(p, k, i)$ the formula

$$1^p{}_{(k)} \bullet \Lambda_{(i)} \equiv^+ \Lambda_{(i)} \bullet 1^{p+1}{}_{(k)} \bullet 01^p{}_{(k)}.$$

One proves $\mathcal{F}(p, k, i)$ for $p \geq 0, k \geq 1$, and $i > p + k$ inductively on p. First $\mathcal{F}(0, k, i)$ is proved inductively on $k \geq 1$, and to this end, $\mathcal{F}(0, 1, i)$ is proved inductively on i starting from $\mathcal{F}(0, 1, 2)$ which corresponds to the first LD-pair. The second formula is proved similarly using induction on $i \geq 0$. □

Proposition 3. *There exists an effective mapping $\widehat{C}$ of $\widehat{\mathbb{S}} \times \widehat{\mathbb{S}}$ into $\widehat{\mathbb{S}}$ such that, for every X, Y in $\widehat{\mathbb{S}}$, the equivalence*

$$X \bullet \widehat{C}(Y, X) \equiv^+ Y \bullet \widehat{C}(X, Y)$$

holds.

Proof. We shall construct the mapping $\widehat{C}$ by defining the values $\widehat{C}(X, Y)$ inductively on the minimal size of a term both in the domain of Ω_X and Ω_Y (a parameter which would probably be hard to introduce by purely combinatorial means). It has been said at the end of §2 that, for any sequence ξ such that the operator Ω_ξ is not empty, the domain of Ω_ξ is the set of all substitutes of some canonical term K_ξ. In the case of a positive sequence X, the operator Ω_X cannot be empty. Moreover, if X, Y are two positive sequences, then the intersection of the domains of Ω_X and Ω_Y is not empty and is the set of all substitutes of a (unique) canonical term $K_{X,Y}$. Then the minimal size of a term both in the domains of Ω_X and of Ω_Y is the size of the term $K_{X,Y}$. The result is clearly true if $K_{X,Y}$ has size 1, for in this case X and Y must be empty.

Now let X, Y be arbitrary positive sequences. Say that the integer k is accessible to X if k is $1 + \operatorname{ind}(1^i, X)$ for some integer i satisfying the hypothesis of Lemma 2. Because the integers $\operatorname{ind}(1^i, X)$ and $\operatorname{ind}(1^i, Y)$ must be 0 for i large enough, every integer which is large enough is accessible to X and Y. Let k be the minimal number which is accessible both to X and Y, and let i and j be the least integers satisfying

$$k = i + \operatorname{ind}(1^i, X) = j + \operatorname{ind}(1^j, Y).$$

By Lemma 2, the sequences $X \bullet \Lambda_{(i)}$ and $Y \bullet \Lambda_{(j)}$ are $\equiv^+$-equivalent to sequences in $\mathcal{S}^+$ such that k is the index of Λ in both of them. So for $e = 0, 1$ there exist sequences X_e, Y_e in $\widehat{\mathbb{S}}$ satisfying

$$(1) \qquad \begin{cases} X \bullet \Lambda_{(i)} \equiv^+ \Lambda_{(k)} \bullet 1X_1 \bullet 0X_0, \\ Y \bullet \Lambda_{(j)} \equiv^+ \Lambda_{(k)} \bullet 1Y_1 \bullet 0Y_0. \end{cases}$$

Claim 1. *If k is not 0, at least one of i, j is strictly smaller than k.*

Proof. Assume that i is equal to k. By construction, we must have

$$k-1+\mathrm{ind}(1^{k-1}, X) < k,$$

and therefore the index of 1^{k-1} in X is 0. Let i' be the least integer satisfying $i'+\mathrm{ind}(1^{i'}, X) = k-1$. For l smaller than i', $l+\mathrm{ind}(1^l, X)$ cannot be greater than k, since k is accessible to X, and cannot be $k-1$ by definition of i'. So $k-1$ must be accessible to X. Now if both i and j were equal to k, $k-1$ would be accessible to X and Y, contradicting the definition of k. □

Claim 2. *The terms $K_{X,Y}$ and $K_{X\bullet\Lambda_{(i)},Y\bullet\Lambda_{(j)}}$ coincide.*

Proof. The result is trivial if k is 0 since i and j are 0 as well. Assume $k \geq 1$. By Claim 1 we know that at least one of i or j is strictly below k. We assume $i < k$ in the sequel. This implies that the index of 1^i in X is not 0. Now observe that a term P belongs to the domain of $\Omega_{1^p{}_{(q)}}$ if and only if its right height, defined as the length of its rightmost branch when viewed as a binary tree, is at least $p+q+2$ and that the right height is invariant under any transformation Ω_ξ. So assume that P lies in the domain of Ω_X: because of the factor $1^i_{(k-i)}$ in the sequence X, the right height of P must be at least $i+(k-i)+2$, i.e., $k+2$. Therefore, the term P must lie in the domain of $\Omega_{\Lambda_{(k)}}$ and therefore, in the domain of $\Omega_{X\bullet\Lambda_{(i)}}$ and $\Omega_{Y\bullet\Lambda_{(j)}}$ since $i \leq k$ and $j \leq k$ hold. □

Claim 3. *For $e = 0, 1$, the size of K_{X_e,Y_e} is strictly less than the size of $K_{X,Y}$.*

Proof. Let P be the term $K_{X,Y}$. By Claim 2, P lies in the domain of $\Omega_{X\bullet\Lambda_{(i)}}$; then by (1) it lies in the domain of $\Omega_{\Lambda_{(k)}\bullet 1X_1\bullet 0X_0}$. Hence, if $Q_0[Q_1]$ is the image of P under $\Omega_{\Lambda_{(k)}}$, the term Q_e lies in the domain of X_e for $e = 0, 1$. Similarly Q_e lies in the domains of Y_e for $e = 0, 1$. So size of K_{X_e,Y_e} is at most the size of Q_e, and by construction the latter one is strictly below the size of P, i.e., of $K_{X,Y}$. □

We may therefore apply the induction hypothesis to the sequences X_e and Y_e for $e = 0$ and $e = 1$. We obtain

$$\begin{aligned}
X \bullet \Lambda_{(i)} \bullet 1\widehat{C}(Y_1, X_1) \bullet 0\widehat{C}(Y_0, X_0)& \\
&\equiv^+ \Lambda_{(k)} \bullet 1X_1 \bullet 0X_0 \bullet 1\widehat{C}(Y_1, X_1) \bullet 0\widehat{C}(Y_0, X_0)\\
&\equiv^+ \Lambda_{(k)} \bullet 1X_1 \bullet 1\widehat{C}(Y_1, X_1) \bullet 0X_0 \bullet 0\widehat{C}(Y_0, X_0)\\
&\equiv^+ \Lambda_{(k)} \bullet 1Y_1 \bullet 1\widehat{C}(X_1, Y_1) \bullet 0Y_0 \bullet 0\widehat{C}(X_0, Y_0)\\
&\equiv^+ \Lambda_{(k)} \bullet 1Y_1 \bullet 0Y_0 \bullet 1\widehat{C}(X_1, Y_1) \bullet 0\widehat{C}(X_0, Y_0)\\
&\equiv^+ Y \bullet \Lambda_{(j)} \bullet 1\widehat{C}(X_1, Y_1) \bullet 0\widehat{C}(Y_0, X_0).
\end{aligned}$$

If we define $\widehat{C}(Y, X)$ to be the sequence

$$\Lambda_{(i)} \bullet 1\widehat{C}(Y_1, X_1) \bullet 0\widehat{C}(Y_0, X_0),$$

the symmetry of the construction shows that $\widehat{C}(X, Y)$ is $\Lambda_{(j)} \bullet 1\widehat{C}(X_1, Y_1) \bullet 0\widehat{C}(Y_0, X_0)$, and the desired properties are satisfied. □

Corollary 4. *The monoid $\widetilde{B}_\infty^+$ is right regular: for any positive sequences X, Y in $\mathscr{S}^+$, there exist positive sequences X', Y' satisfying $X \bullet X' \equiv^+ Y \bullet Y'$.*

Let $\widehat{N}$ and $\widehat{D}$ be the numerator and denominator mappings associated with $\widehat{C}$-reduction (and any parsing convention about expressing any sequence as a product of sequences in $\widehat{\mathbb{S}}$ and of inverses of sequences in $\widehat{\mathbb{S}}$). Since $\widehat{C}$ is effective, the mappings $\widehat{N}$ and $\widehat{D}$ are effective as well, and by the preceding result they are everywhere defined on $\mathscr{S}$, and the equivalence

$$\xi \equiv^+ \widehat{N}(\xi) \bullet \overline{\widehat{D}(\xi)}$$

holds for any sequence ξ in $\mathscr{S}$.

This could suggest to use from now on the reduction associated with $\widehat{C}$. The problem is that beyond the existence result we also need some uniqueness property. Typically we would like to compare the numerators and denominators of $\equiv$-sequences with respect to the relation $\equiv^+$. This seems very uneasy in the case of $\widehat{C}$-reduction, while this will prove to be rather easy in the case of C-reduction. Since the transfer of properties from one complement to the other one is possible, we finally obtain optimal results.

Lemma 5. (i) *The pairs $(u \bullet C(v, u), v \bullet C(u, v))$ with u, v in $\mathbb{S}$ generate the congruence $\equiv^+$.*

(ii) *For any u, v, w in $\mathbb{S}$, the sequences*

$$C(C(u, v), C(w, v)) \quad \textit{and} \quad C(C(u, w), C(v, w))$$

exist and are $\equiv^+$-equivalent.

(iii) *For any positive sequence X, the lengths of the sequences X' satisfying $X' \equiv^+ X$ are bounded.*

Proof. Point (i) is trivial. Point (ii) is just a (long) verification by examination of all possible mutual positions of the points u, v, w in $\mathbb{S}$. For point (iii) we observe that if Ω_X maps the term P to the term Q, so does every operator $\Omega_{X'}$ with $X' \equiv^+ X$, and it follows that the length of X' is certainly bounded by the difference between the sizes of Q and P, since every elementary transformation Ω_w strictly increases the size of any term to which it is applied. □

Lemma 6. *For any positive sequences X, X', Y, Y' in $\mathscr{S}^+$ the following are equivalent.*

(i) *$X \bullet X' \equiv^+ Y \bullet Y'$ holds,*

(ii) *the sequences $C(X, Y)$ and $C(Y, X)$ exist, and for some Z in $\mathscr{S}^+$ the equivalences*

$$X' \equiv^+ C(Y, X) \bullet Z, \qquad Y' \equiv^+ C(X, Y) \bullet Z$$

are satisfied.

Proof. For X in $\mathscr{S}^+$ let us denote by $\nu(X)$ the supremum of the lengths of the sequences of X' satisfying $X' \equiv^+ X$ and let us write $X \equiv_1^+ Y$ if Y is equal to X or is obtained from X by replacing exactly one subsequence $u \bullet C(v, u)$ by the corresponding sequence $v \bullet C(u, v)$. For $p \leq \infty$ let $\equiv_p^+$ be the pth power of $\equiv_1^+$ and let $\mathscr{P}_{n,p}^k$ be the following statement:

"Assume $X \bullet X' \equiv_p^+ Y \bullet Y'$, $\nu(X \bullet X') \leq n$, $\nu(X) \leq k$ and $\nu(Y) \leq k$. Then $C(X, Y)$ and $C(Y, X)$ exist and some Z in $\mathscr{S}^+$ satisfies

$$X' \equiv^+ C(Y, X) \bullet Z \quad \text{and} \quad Y' \equiv^+ C(X, Y) \bullet Z."$$

The statement $\mathscr{P}^k_{n,p}$ if proved for any k, n, $p \leq \infty$ by a triple induction, first on p (using Lemma 5(ii)), then on n, and finally on k (more details appear in [11]). So $\mathscr{P}^{\infty}_{\infty,\infty}$ is true, which exactly means that point (ii) follows from point (i). The converse implication is obvious by definition of the complement mapping C. □

It follows that the monoid $\widetilde{B}^+_\infty$ admits left cancellation. Indeed for every positive sequence X the complement $C(X, X)$ exists and is obviously empty, so $X \bullet X' \equiv^+ X \bullet Y'$ implies $X' \equiv^+ Y'$.

By the previous lemma the existence of the complement $\widetilde{C}(X, Y)$ implies the existence of the complement $C(X, Y)$ for any positive sequences X, Y. So we have (use Lemma 1 for the remark about the operators)

Proposition 7 (Effective version of Property B, existence part). *The (effective) mappings N and D are defined everywhere on $\mathscr{S}$. For any sequence σ in $\mathscr{S}$, the equivalence*

$$\xi \equiv^+ N(\xi) \bullet \overline{D(\xi)}$$

holds, and moreover the operator Ω_ξ is included in the operator $\Omega_{N(\xi)\bullet\overline{D(\xi)}}$.

The advantage of coming back to C-reduction is that Lemma 6 gives an additional uniqueness result.

Definition. For X, Y, X', Y' in $\mathscr{S}^+$, $(X, Y) \equiv^{+(2)} (X', Y')$ stands for

$$(\exists Z, Z')(X \bullet Z \equiv^+ X' \bullet Z' \quad \text{and} \quad Y \bullet Z \equiv^+ Y' \bullet Z').$$

Proposition 8 (Effective version of Property B, uniqueness part). *For any sequences ξ, ξ' in $\mathscr{S}$, $\xi \equiv \xi'$ is equivalent to*

$$(N(\xi), D(\xi)) \equiv^{+(2)} (N(\xi'), D(\xi')).$$

Proof. Write $\xi \equiv' \xi'$ for $(N(\xi), D(\xi)) \equiv^{+(2)} (N(\xi'), D(\xi'))$. By right regularity of the monoid $\widetilde{B}^+_\infty$ the relation $\equiv^{+(2)}$ on $\mathscr{S}^+ \times \mathscr{S}^+$ is transitive and so is the relation $\equiv'$ on $\mathscr{S}$. So in order to prove that $\xi \equiv \xi'$ implies $\xi \equiv' \xi'$ it suffices to establish $\xi \equiv' \xi'$ for a particular family of pairs (ξ, ξ') which generate the equivalence $\equiv$. We choose the pairs $(\xi_1 \bullet \eta \bullet \xi_2, \xi_1 \bullet \eta' \bullet \xi_2)$, where (η, η') is either an LD-pair or a pair $(\overline{w} \bullet w, \varepsilon)$, two cases where the result is obvious, or a pair $(w \bullet \overline{w}, \varepsilon)$. In this case the result follows from the compatibility of the operation C with respect to the congruence $\equiv^+$, which in turn follows from Lemma 6. □

Definition. For P, Q in $\mathscr{T}_a$, $F(P, Q)$ and $G(P, Q)$ are the numerator and the denominator of $\varphi(P, Q)$.

(By construction $G(P, Q)$ is $F(Q, P)$.) The effective version of Property B yields

Fact B (effective version). *Let P, Q be two terms in $\mathscr{T}_a$ and n be any integer at least equal to* $\sup(h(P), h(Q))$.

(i) *The operators $\Omega_{F(P,Q)}$ and $\Omega_{G(P,Q)}$ respectively map $P[a^{[n]}]$ and $Q[a^{[n]}]$ to a common expansion.*

(ii) *If P and Q are LD-equivalent, then $(F(P, Q), G(P, Q)) \equiv^{+(2)} (0X', 0Y')$ holds for some positive sequences X' and Y'.*

According to the scheme of §1 we shall take the

Comparison algorithm. (Input: two terms P, Q in $\mathscr{T}_a$.)

Step B. Determine $F(P, Q)$ and $G(P, Q)$.

Example. Let again P be the term $a[a][a[a[a]]]$ and Q be the term $a[a[a][a[a]]]$. We had

$$\varphi(P, Q) = 1 \bullet \overline{\Lambda} \bullet \overline{1} \bullet \overline{11} \bullet \overline{\Lambda} \bullet 1 \bullet 11 \bullet 1 \bullet \overline{11} \bullet \Lambda,$$

and, as was computed above (Figure 1), we obtain

$$F(P, Q) = 1 \bullet 11 \bullet 01 \bullet 1 \bullet 0 \quad \text{and} \quad G(P, Q) = 11 \bullet 1 \bullet 0 \bullet 11 \bullet 01 \bullet 10 \bullet 00.$$

Remark. The projection to B_∞ of the elements of $\widehat{\mathbb{S}}$ gives canonical representatives for the positive braids with the property that no two strands may cross each other twice (a similar geometrical characterization of the sequences of $\mathscr{S}$ which are $\equiv$-equivalent to an element of $\widehat{\mathbb{S}}$ exists). When only the generators up to σ_{n-1} are used, such positive braids turn out to be exactly the $n!$ left divisors of Garside's universal word Δ_n (see [29] or [15]). Right regularity of the monoid $\widetilde{B}^+_\infty$, when projected, gives a new proof for the right regularity of the braid monoid B^+_∞. When the present proof is compared with Garside's original argument, the role of the words Δ_n is more or less played by the sequences $\widetilde{\Delta}_P$ in $\widetilde{\mathbb{S}}$ such that the operator $\Omega_{\widetilde{\Delta}_P}$ maps the term P to the term ∂P.

4. Effective version of Property C: The sign of $\widetilde{B}_\infty$

In order to complete the scheme proposed in §1 it remains to extract an effective version of Property C which deals with the behaviour of left subterms in term expansions. This will be very easy.

Definition. For X a positive sequence in $\mathscr{S}^+$ and p a nonnegative integer, the *dilatation* of p by X and the pth *trace* of X are the integer $\mathrm{Dil}(p, X)$ and the positive sequence $\mathrm{Tr}^p(X)$ inductively defined by the following rules:

$$\mathrm{Dil}(p, \varepsilon) = p, \quad \mathrm{Tr}^p(\varepsilon) = \varepsilon,$$

$$\mathrm{Dil}(p, w) = \begin{cases} p+1 & \text{if } w \text{ is } 0^i \text{ for some } i < p, \\ p & \text{otherwise}, \end{cases}$$

$$\mathrm{Tr}^p(w) = \begin{cases} v & \text{if } w = 0^p v, \\ \varepsilon & \text{if } 0^p \text{ is not a prefix of } w, \end{cases}$$

$$\mathrm{Dil}(p, X, \bullet v) = \mathrm{Dil}(\mathrm{Dil}(p, X), v), \quad \mathrm{Tr}^p(X \bullet v) = \mathrm{Tr}^p(X) \bullet \mathrm{Tr}^{\mathrm{Dil}(p, X)}(v).$$

An immediate induction shows that for every sequence X the successive values of $\mathrm{Dil}(p, X)$ make a strictly increasing sequence.

Proposition 1 (Effective version of Property C, existence part). *Assume that X is a positive sequence and that Ω_X maps P to Q. Assume moreover that the subterm $l^p(P)$ exists, or that $l^{\mathrm{Dil}(p, X)}(Q)$ exists, or that $\mathrm{Tr}^p(X)$ is nonempty. Then $\Omega_{\mathrm{Tr}^p(X)}$ maps $l^p(P)$ to $l^{\mathrm{Dil}(p, X)}(Q)$.*

Proof. Use induction on the length of X, and distinguish the various possible cases when X is just a point in $\mathbb{S}$. □

Using induction on the length of the positive sequence Y, one extends the product formula of the definition, obtaining for any X, Y in $\mathscr{S}^+$ the equalities

$$\mathrm{Dil}(p, X \bullet Y) = \mathrm{Dil}(\mathrm{Dil}(p, X), Y), \quad \mathrm{Tr}^p(X \bullet Y) = \mathrm{Tr}^p(X) \bullet \mathrm{Tr}^{\mathrm{Dil}(p, X)}(Y).$$

A similar induction shows that Tr^p is the pth iterate of Tr^1 (henceforth denoted by Tr) and that the following equalities hold:

$$\mathrm{Dil}(p + q, X) = \mathrm{Dil}(p, X) + \mathrm{Dil}(q, \mathrm{Tr}^p(X)), \quad \mathrm{Tr}^{p+q}(X) = \mathrm{Tr}^p(\mathrm{Tr}^q(X)).$$

The main result about dilatation and trace is the following compatibility with the congruence $\equiv^+$.

Lemma 2. *Assume that X, Y are positive sequences and $X \equiv^+ Y$ holds. Then*

$$\mathrm{Dil}(p, X) = \mathrm{Dil}(p, Y) \quad \textit{and} \quad \mathrm{Tr}^p(X) \equiv^+ \mathrm{Tr}^p(Y)$$

hold for every $p \geq 0$.

Proof. Using the product formulas above, it suffices to prove the result when (X, Y) is an LD-pair. One then reduces to the case where the greatest common prefix of the points in X and Y is Λ using the following rules:

$$\mathrm{Dil}(p, uZ) = \begin{cases} \mathrm{Dil}(p-k, Z) + k & \text{if } u \text{ is } 0^k \text{ with } k \geq p, \\ p & \text{otherwise;} \end{cases}$$

$$\mathrm{Tr}^p(uZ) = \begin{cases} \mathrm{Tr}^{p-k} Z & \text{if } u \text{ is } 0^k \text{ with } k \leq p, \\ vZ & \text{if } u \text{ is } 0^p v, \\ \varepsilon & \text{otherwise.} \end{cases}$$

A direct computation in the finitely many remaining cases completes the proof. □

Let us write from now on $\mathrm{dil}(X)$ for $\mathrm{Dil}(1, X)$.

Proposition 3 (Effective version of Property C, uniqueness part). *Assume that the positive sequences X, Y, X', Y' satisfy $(X, Y) \equiv^{+(2)} (X', Y')$. Then the integers*

$$\mathrm{dil}(X) - \mathrm{dil}(Y) \quad \textit{and} \quad \mathrm{dil}(X') - \mathrm{dil}(Y')$$

have the same sign $(> 0, < 0,$ *or* $= 0)$.

Proof. Assume $X \bullet Z \equiv^+ X' \bullet Z'$ and $Y \bullet Z \equiv^+ Y' \bullet Z'$. By Lemma 2 the integers $\mathrm{dil}(X \bullet Z)$ and $\mathrm{dil}(X' \bullet Z')$ are equal. Now $\mathrm{dil}(X \bullet Z)$ is $\mathrm{Dil}(\mathrm{dil}(X), Z)$, and one obtains

$$\mathrm{Dil}(\mathrm{dil}(X), Z) = \mathrm{Dil}(\mathrm{dil}(X'), Z'),$$
$$\mathrm{Dil}(\mathrm{dil}(Y), Z) = \mathrm{Dil}(\mathrm{dil}(Y'), Z').$$

Because the mappings $p \mapsto \mathrm{Dil}(p, Z)$ and $p \mapsto \mathrm{Dil}(p, Z')$ are strictly increasing, the order between $\mathrm{dil}(X)$ and $\mathrm{dil}(Y)$ has to be the same as the order between $\mathrm{dil}(X')$ and $\mathrm{dil}(Y')$. □

Definition. For P, Q in $\mathscr{T}_a$, $f(P, Q)$ is $\mathrm{dil}(F(P, Q))$ and $g(P, Q)$ is $\mathrm{dil}(G(P, Q))$.

(Again $g(P, Q)$ is equal to $f(Q, P)$.) By the effective version of Property C we have

Fact C (Effective version). *Let P, Q be two terms in $\mathcal{T}_a$.*

(i) *For some term R, the term $l^{f(P,Q)}(R)$ is an extension of P and the term $l^{g(P,Q)}(R)$ is an extension of Q (more precisely the operator $\Omega_{\mathrm{Tr}(F(P,Q))}$ maps P to $l^{f(P,Q)}(R)$ and the operator $\Omega_{\mathrm{Tr}(G(P,Q))}$ maps Q to $l^{g(P,Q)}(R)$).*

(ii) *If P and Q are LD-equivalent, then the integers $f(P, Q)$ and $g(P, Q)$ are equal.*

According to the scheme of §1 we take the

Comparison algorithm. (Input: two terms P, Q in $\mathcal{T}_a$.)

Step C. Compute the integers $f(P, Q)$ and $g(P, Q)$.

Example. Let P be the term $a[a][a[a[a]]]$ and Q be the term $a[a[a][a[a]]]$. We had

$$F(P, Q) = \Lambda \bullet 11 \bullet 01 \bullet 1 \bullet 0 \quad \text{and} \quad G(P, Q) = 11 \bullet 1 \bullet 0 \bullet 11 \bullet 01 \bullet 10 \bullet 00.$$

We find now

$$f(P, Q) = g(P, Q) = 1,$$

and we can verify that the operator $\Omega_{\mathrm{Tr}(F(P,Q))}$, which is $\Omega_{1\bullet\Lambda}$, and the operator $\Omega_{\mathrm{Tr}(G(P,Q))}$, which is $\Omega_{\Lambda\bullet1\bullet0}$, map respectively P and Q to a common extension $a[a][a[a]][a[a][a[a]]]$.

As we noted in the beginning the converse of implication (ii) in Fact C is obvious by construction. So finally we have obtained that the terms P and Q are LD-equivalent if and only if the integers $f(P, Q)$ and $g(P, Q)$ (i.e., $f(Q, P)$) are equal. Since the mappings χ, N, D, and dil are effective, so are the mappings f and g, and we have completed a proof of

Theorem 4. *The word problem for the relation $=_{\mathrm{LD}}$ in the case of one variable is decidable.*

Remark. Proposition 3 claims the existence of a well-defined *sign* for the elements of $\widetilde{B}_\infty$: if the sign of a sequence ξ in $\mathcal{S}$ is defined as the sign (> 0, > 0, or $= 0$) of the integer

$$\mathrm{dil}(N(\xi)) - \mathrm{dil}(D(\xi)),$$

then Proposition 3 together with Proposition 3.8 shows that $\equiv$-equivalent sequences have the same sign.

We finish this section with an evaluation of the algorithmic complexity of the comparison process defined above. We shall only sketch the proof.

Proposition 5. *Let* $\exp^*$ *be the iterated exponential function defined by* $\exp^*(0) = 1$ *and* $\exp^*(n+1) = 2^{\exp^*(n)}$. *Then the space complexity of the above comparison method for the terms P, Q is bounded by* $\exp^*(O(2^n))$ *where n is the sum of the sizes of P and Q.*

Proof. Let us say that a sequence ξ in $\mathcal{S}$ has *degree at most* n if it can be written as the product of n sequences which are elements of $\widehat{\mathbb{S}}$ or inverses of such elements. It is easy to show that the length, and therefore the degree, of the sequence $\varphi(P, Q)$ is bounded by 2^n where n is as above. Assume that X and Y are simple sequences, and the term P lies in the domain of the operator $\Omega_{\overline{Y}\bullet X}$. The term P lies in the domain of the operator $\Omega_{\widehat{C}(X,Y)}$, and because $\widehat{C}(X, Y)$ belongs to $\widehat{\mathbb{S}}$, the term ∂P is an extension of the image of P under

$\Omega_{\widehat{C}(X,Y)}$. It follows that the length of the sequence $\widehat{C}(X, Y)$ is bounded by the size of ∂P, which is itself bounded by 2^m where m is the size of P. By Lemma 3.6 the same bound holds for $C(X, Y)$. By iterating the process one shows that if ξ has degree n and the term P lies in the domain of Ω_ξ, then the lengths of the numerator and denominator of ξ are bounded by the size of the term $\partial^n P$ and, actually, that the whole computation of these sequences can be made inside this space bound. Determination of the sign does not require any additional space, thus one obtains the above bound for the whole process. □

Observe that the previous bound, even if too high for a really practical use, is very low in the hierarchy of fast-growing functions. The determination of the normal form of a term described in [10] has essentially the same complexity. On the other hand, it is not clear that the comparison process associated with Laver's normal forms in [24] or [25] is primitive recursive.

5. Free left distributive structures

Once the construction of §§2–4 is complete, it becomes very easy to deduce several previously conjectured properties for the free left distributive systems and the partial monoid $\mathscr{M}_{\mathrm{LD}}$. We begin with

Proposition 1. *The relation $\sqsubset_{\mathrm{LD}}$ is antireflexive on $\mathscr{T}_a$.*

Proof. We show that $P \sqsubset Q$ implies that the sequence $\varphi(P, Q)$ has positive sign: this implies that P and Q are not LD-equivalent since the effective version of Fact C claims that $\varphi(P, Q)$ has sign 0 if P and Q are LD-equivalent. So assume that Q is equal to $P[Q_1]\cdots[Q_k]$ for some $k \geq 1$. The explicit computation of the sequence $\varphi(P, Q)$ shows that it has the form

$$1\xi_0 \bullet \Lambda \bullet 1\xi_1 \bullet \cdots \bullet \Lambda \bullet 1\xi_k,$$

and we claim that any such sequence is strictly positive. Indeed let ξ be any sequence and w be a point of $\mathbb{S}$. Let X be $C(w, D(\xi))$ and Y be $C(D(\xi), w)$. Then $N(\xi \bullet w)$ is $N(\xi) \bullet X$ and $D(\xi \bullet w)$ is Y.

If w is not Λ, $\mathrm{dil}(w)$ is 1, and one obtains

$$\begin{aligned}\mathrm{dil}(D(\xi \bullet w)) &= \mathrm{Dil}(1, Y) = \mathrm{Dil}(\mathrm{dil}(w), Y) = \mathrm{dil}(w \bullet Y)\\ &= \mathrm{dil}(D)(\xi) \bullet X) = \mathrm{Dil}((\mathrm{dil}(D(\xi)), X)),\\ \mathrm{dil}(N(\xi \bullet w)) &= \mathrm{Dil}(\mathrm{dil}(N(\xi)), X),\end{aligned}$$

which show that $\xi \bullet w$ and ξ always have the same sign.

Now if w is Λ, the second formula remains true; but because $\mathrm{dil}(\Lambda)$ is 2, the first one becomes

$$\begin{aligned}\mathrm{dil}(D(\xi \bullet \Lambda)) &= \mathrm{Dil}(1, Y) < \mathrm{Dil}(2, Y) = \mathrm{Dil}(\mathrm{dil}(\Lambda), Y)\\ &= \mathrm{dil}(\Lambda \bullet Y) = \mathrm{dil}(D(\xi) \bullet X) = \mathrm{Dil}(\mathrm{dil}(D(\xi)), X)),\end{aligned}$$

and this shows that the sign of $\xi \bullet \Lambda$ is strictly positive whenever the sign of ξ is nonnegative. The claim follows: the sequence $1\xi_0$ has sign 0, hence $1\xi_0 \bullet \Lambda$ is strictly positive, and the subsequent products by sequences $1\xi_i$ or Λ will not modify the sign. □

The antireflexivity of the relation $\sqsubset_{\mathrm{LD}}$ gives several corollaries. In the sequel we denote by $\mathfrak{f}$ the free left distributive system with one generator, i.e., the structure $\mathscr{T}_a/ =_{\mathrm{LD}}$. By the results of [6] or [23] we have

Theorem 2. *The relation $\sqsubset_{\mathrm{LD}}$ induces a linear ordering $<$ on $\mathfrak{f}$ which is compatible with left translations and satisfies $x < x[y]$ for every x, y. In particular, $\mathfrak{f}$ admits left cancellation.*

It was shown in [5] that the existence of distinct LD-equivalent terms in $\mathcal{T}_\Sigma$ having the same projection on $\mathcal{T}_a$ (when every element of Σ is projected onto a) contradicts the antireflexivity of the relation $\sqsubset_{\mathrm{LD}}$. We deduce now

Theorem 3. *The word problem for the relation $=_{\mathrm{LD}}$ in the case of any number of variables is decidable.*

Proof. Let P, Q be arbitrary terms in $\mathcal{T}_\sigma$, and let P^τ, Q^τ be their projections onto $\mathcal{T}_a$. If P^τ and Q^τ are not LD-equivalent, clearly P and Q cannot be LD-equivalent. Let X be the sequence $\mathrm{Tr}(F(P^\tau, Q^\tau))$ and Y be the sequence $\mathrm{Tr}(G(P^\tau, Q^\tau))$. By Fact C, if P^τ and Q^τ are LD-equivalent, the operators Ω_X and Ω_Y map respectively P^τ and Q^τ to a common extension R. Let R_1 be the image of P under Ω_X and R_2 be the image of Q under Ω_Y. By construction the term R is both R_1^τ and R_2^τ. If R_1 and R_2 are equal, we may conclude at once that P and Q are LD-equivalent. Conversely if P and Q are LD-equivalent, so are R_1 and R_2. By the remark above this implies that R_1 and R_2 must be equal. □

The relation $\sqsubset_{\mathrm{LD}}$ is still antireflexive in the case of any number of variables because any counterexample in $\mathcal{T}_\Sigma$ would project to a counterexample in $\mathcal{T}_a$. It follows that any linear ordering on the variables generates, together with the projection of $\sqsubset_{\mathrm{LD}}$, a well-defined linear ordering on the free left distributive system generated by these variables (see [9] for details).

Among other properties, one also obtains that the normal forms for terms of $\mathcal{T}_a$ *modulo* LD-equivalence which are defined by Richard Laver in [24] and [25] under the assumption that the relation $\sqsubset_{\mathrm{LD}}$ is antireflexive (and therefore under the strong set-theoretical assumption) always exist. Similarly [10] introduces a new normal form, and the antireflexivity of $\sqsubset_{\mathrm{LD}}$ directly corresponds to the uniqueness of this form. Finally one also obtains the correctness of the conjectural comparison algorithm presented in [7] (but the termination problem remains open).

From the point of view of the description of the free left distributive systems, we can now answer two natural questions, namely, the one of giving a precise description of the connection between the structural monoid $\mathcal{M}_{\mathrm{LD}}$ and the group $\widetilde{B}_\infty$ and the one of defining a realization of the structure $\mathfrak{f}$ by embedding it into some "usual" structure. The following result shows the correctness of the intuition that the LD-pairs generate all left-distributivity identities.

Theorem 4. (i) *The compatibility relation on $\mathcal{M}_{\mathrm{LD}}$ is a congruence; if Ω_ξ and Ω_η are nonempty, they are compatible if and only if they are strongly compatible if and only if $\xi \equiv \eta$ holds.*

(ii) *The quotient structure of $\mathcal{M}_{\mathrm{LD}}$ under compatibility is isomorphic to the subset of the group $\widetilde{B}_\infty$ made by the elements $x^{-1}y$ where x and y are images of sequences of the form $\xi_0 \bullet 1\xi_1 \bullet 11\xi_2 \bullet \cdots \bullet 1^n\xi_n$ with $\xi_0, \dots, \xi_n$ in the image of χ.*

Proof. Assume that Ω_ξ and Ω_η both map the term P (in $\mathcal{T}_a$) to the term Q. By Proposition 2.5 we have

$$0\xi \equiv \overline{\chi(P)} \bullet \chi(Q) \equiv 0\eta.$$

By Proposition 3.8 we deduce

$$(N(0\xi), D(0\xi)) \equiv^{+(2)} (N(0\eta), D(0\eta)),$$

hence

$$(0N(\xi), 0D(\xi)) \equiv^{+(2)} (0N(\eta), 0D(\eta)).$$

So there exist positive sequences Z, Z' satisfying

$$0N(\xi) \bullet Z \equiv^{+} 0N(\eta) \bullet Z' \quad \text{and} \quad 0D(\xi) \bullet Z \equiv^{+} 0D(\eta) \bullet Z'.$$

By applying the trace operation Tr defined in §4 we deduce

$$N(\xi) \bullet \mathrm{Tr}(Z) \equiv^{+} N(\eta) \bullet \mathrm{Tr}(Z') \quad \text{and} \quad D(\xi) \bullet \mathrm{Tr}(Z) \equiv^{+} D(\eta) \bullet \mathrm{Tr}(Z')$$

because $\mathrm{Tr}(0X)$ is always X. This shows $(N(\xi), D(\xi)) \equiv^{+(2)} (N(\eta), D(\eta))$, and therefore $\xi \equiv \eta$.

Point (ii) follows from the fact that if the operator Ω_ζ maps the term $P_1[P_2[\cdots[P_h]\cdots]]$ to the term $Q_1[Q_2[\cdots[Q_h]\cdots]]$, so does the operator $\Omega_{\overline{\xi}\bullet\eta}$, where ξ is $\prod_1^h 1^{k-1}\chi(P_k)$ and η is $\prod_1^h 1^{k-1}\chi(Q_k)$. □

Remark. Define an LD-category to be a category equipped with a bifunctor which is left distributive up to natural isomorphisms. Then the above presentation of $\mathscr{M}_{\mathrm{LD}}$ modulo compatibility gives a full solution to the coherence problem associated with LD-categories. The analogue of Mac Lanes's pentagon in the case of associativity [27] is here the heptagon associated with the first LD-pair.

As a corollary to the latter theorem we have

Propostion 5. *The relation $\equiv$ on $\mathscr{S}$ (i.e., the word problem for the group $\widetilde{B}_\infty$ as presented above) is decidable.*

Proof. For any sequence ξ in $\mathscr{S}$, $\xi \equiv \varepsilon$ holds if and only if $N(\xi) \equiv D(\xi)$ holds and therefore, if and only if the operators $\Omega_{N(\xi)}$ and $\Omega_{D(\xi)}$ (which cannot be empty since $N(\xi)$ and $D(\xi)$ are positive sequences) agree on the intersection of their domains. This can be decided by finding a term P which belongs to both domains and comparing its images. Because the construction of the canonical term K_X for X a positive sequence is effective, the whole process is effective and even is primitive recursive. □

Using the group $\widetilde{B}_\infty$ we now describe a realization of the free left distributive system $\mathfrak{f}$. Observe that since $\widetilde{B}_\infty$ represents to some extent the left distributivity identities, we thus construct a model of left distributivity whose elements are left distributivity identities themselves, a situation which is reminiscent of the proof of Gödel's completeness theorem for first-order logic by means of Henkin's constants. We recall Laver's criterion for freeness.

Lemma 6 [24]. *If $\mathfrak{g}$ is an antireflexive LD-system, then every substructure of $\mathfrak{g}$ with one generator is free.*

Proof. Let π be the projection of $\mathscr{T}_a$ onto a singly generated substructure $\mathfrak{g}'$ of $\mathfrak{g}$. The antireflexivity of $\mathfrak{g}$ implies that the projection of the relation $\sqsubset_{\mathrm{LD}}$

on $\mathfrak{g}'$ is a strict order $<$. If P, Q are LD-inequivalent terms, either $P \sqsubset_{\mathrm{LD}} Q$ or $Q \sqsubset_{\mathrm{LD}} P$ holds, which implies $\pi(P) < \pi(Q)$ or $\pi(Q) < \pi(P)$, and in both cases $\pi(P) \neq \pi(Q)$. □

Theorem 7. *Let H_0 be the subgroup of $\widetilde{B}_\infty$ generated by the images of the length 1 sequences $0w$. The bracket on $\mathscr{S}$ induces a well-defined left distributive operation on the right cosets set $\widetilde{B}_\infty/H_0$. Moreover, the closure of any element of $\widetilde{B}_\infty/H_0$ under this bracket is a free left distributive system.*

Proof. The compatibility of bracket with the congruence $\equiv$, i.e., with the projection of $\mathscr{S}$ onto $\widetilde{B}_\infty$, is obvious. Then the compatibility with the right equivalence relation associated with H_0 follows from formula (2) in the proof of Proposition 2.5. Formula (1) of the same proof shows that collapsing H_0 is exactly what is needed to drop the obstruction to left distributivity. By Laver's criterion it suffices to show that the left distributive structure $\widetilde{B}_\infty/H_0$ is antireflexive. The point is to show that the images of two terms P and $P[Q_1]\cdots[Q_k]$ in $\widetilde{B}_\infty$ cannot be equivalent modulo H_0. By construction these images are the projections of the sequences $\chi(P)$ and $\chi(P[Q_1]\cdots[Q_k])$, and we have to show that the quotient $\overline{\chi(P)}\chi(P[Q_1]\cdots[Q_k])$ cannot belong to H_0. But we just have seen above in the proof of Proposition 1 that the elements of H_0 have sign 0, while any sequence as above is strictly positive. □

6. Braid colourings

In this section we project the previous constructions involving the group $\widetilde{B}_\infty$ to similar constructions involving the braid group B_∞ (which is a quotient of the group $\widetilde{B}_\infty$). The main technical tool is the use of the elements of the free left distributive structure $\mathfrak{f}$ for colouring the strings in braids. We obtain a new comparison algorithm for deciding LD-equivalence of terms and a realization of the free left distributive structure $\mathfrak{f}$ inside the braid group B_∞.

The existence of an action of the braids on left distributive structures is well known: see for instance [2]. This action can be considered here as the projection to B_∞ of an action of $\widetilde{B}_\infty$ associated with the operators Ω_ξ.

Notation for braids will be similar to those used for $\widetilde{B}_\infty$: the elements of B_∞ are represented by *braid words* which are treated as finite sequences of factors of the form i or $\bar{i}$ with i a positive integer. The free monoid of all such braid words is denoted by $\mathscr{W}$, while the submonoid of all positive braid words (the ones involving no factor $\bar{i}$) is denoted by $\mathscr{W}^+$. We write $\equiv^+$ for the congruence on $\mathscr{W}^+$ generated by all pairs $(i \bullet j, j \bullet i)$ with $|i-j| \geq 2$ and all pairs $(i \bullet i+1 \bullet i, i+1 \bullet i \bullet i+1)$, and $\equiv$ for the congruence on $\mathscr{W}$ generated by $\equiv^+$ and the pairs $(i \bullet \bar{i}, \varepsilon)$, $(\bar{i} \bullet i, \varepsilon)$. Then the group B_∞ is $\mathscr{W}/\equiv$. The monoid $\mathscr{W}^+/\equiv^+$ is denoted by B_∞^+. One knows [17] that $\equiv^+$ is the restriction of $\equiv$ to $\mathscr{W}^+$, and therefore B_∞^+ may be identified with a submonoid of B_∞. The projection of $\mathscr{W}$ onto B_∞ is denoted σ, so $\sigma(i)$ is exactly the braid σ_i.

Let us assume first that $\mathfrak{g}$ is any set endowed with a bracket. For i a positive integer, let $\Theta_{\mathfrak{g}}^i$ be the operator defined on the set $\mathfrak{g}^{\mathbb{N}}$ of all infinite sequences from $\mathfrak{g}$ by

$$\Theta_{\mathfrak{g}}^i : \langle x_1, x_2, \ldots \rangle \mapsto \langle x_1, x_2, \ldots, x_i[x_{i+1}], x_i, x_{i+2}, \ldots \rangle.$$

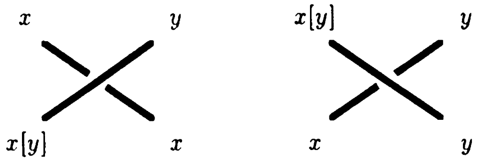
We extend this definition to positive braid words for obtaining an action on the right; i.e., we require that for A, B in $\mathscr{W}^+$, $\Theta_{\mathfrak{g}}^{A\bullet B}$ be the composition of $\Theta_{\mathfrak{g}}^{B}$ and $\Theta_{\mathfrak{g}}^{A}$. Now a simple verification shows that the congruence $\equiv^+$ is compatible with this action if (and only if) the bracket on $\mathfrak{g}$ is left distributive. In this case we obtain a well-defined action of B_∞^+ on $\mathfrak{g}^{\mathbb{N}}$.

The natural hypothesis for extending this action to B_∞ is to assume that the left translations in $\mathfrak{g}$ are bijective, so that $\mathfrak{g}$ is an *automorphic set* (in [2]), a *rack* (in [16]), or, in a different formulation, a *crystal* (in [18]). Actually, if we only assume that left translations in $\mathfrak{g}$ are injective, i.e., that $\mathfrak{g}$ is a left cancellative LD-system, we obtain a partial but well-defined action of arbitrary sequences by

$$\Theta_{\mathfrak{g}}^{\bar{i}} : \langle x_1 , x_2 , \dots \rangle \mapsto \langle x_1 , x_2 , \dots , x_{i+1} , z , x_{i+2} , \dots \rangle$$

where z is the unique element of $\mathfrak{g}$ satisfying $x_{i+1}[z] = x_i$ if such an element exists.

The geometrical meaning of the action $\Theta^{\mathfrak{g}}$ is clear: we colour the strings of the braids using elements of $\mathfrak{g}$, and the colours change at each crossing according to the following rules.



Definition. The sequences in $\mathfrak{g}^{\mathbb{N}}$ are called $\mathfrak{g}$-*colourings*, and a $\mathfrak{g}$-colouring $\vec{x}$ is *permitted* for the braid word α if $\vec{x}$ belongs to the domain of the operator $\Theta_{\mathfrak{g}}^{\alpha}$. The image of $\vec{x}$ under $\Theta_{\mathfrak{g}}^{\alpha}$ is then denoted by $\vec{x}^{\alpha}$.

If the LD-system $\mathfrak{g}$ is not a rack, the action $\Theta_{\mathfrak{g}}$ is only a partial action, which means that it can be impossible to propagate along a given braid a given initial choice of $\mathfrak{g}$-colours for the strings. But the main technical point is that there always exists for a given braid a convenient choice of initial $\mathfrak{g}$-colours which can be propagated throughout the braid.

Let us first observe that the tools used in §3 for sequences in $\mathscr{S}$ project to braid words. In particular, the complement mapping C on $\mathscr{S}^+$ immediately projects to a similar complement mapping C_R on positive braid words. This complement gives rise to a reduction of braid words, and all results available for reduction in $\mathscr{S}$ project without modification. In particular, we obtain two mappings N_R, D_R of $\mathscr{W}$ to $\mathscr{W}^+$ such that every braid word α reduces (with respect to C_R) to the $\equiv$-equivalent braid word $N_R(\alpha)\bullet\overline{D_R(\alpha)}$ (see [11] for more details).

But we also observe that the braid relations are symmetric (in contradistinction with the relations used on $\mathscr{S}$). Therefore we can also define a *left complement* for braid words and, using the symmetric notion of a left reduction, show the existence of two mappings N_L, D_L of $\mathscr{W}$ to $\mathscr{W}^+$ such that every braid word α, using left reduction, gives an $\equiv$-equivalent braid word $\overline{D_L(\alpha)} \bullet N_L(\alpha)$.

Lemma 1. *Assume that* $\mathfrak{g}$ *is a left-cancellative LD-system.*

(i) *For every finite family of braid words* $\alpha_1, \dots, \alpha_p$, *there exists a* $\mathfrak{g}$*-colouring which is permitted for* $\alpha_1, \dots, \alpha_p$.

(ii) *If* α *and* α' *are* $\equiv$*-equivalent, then* $\vec{x}^{\alpha} = \vec{x}^{\alpha'}$ *holds for every* $\mathfrak{g}$*-colouring* $\vec{x}$ *which is both* α*- and* α'*-permitted.*

Proof. (i) If A, B are positive words, then $\Theta_{\mathfrak{g}}^{A}$ and $\Theta_{\mathfrak{g}}^{B}$ are defined everywhere on $\mathfrak{g}^{\mathbb{N}}$. By construction the domain of $\Theta_{\mathfrak{g}}^{\overline{A}}$ includes the image of $\Theta_{\mathfrak{g}}^{A}$ and so does the domain of $\Theta_{\mathfrak{g}}^{\overline{A}\bullet B}$ since by construction $(\vec{x}^{A})^{\overline{A}}$ is $\vec{x}$.

Claim. *If* α *is left reducible to* β, *then* $\Theta_{\mathfrak{g}}^{\alpha}$ *includes* $\Theta_{\mathfrak{g}}^{\beta}$ (*as a set of pairs*).

Proof. We may assume that α is left reducible to β in one step and even that α is $i\bullet\overline{j}$ for some nonnegative integers i, j. The critical case is for $|i-j| = 1$. Assume, for example, $\alpha = 1\bullet\overline{2}$, so that β is $\overline{2}\bullet\overline{1}\bullet 2\bullet 1$. The hypothesis that $\langle x_1, x_2, \dots\rangle$ is permitted for $\overline{2}\bullet\overline{1}$ implies that there exist z_1 and z_2 in $\mathfrak{g}$ satisfying $x_2 = x_3[z_2]$ and $x_1 = x_3[z_1]$. It follows that $\langle x_1[x_2], x_1, x_3, \dots\rangle$ is permitted for $\overline{2}$, and one has

$$\begin{aligned}\langle x_1, x_2, x_3, x_4, \dots\rangle^{1\bullet\overline{2}} &= \langle x_1[x_2], x_3, z_1, x_4, \dots\rangle\\ &= \langle x_1, x_2, x_3, x_4, \dots\rangle^{\overline{2}\bullet\overline{1}\bullet 2\bullet 1},\end{aligned}$$

which proves the claim. □

We deduce that $\Theta_{\mathfrak{g}}^{\alpha}$ includes $\Theta_{\mathfrak{g}}^{\overline{D_L(\alpha)}\bullet N_L(\alpha)}$ and therefore, that the domain of $\Theta_{\mathfrak{g}}^{\alpha}$ includes the image of $\Theta_{\mathfrak{g}}^{D_L(\alpha)}$. So the result is proved in the case of one braid word.

For the extension to several words $\alpha_1, \dots, \alpha_p$, we just have to verify that the images of $\Theta_{\mathfrak{g}}^{D_L(\alpha_1)}, \dots, \Theta_{\mathfrak{g}}^{D_L(\alpha_p)}$ cannot be disjoint. But the intersection of these images includes the image of $\Theta_{\mathfrak{g}}^{A}$, where A is the left least common multiple of $D_L(\alpha_1), \dots, D_L(\alpha_p)$, which exists by left regularity of the monoid B_∞^+.

(ii) A similar argument shows that if α is right-reducible to β, then $\Theta_{\mathfrak{g}}^{\alpha}$ is included in $\Theta_{\mathfrak{g}}^{\beta}$. Now assume that α and α' are $\equiv$-equivalent and $\vec{x}$ is permitted for α and α'. By (the projection to B_∞ of) Proposition 3.8 there must exist positive braid words C, C' satisfying

$$\begin{cases} N_R(\alpha)\bullet C \equiv^+ N_R(\alpha')\bullet C', \\ D_R(\alpha)\bullet C \equiv^+ D_R(\alpha')\bullet C'. \end{cases}$$

Now $\vec{x}$ is permitted for α, hence for $N_R(\alpha)\bullet\overline{D_R(\alpha)}$, and for $N_R(\alpha)\bullet C\bullet\overline{C}\bullet\overline{D_R(\alpha)}$ as well. We then obtain

$$\begin{aligned}\vec{x}^{\alpha} &= \vec{x}^{N_R(\alpha)\bullet\overline{D_R(\alpha)}} = \vec{x}^{N_R(\alpha)\bullet C\bullet\overline{C}\bullet D_R(\alpha)} = (\vec{x}^{N_R(\alpha)\bullet C})^{\overline{D_R(\alpha)\bullet C}}\\ &= (\vec{x}^{N_R(\alpha')\bullet C'})^{\overline{D_R(\alpha')\bullet C'}} = \vec{x}^{N_R(\alpha')\bullet\overline{D_R(\alpha')}} = \vec{x}^{\alpha'}.\end{aligned}$$

Observe that the previous argument is needed because if one uses an arbitrary sequence of words witnessing for the equivalence of α and α', one cannot assume that $\vec{x}$ is permitted for the intermediate terms. □

Thus the image of a $\mathfrak{g}$-colouring under a braid is well defined when it exists. The Burau representation and therefore the Alexander polynomial of a braid can be constructed using the colourings associated with the bracket defined by

$$x[y] = (1-t)x + ty,$$

while the Wirtinger presentation for the fundamental group of the complement of the closure of the braid is associated with the conjugacy bracket in a free group.

By the results of §5 the free LD-systems, and in particular the structure $\mathfrak{f}$, are left cancellative. We can therefore consider colourings of braids by elements of $\mathfrak{f}$. The existence of the linear ordering $<$ on $\mathfrak{f}$ will give a powerful criterion for separating braids.

Definition. A braid is *σ_i-positive* if it has a decomposition (with respect to the generators σ_k) where σ_i occurs but σ_i^{-1} does not.

Proposition 2. *The generator σ_i occurs in every decomposition of a σ_i-positive braid; in particular, a σ_i-positive braid cannot be trivial.*

Proof. Assume that α is a braid word where $\bar{\imath}$ does not occur. Let $\langle x_1^0, x_2^0, \dots\rangle$ be any α-permitted $\mathfrak{f}$-colouring. Consider the sequences $\langle x_1^p, x_2^p, \dots, \rangle$ inductively defined by

$$\langle x_1^{p+1}, x_2^{p+1}, \dots\rangle = \langle x_1^p, x_2^p, \dots\rangle^{e_{p+1}},$$

where $e_1, \dots, e_n$ are the successive factors of α (of the form k or $\bar{k}$), i.e., follow the successive transformations of the colours. Let $\dot{a}$ denote the class of a in $\mathfrak{f}$. By left distributivity one has

$$x_1^{p+1}[\cdots[x_i^{p+1}[\dot{a}]]\cdots] = \begin{cases} x_1^p[\cdots[x_i^p[\dot{a}]]\cdots] & \text{if } e_p \neq i, \bar{\imath}, \\ x_1^p[\cdots[x_i^p[x_{i+1}^p][\dot{a}]]\cdots] & \text{if } e_p = i. \end{cases}$$

For any $x_1, \dots, x_{i+1}$ in $\mathfrak{f}$, one has

$$x_i <_{\mathfrak{f}} x_i[x_{i+1}]$$

by definition of the ordering $<_{\mathfrak{f}}$, which implies

$$x_i[\dot{a}] <_{\mathfrak{f}} x_i[x_{i+1}][\dot{a}]$$

because $x[\dot{a}]$ is easily proved to be an immediate successor of x for $<_{\mathfrak{f}}$ and

$$x_1[\cdots[x_i[\dot{a}]]\cdots] <_{\mathfrak{f}} x_1[\cdots[x_i[x_{i+1}][\dot{a}]]\cdots]$$

because $<_{\mathfrak{f}}$ is compatible with bracket on the left. So the sequence of all $x_1^p[\cdots[x_i^p[\dot{a}]]\cdots]$ is nondecreasing, and if i occurs at least once in α, we have

$$x_1^0[x_2^0[\cdots[x_i^0[\dot{a}]]\cdots]] <_{\mathfrak{f}} x_1^n[x_2^n[\cdots[x_i^n[\dot{a}]]\cdots]].$$

By Lemma 1, $\alpha \equiv \varepsilon$ would imply $x_k^0 = x_k^n$ for every k, and therefore

$$x_1^0[x_2^0[\cdots[x_i^0[\dot{a}]]\cdots]] = x_1^n[x_2^n[\cdots[x_i^n[\dot{a}]]\cdots]].$$

Hence $\alpha \equiv \varepsilon$ cannot hold if i occurs in α but $\bar{\imath}$ does not. □

The closure of a σ_i-positive braid is a link diagram K with the property that some closed curve intersects K only at positive crossings. Since no conjugate of a σ_i-positive braid may be trivial, we may state that any link diagram with the above property cannot be regularly isotopic to the unknot. (The corresponding property for ambient isotopy is trivially false: take the closure of σ_i.)

Because the group B_∞ is the quotient of $\widetilde{B}_\infty$ under the normal subgroup generated by the subgroup H_0 and the explicit definition of the bracket on $\mathscr{S}$ is compatible with the projection onto B_∞, one obtains a well-defined left distributive bracket. A simple translation of the definition yields

Lemma 3. *Let s be the shift endomorphism of the group B_∞ which for every i maps σ_i to σ_{i+1}. Then the bracket on B_∞ defined by*

$$x[y] = x \bullet s(y) \bullet \sigma_1 \bullet s(x)^{-1}$$

is left distributive.

A direct verification of left distributivity, however, is straightforward, but guessing the definition without the approach of §1 seems difficult. By Proposition 2 we easily obtain

Theorem 4. *The bracket on B_∞ is antireflexive, and therefore the closure of any braid under bracket is a free left distributive system.*

Proof. An immediate computation (which is parallel to the one in the proof of Proposition 5.1) shows that for any $x, y_1, \ldots, y_k$ in B_∞ the braid

$$x^{-1}(x[y_1]\cdots[y_k])$$

is σ_1-positive, and therefore it cannot be trivial. Then apply Lemma 5.6. □

We may identify from now on the structure $\mathfrak{f}$ with the closure of the trivial braid 1 in B_∞. With this convention the class $\dot{a}$ of a in $\mathfrak{f}$ is identified with the braid 1.

Definition. The mapping χ' of $\mathscr{T}_a$ into $\mathscr{W}$ is inductively defined by

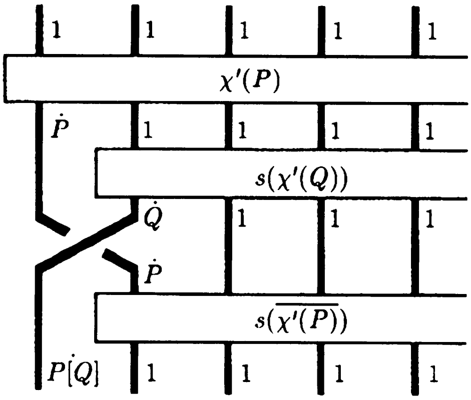
$$\chi'(P) = \begin{cases} \varepsilon & \text{if } P \text{ is } a, \\ \chi'(Q) \bullet s(\chi'(R)) \bullet 1 \bullet \overline{s(\chi'(Q))} & \text{if } P \text{ is } Q[R] \end{cases}$$

where s is the morphism of $\mathscr{W}$ such that $s(i)$ is $i+1$ and $s(\bar{i})$ is $\overline{i+1}$.

Lemma 5. *For any P in $\mathscr{T}_a$, the braid $\sigma(\chi'(P))$ is the class of P in $\mathfrak{f}$, the $\mathfrak{f}$-colouring $\langle 1, 1, 1, \ldots\rangle$ is permitted for braid $\sigma(\chi'(P))$, and one has*

$$\langle 1, 1, 1 \ldots, \rangle^{\chi'(P)} = \langle \dot{P}, 1, 1, \ldots\rangle.$$

The proof is immediate from the inductive definition of $\chi'(P)$ and is illustrated in the figure. Observe that the braid word $\chi'(P)$ is nothing but an exact transcription of the sequence $\chi(P)$ since by construction all factors in $\chi(P)$ have the form 1^i.



By Theorem 6.4 we have a new comparison algorithm for deciding LD-equivalence:

Proposition 6. *Two terms P, Q in $\mathcal{T}_a$ are LD-equivalent if and only if the braid words $\chi'(P)$ and $\chi'(Q)$ are $\equiv$-equivalent.*

Example. As in the first sections let P be the term $a[a][a[a[a]]]$ and Q be the term $a[a[a][a[a]]]$. The braids words $\chi'(P)$ and $\chi'(Q)$ are respectively

$$1 \bullet 3 \bullet 2 \bullet 1 \bullet \overline{2} \quad \text{and} \quad 2 \bullet 3 \bullet 2 \bullet \overline{3} \bullet 1,$$

which are $\equiv$-equivalent.

This new comparison process is more efficient than that described in §5 and we lower the complexity bound for $=_{\mathrm{LD}}$ down to

Theorem 7. *The word problem for the relation $=_{\mathrm{LD}}$ in the case of one variable has at most an exponential complexity.*

Proof. The length of the sequence $\chi'(P)$ is bounded by an exponential with respect to the size of P since the inductive definition gives

$$\operatorname{length}(\chi'(Q[R])) = 2.\operatorname{length}(\chi'(Q)) + \operatorname{length}(\chi'(R)) + 1.$$

The braid words comparison has a polynomial complexity, so the algorithm of Proposition 6 has an exponential complexity. □

Remarks. 1. The quotients of B_∞ inherit the left distributive structure whenever the projection is compatible with the shift endomorphism. When projecting onto the permutations of the integers, the quotient bracket happens to be isomorphic to the bracket on the injections of the positive integers constructed in [4]. It is known that the corresponding monogenic LD-systems $\mathfrak{d}$ are not free. Extension to the case of Hecke algebras could give rise to new examples. When collapsing as far as the integers using the exponent sum, the associated bracket is the 'trivial' bracket on $\mathbb{Z}$ defined by $a[b] = b + 1$.

2. The property of braids stated as Proposition 6.2 is a topological counterpart to the antireflexivity of the relation $\sqsubset_{\mathrm{LD}}$. Indeed it implies the above construction of an antireflexive LD-system and therefore, the antireflexivity of $\mathfrak{f}$ itself. In the present paper the property is deduced from the previously established antireflexivity of $\sqsubset_{\mathrm{LD}}$ (observe that the proof of Proposition 6.2 is especially easy if one restricts to the case of σ_1-positive braids). But conversely a direct argument for Proposition 6.2 shows the existence of an antireflexive LD-system and therefore can replace the study of the group $\widetilde{B}_\infty$ for proving the antireflexivity of $\sqsubset_{\mathrm{LD}}$. David Larue in [22] has obtained such a direct proof using a free group endowed with conjugacy to colour the strings in a braid.

7. A linear ordering on the braid groups

In the previous section we have used the braid colourings to define inside the braid group B_∞ a realization of the free LD-system $\mathfrak{f}$. We shall now use these colourings to transfer order properties from $\mathfrak{f}$ to B_∞. What makes such a transfer possible is the fact that, because $\mathfrak{f}$ is the most general left distributive structure, any $\mathfrak{f}$-colouring of a braid word completely captures the underlying braid—a property which could not hold with other colourings.

In Theorem 6.4 we have realized the elements of the free LD-system $\mathfrak{f}$ as braids. We turn now to the converse direction and investigate the representation of any braid in terms of the elements of $\mathfrak{f}$.

Definition. A $\mathfrak{f}$-colouring is *finite* if it has only finitely many components not equal to 1. The constant $\mathfrak{f}$-colouring $\langle 1, 1, \dots \rangle$ is denoted by $\vec{1}$. For $\langle a_1, a_2, \dots \rangle$ a finite $\mathfrak{f}$-colouring, one sets

$$\Pi(\langle a_1, a_2, \dots \rangle) = \prod_{k=1}^{\infty} s^{k-1}(a_k)$$

(where s is the shift endomorphism).

Lemma 1. (i) *For every finite $\mathfrak{f}$-colouring $\vec{x}$, there exists a braid word α satisfying*

$$\sigma(\alpha) = \Pi(\vec{x}) \quad \textit{and} \quad \vec{1}^{\alpha} = \vec{x}.$$

(ii) *The equality*

$$\Pi(\vec{x}^{\alpha}) = \Pi(\vec{x}) \cdot \sigma(\alpha)$$

holds for every braid word α and every α-permitted finite $\mathfrak{f}$-colouring $\vec{x}$.

Proof. (i) Assume that $\vec{x}$ is $\langle \dot{P}_1, \dot{P}_2, \dots \rangle$, where $\dot{P}$ denotes the class of the term P in $\mathfrak{f}$. By Lemma 6.5 the colouring $\vec{1}$ is permitted for $\chi'(P_k)$ and $\vec{1}^{\chi'(P_k)}$ is $\langle \dot{P}_k, 1, 1 \dots \rangle$. So we successively obtain

$$\vec{1}^{\chi'(P_1)} = \langle \dot{P}_1, 1, 1, \dots \rangle,$$
$$\vec{1}^{\chi'(P_1) \bullet s(\chi'(P_2))} = \langle \dot{P}_1, \dot{P}_2, 1, \dots \rangle,$$
$$\dots$$

and the formula with $\alpha = \prod_k s^{k-1}(\chi'(P_k))$ follows using an easy induction.

(ii) It suffices to prove the equality in the case of a single factor, say i. We have

$$\begin{aligned} \Pi(\langle x_1, x_2, \dots \rangle^i) &= \Pi(\langle x_1, x_2, \dots, x_i[x_{i+1}], x_i, x_{i+2}, \dots \rangle) \\ &= x_1 \cdot s(x_2) \cdots s^{i-1}(x_i[x_{i+1}] \cdot s^i(x_i) \cdot s^{i+1}(x_{i+2}) \cdots \\ &= x_1 \cdot s(x_2) \cdots s^{i-1}(x_i) \cdot s^i(x_{i+1}) \cdot \sigma_i \cdot s^i(\overline{x_i}) \cdot s^i(x_i) \cdot s^{i+1}(x_{i+2}) \cdots \\ &= x_1 \cdot s(x_2) \cdots s^{i-1}(x_i) \cdot s^i(x_{i+1}) \cdot \sigma_i \cdot^{i+1} (x_{i+2}) \cdots \\ &= \Pi(\langle x_1, x_2, \dots \rangle) \cdot \sigma_i, \end{aligned}$$

because the factor σ_i commutes with all $s^{k-1}(c_k)$ for $k \geq i + 2$. □

We deduce that the action $\Theta_{\mathfrak{f}}$ is strongly faithful in the following sense:

Proposition 2. *For any two braid words α, β, the following are equivalent:*

(i) *there exists a finite $\mathfrak{f}$-colouring $\vec{x}$ such that $\vec{x}^{\alpha}$ and $\vec{x}^{\beta}$ exist and are equal;*

(ii) *for every $\mathfrak{f}$-colouring $\vec{x}$ which is α- and β-permitted the values $\vec{x}^{\alpha}$ and $\vec{x}^{\beta}$ are equal;*

(iii) *$\alpha \equiv \beta$ holds.*

Proof. Owing to Lemma 6.1 we have only to show that (i) implies (iii). Now by Lemma 1(ii), when (i) is satisfied, we obtain

$$\sigma(\alpha) = \Pi(\vec{x})^{-1}\Pi(\vec{x}^{\alpha}) = \Pi(\vec{x})^{-1}\Pi(\vec{x}^{\beta}) = \sigma(\beta). \quad \square$$

We can also express every braid in terms of the elements of $\mathfrak{f}$ and their translated images.

Proposition 3. (i) *The mapping* Π *is an injection of the set of all finite* $\mathfrak{f}$-*colourings into* B_∞.

(ii) *Every positive braid has a unique expression as* $\Pi(\vec{x})$ *where* $\vec{x}$ *is a finite* $\mathfrak{f}$-*colouring.*

(iii) *Every braid* $\sigma(\alpha)$ *is equal to* $(\Pi(\vec{x}))^{-1}\Pi(\vec{x}^\alpha)$ *where* $\vec{x}$ *is any* α-*permitted finite* $\mathfrak{f}$-*labelling.*

Proof. For (i) assume that $\vec{x}$ and $\vec{y}$ are finite $\mathfrak{f}$-colourings. By Lemma 1(i) there exist braid words α and β satisfying

$$\begin{cases} \sigma(\alpha) = \Pi(\vec{x}) \quad \text{and} \quad \vec{1}^\alpha = \vec{x}, \\ \sigma(\beta) = \Pi(\vec{y}) \quad \text{and} \quad \vec{1}^\beta = \vec{y}. \end{cases}$$

If $\Pi(\vec{x})$ and $\Pi(\vec{y})$ are equal, the braid words α and β are $\equiv$-equivalent, and by Lemma 6.1 the colourings $\vec{1}^\alpha$ and $\vec{1}^\beta$ are equal.

Point (iii) follows from Lemma 1(ii), and point (ii) is a particular case: if A is a positive braid word, the colouring $\vec{1}$ is certainly A-permitted, and $\sigma(A) = \Pi(\vec{1}^A)$ holds. □

We turn to the construction of a linear ordering on B_∞. We begin two auxiliary results about LD-equivalence.

Definition. Two terms P, Q in $\mathcal{T}_\Sigma$ are *strongly LD-inequivalent* if Q is obtained from P by modifying its last variable (and this one only).

Because the rightmost variable in a term is invariant under LD-equivalence, strongly LD-inequivalent terms must be LD-inequivalent.

Lemma 4. *Assume that* P', Q' *are strongly LD-inequivalent terms and that* $P' \sqsubset_{\mathrm{LD}} P$ *and* $Q' \sqsubset_{\mathrm{LD}} Q$ *hold. Then* P *and* Q *are not LD-equivalent.*

Proof. Assume $P =_{\mathrm{LD}} Q$. By three calls to Property B there exists a common extension R of P and Q and integers p and q such that $l^p(R)$ is an extension P' and $l^q(R)$ is an extension of Q'. Let b (resp. c) be the rightmost variable of P' (resp. Q'). The integers p and q cannot be equal since the rightmost variable of $l^p(R)$ must be b while the rightmost variable of $l^q(R)$ must be c. Assume $p > q$, and let P'' be the term obtained from $l^q(R)$ by replacing the rightmost occurrence of c by b. Now P'' is LD-equivalent to the term obtained from Q' by replacing the rightmost occurrence of c by b, which is P' by hypothesis. So P'' must be LD-equivalent to P' and therefore, to its own prefix $l^p(R)$, contradicting the antireflexivity of $\sqsubset_{\mathrm{LD}}$. □

For R a binary relation on the set X, we denote by R^* the lexicographical extension of R to $X^{\mathbf{N}}$. Thus for any two $\mathfrak{f}$-colourings $\vec{x}$, $\vec{y}$, $\vec{x} <_{\mathfrak{f}}^* \vec{y}$ holds if there exists an integer i such that $x_k = y_k$ holds for $k < i$ and $x_i <_{\mathfrak{f}} y_i$ holds. The relation $<_{\mathfrak{f}}^*$ is a strict linear ordering on $\mathfrak{f}$-colourings.

Lemma 5. *For any two positive braid words* A, B, *the following are equivalent*:

(i) *there exists a finite* $\mathfrak{f}$-*colouring* $\vec{x}$ *and* $\vec{x}^A <_{\mathfrak{f}}^* \vec{x}^B$;

(ii) *every finite* $\mathfrak{f}$-*colouring* $\vec{x}$ *satisfies* $\vec{x}^A <_{\mathfrak{f}}^* \vec{x}^B$;

(iii) $\vec{1}^A <_{\mathfrak{f}}^* \vec{1}^B$ *holds.*

Proof. We first show that (iii) implies (ii). Assume $(\vec{\mathbf{1}})^A <_{\mathfrak{f}}^* (\vec{\mathbf{1}})^B$. We fix an infinite set Σ and a sequence $a_1, a_2, \ldots$ of distinct elements of Σ. The free LD-system $\mathscr{T}_\Sigma/{=_{\mathrm{LD}}}$ is denoted by $\mathfrak{f}_\Sigma$. The relation $\sqsubset_{\mathrm{LD}}$ induces on $\mathfrak{f}_\Sigma$ a (strict) partial ordering denoted $<_{\mathfrak{f}_\Sigma}$. We claim that

$$(1) \qquad \langle \dot{a}_1, \dot{a}_2, \ldots \rangle^A <_{\mathfrak{f}_\Sigma}^* \langle \dot{a}_1, \dot{a}_2, \ldots \rangle^B$$

holds, where $\dot{P}$ denotes the class P in $\mathfrak{f}_\Sigma$. Then any mapping of Σ into $\mathfrak{f}$ extends to a projection of $\mathfrak{f}_\Sigma$ into $\mathfrak{f}$ which is compatible with the orderings $<_{\mathfrak{f}_\Sigma}$ and $<_{\mathfrak{f}}$, so for every $\mathfrak{f}$-colouring $\vec{\mathfrak{x}}$ the inequality (1) implies $\vec{\mathfrak{x}}^A <_{\mathfrak{f}}^* \vec{\mathfrak{x}}^B$, which establishes point (ii).

In order to prove the claim, choose n large enough so that no factor greater than $n-1$ occurs in A or B. Denote by P and Q respectively the images of the term $a_1[a_2[\cdots[a_n]\cdots]]$ under $\Omega_{A\sharp}$ and $\Omega_{B\sharp}$ where $\sharp$ denotes the morphism of $\mathscr{W}$ to $\mathscr{S}$ which map i to 1^{i-1}. Let P_k (resp. Q_k) denote the subterm $P_{(1^{k-1}0)}$ (resp. $Q_{(1^{k-1}0)}$). For each term R in $\mathscr{T}_\Sigma$ we denote by R^τ the term in $\mathscr{T}_a$ obtained from R by replacing any element of Σ by a. The hypothesis $\vec{\mathbf{1}}^A <_{\mathfrak{f}}^* \vec{\mathbf{1}}^B$ is $P^\tau \sqsubset_{\mathrm{LD}}^* Q^\tau$, and inequality (1) is $P \sqsubset_{\mathrm{LD}}^* Q$.

Consider the least i such that $P_i =_{\mathrm{LD}} Q_i$ fails. Such an i must exist, since otherwise one would have

$$\langle \dot{a}_1, \dot{a}_2, \ldots \rangle^A = \langle \dot{a}_1, \dot{a}_2, \ldots \rangle^B$$

which projects onto $P^\tau =_{\mathrm{LD}} Q^\tau$, contradicting the hypothesis. For $k < i$ the equivalence $P_k =_{\mathrm{LD}} Q_k$ projects onto $P_k^\tau = \mathrm{LD} Q_k^\tau$. Because two LD-inequivalent terms of $\mathscr{T}_a$ must be $\sqsubset_{\mathrm{LD}}$-comparable, three cases may occur.

Case 1. $Q_i^\tau \sqsubset_{\mathrm{LD}} P_i^\tau$ holds. Then $Q^\tau \sqsubset_{\mathrm{LD}}^* P^\tau$ holds, which contradicts the hypothesis $P^\tau \sqsubset_{\mathrm{LD}}^* Q^\tau$.

Case 2. $P_i^\tau =_{\mathrm{LD}} Q_i^\tau$ holds. Choose positive sequences Z, Z' in $\mathscr{S}^+$ such that Ω_Z and $\Omega_{Z'}$ map P_i^τ and Q_i^τ respectively to a common expansion R. Assume that Ω_Z maps P_i to P' and $\Omega_{Z'}$ maps Q_i to Q'. The term R is P'^τ and Q'^τ, so because P' and Q' are not LD-equivalent, they must have a 'variable disagreement', i.e., there exist terms $R_1, \ldots, R_p$ and distinct variables b, c such that the patterns $R_1[\cdots[R_p[b$ and $R_1[\cdots[R_p[c$ are prefixes of the *words* P' and Q'. Using easy left distributivity transformations one deduces

$$R_1[\cdots[R_p[b]]\cdots] \sqsubset_{\mathrm{LD}} P' \quad \text{and} \quad R_1[\cdots R_p[c]]\cdots] \sqsubset_{\mathrm{LD}} Q',$$

whence

$$R_1[\cdots[R_p[b]\cdots] \sqsubset_{\mathrm{LD}} P_i \quad \text{and} \quad R_1[\cdots[R_p[c]]\cdots] \sqsubset_{\mathrm{LD}} Q_i.$$

By distributivity again one obtains

$$P_1[\cdots[P_{i-1}[R_1[\cdots[R_p[b]]\cdots]]]\cdots] \sqsubset_{\mathrm{LD}} P$$

and

$$P_1[\cdots[P_{i-1}[R_1[\cdots[R_p[c]]\cdots]]]\cdots]_{\mathrm{LD}} \sqsubset Q,$$

which shows that the terms P and Q are strongly LD-inequivalent. By Lemma 4, this contradicts the equivalence $P =_{\mathrm{LD}} Q$ which holds since the terms P and Q are extensions of the term $a_1[a_2[\cdots[a_n]\cdots]]$.

Case 3. $Q_i^\tau \sqsubset_{\mathrm{LD}} P_i^\tau$ holds. As above, choose positive sequences Z, Z' such that Ω_Z and $\Omega_{Z'}$ map P_i^τ and Q_i^τ respectively to terms R, S such that one is a strict prefix of the other one. Assume $R \sqsubset S$. Assume that Ω_Z maps P_i to P' and $\Omega_{Z'}$ maps Q_i to Q'. Then either P' is a strict prefix of Q' or they have a 'variable disagreement'. As in Case 2 the latter situation is impossible. So $P_i \sqsubset_{\mathrm{LD}} Q_i$ holds, which implies $P \sqsubset_{\mathrm{LD}}^* Q$. Since Case 3 was the only possible case, this proves inequality (1), and therefore (ii) follows from (iii).

It follows that for any pair of positive sequences A, B, either $(\vec{\boldsymbol{x}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{x}})^B$ holds for every $\vec{\boldsymbol{x}}$, or $(\vec{\boldsymbol{x}})^A = (\vec{\boldsymbol{x}})^B$ holds for every $\vec{\boldsymbol{x}}$, or $(\vec{\boldsymbol{x}})^B <_{\mathfrak{f}}^* (\vec{\boldsymbol{x}})^A$ holds for every $\vec{\boldsymbol{x}}$. So if $(\vec{\boldsymbol{x}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{x}})^B$ holds for at least one $\vec{\boldsymbol{x}}$, necessarily it holds for every $\vec{\boldsymbol{x}}$ and in particular, for $\vec{\mathbf{1}}$. So the proof of the lemma is complete. □

We are ready to define a linear ordering on B_∞ using the lexicographical extension of $<_{\mathfrak{f}}$. This ordering is constructed so that every generator σ_i is preponderant over all σ_k with $k \geq i$.

Definition. Assume that $\prec$ is an ordering on a group G. For a in G and X a subset of G, we say that a is *infinitely large* with respect to X if $x \prec yay^{-1}$ holds for every x, y in the subgroup generated by X.

Theorem 6. (i) *There exists a unique ordering $<$ on the braid group B_∞ which is compatible with left translations and is such that, for every i, the generator σ_i is infinitely large with respect to the family of all σ_k with $k > i$.*

(ii) *This ordering is linear and compatible with the shift endomorphism. It extends the left-divisibility ordering on B_∞ and the linear ordering $<_{\mathfrak{f}}$ on $\mathfrak{f}$.*

(iii) *For any braid words α, β, the inequality $\sigma(\alpha) < \sigma(\beta)$ holds if and only if $(\vec{\boldsymbol{x}})^\alpha <_{\mathfrak{f}}^* (\vec{\boldsymbol{x}})^\beta$ holds for every finite $\mathfrak{f}$-colouring $\vec{\boldsymbol{x}}$ which is permitted for α and β if and only if this inequality holds for at least one such $\mathfrak{f}$-colouring.*

(iv) *There exists a primitive recursive algorithm for comparing braid words with respect to $<$.*

Proof. Say that a braid is *positive* if it can be written as $\sigma(\overline{A} \bullet B)$ where A, B are positive words satisfying $(\vec{\mathbf{1}})^A <_{\mathfrak{f}}^* (\vec{\mathbf{1}})^B$. We denote by B_∞^{++} the set of all positive braids and construct our ordering consistently with this notion of positivity. Clearly B_∞^+ is included in B_∞^{++}, and because $<_{\mathfrak{f}}^*$ is antireflexive, 1 does not belong to B_∞^{++}.

Claim 1. The braid x belongs to B_∞^{++} if and only if $(\vec{\mathbf{1}})^A <_{\mathfrak{f}}^* (\vec{\mathbf{1}})^B$ holds for *every* expression of x as $\sigma(\overline{A} \bullet B)$ with A, B positive braid words.

Proof. If $\overline{A} \bullet B$ and $\overline{A'} \bullet B'$ are $\equiv$-equivalent, there exist positive words C, C' satisfying

$$C \bullet A \equiv C' \bullet A', \quad C \bullet B \equiv C' \bullet B',$$

and by Lemma 5 we have the equivalences

$$\vec{\mathbf{1}}^A <_{\mathfrak{f}}^* \vec{\mathbf{1}}^B \Leftrightarrow (\vec{\mathbf{1}}^C)^A <_{\mathfrak{f}}^* (\vec{\mathbf{1}}^C)^B \Leftrightarrow (\vec{\mathbf{1}}^{C'})^{A'} <_{\mathfrak{f}}^* (\vec{\mathbf{1}}^{C'})^{B'} \Leftrightarrow \vec{\mathbf{1}}^{A'} <_{\mathfrak{f}}^* \vec{\mathbf{1}}^{B'}. \quad \square$$

Claim 2. The set B_∞^{++} is stable under product.

Proof. Assume that $\sigma(\overline{A} \bullet B)$ and $\sigma(\overline{A'} \bullet B')$ belong to B_∞^{++}. Choose positive words A'' and B'' satisfying $A'' \bullet B \equiv B'' \bullet A'$. Using Lemma 5 again, we have

$$\vec{\mathbf{1}}^{A'' \bullet A} = (\vec{\mathbf{1}}^{A''})^A <_{\mathfrak{f}}^* (\vec{\mathbf{1}}^{A''})^B = (\vec{\mathbf{1}}^{B''})^{A'} <_{\mathfrak{f}}^* (\vec{\mathbf{1}}^{B''})^{B'} = \vec{\mathbf{1}}^{B'' \bullet B'},$$

which shows that $\sigma(\overline{A} \bullet B \bullet \overline{A'} \bullet B')$ belongs to B_∞^{++}. □

Now define the relation $<$ on B_∞ by

$$x < y \Leftrightarrow x^{-1}y \in B_\infty^{++}.$$

Claim 3. The relation $<$ is a strict ordering which is compatible with left translations and extends the left-divisibility partial ordering. This ordering is linear on B_∞ and invariant under the shift endomorphism.

Proof. The first part is obvious from Claim 2 and the definition of $<$. The ordering $<$ is linear because $<_{\mathrm{f}}^*$ is a linear ordering and every braid can be written as $\sigma(\overline{A} \bullet B)$ for some positive words A, B. And because $\vec{\mathbf{1}}^{\alpha} = \langle a_1, a_2, \ldots \rangle$ implies $\vec{\mathbf{1}}^{s(\alpha)} = \langle 1, a_1, a_2, \ldots \rangle$, the set B_∞^{++} is stable under s and $x < y$ is equivalent to $s(x) < s(y)$. □

Claim 4. If $\sigma(\alpha)$ belongs to B_∞^{++}, there exists at least one α-permitted colouring $\vec{\boldsymbol{x}}$ satisfying $\vec{\boldsymbol{x}} <_{\mathrm{f}}^* \vec{\boldsymbol{x}}^{\alpha}$.

Proof. Let $\vec{\boldsymbol{x}}$ be $\vec{\mathbf{1}}^{D_{\mathrm{L}}(\alpha)}$: the colouring $\vec{\boldsymbol{x}}$ is permitted for $\overline{D_{\mathrm{L}}(\alpha)} \bullet N_{\mathrm{L}}(\alpha)$, and one has

$$\vec{\boldsymbol{x}} = \vec{\mathbf{1}}^{D_{\mathrm{L}}(\alpha)} <_{\mathrm{f}}^* \vec{\mathbf{1}}^{N_{\mathrm{L}}(\alpha)} = \vec{\boldsymbol{x}}^{\overline{D_{\mathrm{L}}(\alpha)} \bullet N_{\mathrm{L}}(\alpha)}.$$

But α is left-reducible to $\overline{D_{\mathrm{L}}(\alpha)} \bullet N_{\mathrm{L}}(\alpha)$, so by the claim in the proof of Lemma 6.1 we know that $\vec{\boldsymbol{x}}$ is α-permitted and that $\vec{\boldsymbol{x}}^{\alpha}$ is equal to $\vec{\boldsymbol{x}}^{\overline{D_{\mathrm{L}}(\alpha)} \bullet N_{\mathrm{L}}(\alpha)}$. □

Claim 5. The inequality $s(x) < s(y)\sigma_1 s(z)$ holds for every x, y, z in B_∞.

Proof. It suffices to show that any σ_1-positive braid belongs to B_∞^{++}. Assume that $\sigma(\gamma)$ is σ_1-positive. By Proposition 6.2 we know that $\sigma(\gamma)$ is not 1. Assume that $\sigma(\gamma)$ is not in B_∞^{++}. Then $\sigma(\overline{\gamma})$ belongs to B_∞^{++}, and by Claim 4 there exists a $\overline{\gamma}$-permitted colouring $\vec{\boldsymbol{y}}$ satisfying $\vec{\boldsymbol{y}} <_{\mathrm{f}}^* \vec{\boldsymbol{y}}^{\overline{\gamma}}$, and therefore (by taking $\vec{\boldsymbol{x}} = \vec{\boldsymbol{y}}^{\overline{\gamma}}$) there exists a γ-permitted colouring $\vec{\boldsymbol{x}}$ satisfying $\vec{\boldsymbol{x}}^{\gamma} <_{\mathrm{f}}^* \vec{\boldsymbol{x}}$. Now the proof of Proposition 6.2 gives the inequality $\vec{\boldsymbol{x}} <_{\mathrm{f}}^* \vec{\boldsymbol{x}}^{\gamma}$ for every γ-permitted colouring $\vec{\boldsymbol{x}}$, a contradiction. Hence $\sigma(\gamma)$ belongs to B_∞^{++}. □

This shows that σ_1 is infinitely large with respect to the image of s and therefore, with respect to the family of all σ_k with $k > 2$. Because $<$ is compatible with s, this implies the similar property for the other generators and finishes the proof of the existence of the ordering.

In order to prove the uniqueness, assume that $<'$ is any ordering on B_∞ satisfying the conditions of (i).

Claim 6. Assume that k occurs in the braid word γ but neither $1, 2, \ldots, k-1$ nor $\overline{1}, \overline{2}, \ldots, \overline{k}$ occurs in γ. Then $1 <' \sigma(\gamma)$ holds.

Proof. Assume that no integer $\leq k$ occurs in the braid words $\gamma_0, \gamma_1, \ldots$. We prove inductively on $n \geq 1$ the inequality

$$1 <' \sigma(\gamma_0 \bullet k \bullet \gamma_1 \bullet \cdots \bullet k \bullet \gamma_n).$$

If n is 1, the hypothesis that σ_k is infinitely large for $<'$ with respect to the σ_i with $i > k$ gives

$$\sigma(\overline{\gamma_1} \bullet \gamma_0) <' \sigma(\overline{\gamma_1})\sigma_k\sigma(\gamma_1)$$

which implies, since $<'$ is compatible with left translations,

$$1 <' \sigma(\gamma_0)\sigma_k\sigma(\gamma_1).$$

For the induction we have $1 <' \sigma_k\sigma(\gamma_n)$ which implies

$$\sigma(\gamma_0)\sigma_k \cdots \sigma(\gamma_{n-1}) <' \sigma(\gamma_0)\sigma_k \cdots \sigma(\gamma_{n-1})\sigma_k\sigma(\gamma_n)$$

and therefore $1 <' \sigma(\gamma_0)\sigma_k \cdots \sigma(\gamma_{n-1})$ implies $1 <' \sigma(\gamma)\sigma_k \cdots \sigma(\gamma_n)$. □

Claim 7. For every $\mathfrak{f}$-colourings $\vec{x}, \vec{y}$, $\vec{x} <^*_{\mathfrak{f}} \vec{y}$ implies $\Pi(\vec{x}) <' \Pi(\vec{y})$.

Proof. Assume $x_i = y_i$ for $i < k$ and $x_k <_{\mathfrak{f}} y_k$. By construction the braid $\Pi(\vec{x})^{-1}\Pi(\vec{y})$ has an expression $\sigma(\gamma)$ where γ satisfies the hypothesis of Claim 6. So the relation $1 <' \Pi(\vec{x})^{-1}\Pi(\vec{y})$ holds. Since $<'$ is compatible with left translations, this implies $\Pi(\vec{x}) <' \Pi(\vec{y})$. □

Claim 8. The orderings $<'$ and $<$ coincide.

Proof. Assume that z belongs to B_∞^{++}. By definition there exist positive braid words A, B such that z is $\sigma(\overline{A} \bullet B)$ and $\vec{\mathbf{1}}^A <^*_{\mathfrak{f}} \vec{\mathbf{1}}^B$ holds. By Lemma 1, $\sigma(A)$ is $\Pi(\vec{\mathbf{1}}^A)$ and $\sigma(\beta)$ is $\pi(\vec{\mathbf{1}}^B)$. By Claim 7 one obtains $\sigma(A) <' \sigma(B)$, which implies $1 <' \sigma(\overline{A} \bullet B)$ since $<'$ is compatible with left translations. So $1 < z$ implies $1 <' z$, and then $x < y$ implies $x <' y$. Because $<$ is a linear ordering and $<'$ is an ordering, this is enough to conclude. □

Claim 9. If $\sigma(\alpha) < \sigma(\beta)$ holds, then $\vec{x}^\alpha <^*_{\mathfrak{f}} \vec{x}^\beta$ holds for every finite $\mathfrak{f}$-colouring $\vec{x}$ which is α- and β-permitted.

Proof. Assume that $\vec{x}$ is a finite $\mathfrak{f}$-colouring which is permitted both for α and β. By Claim 7 (and the fact that $<$ and $<^*_{\mathfrak{f}}$ are linear orderings) the inequality $\vec{x}^\alpha <^*_{\mathfrak{f}} \vec{x}^\beta$ is equivalent to $\Pi(\vec{x}^\alpha) < \Pi(\vec{x}^\beta)$, therefore by the formula of Lemma 1(ii) to

$$\Pi(\vec{x})\sigma(\alpha) < \Pi(\vec{x})\sigma(\beta),$$

and finally to $\sigma(\alpha) < \sigma(b)$. □

Point (iii) of the theorem clearly follows. For point (iv), observe that, according to the definition of B_∞^{++}, the comparison of $\sigma(\alpha)$ to 1 consists of reducing α on the left, determining $\vec{\mathbf{1}}^{N_{\mathrm{L}}(\alpha)}$ and $\vec{\mathbf{1}}^{D_{\mathrm{L}}(\alpha)}$, and comparing these colourings with respect to $<^*_{\mathfrak{f}}$. The last two steps respectively correspond to applying the transformations $\Omega_{N_{\mathrm{L}}(\alpha)^\#}$ and $\Omega_{D_{\mathrm{L}}(\alpha)^\#}$ to a term $a^{[n]}$ with n large enough and comparing with respect to $\sqsubset_{\mathrm{LD}}$ the successive subterms $P_{(1^i 0)}$ and $Q_{(1^i 0)}$ of the images P and Q using the reduction in $\widetilde{B}_\infty$ of the associated χ-sequences. By Proposition 4.5 the complexity of this method is bounded by a tower of exponentials, and therefore the relation $<$ on B_∞ is primitive recursive. This finishes the proof of the theorem. □

With the present construction, the order type of $<$ on arbitrary braids is η, while the order type of its restriction to positive braids is $(\omega(1+\eta))^{\omega^*}$ where ω, ω^*, and η respectively denote the order types of the natural numbers, the negative integers, and the rationals. Subsequently Richard Laver proved in [26] that, the restriction of $<$ to B_n^+ is (for every n) a well ordering and that it extends the partial ordering defined in [14]. Actually it is easy to modify slightly the definition to obtain a well ordering on B_∞^+, thus associating with every positive braid a well-defined ordinal rank. We conjecture that the order type of B_∞^+ endowed with this well ordering is ω^{ω^ω}.

As Larue has noted, the existence of the linear ordering $<$ on B_∞ immediately implies that the group B_∞ is torsionfree. We hope for new applications in the future.

References

1. J. Birman, *Braids, links, and mapping class groups*, Ann. of Math. Stud., no. 82, Princeton Univ. Press, 1975.
2. E. Brieskorn, *Automorphic sets and braids and singularities*, Contemp. Math., vol. 78, Amer. Math. Soc., Providence, RI, 1988, pp. 45–117.
3. P. Cartier, *Développements récents sur les groupes de tresses, applications 'a la topologie et à l'algèbre*, Séminaire Bourbaki, exposé 716, 1989.
4. P. Dehornoy, *Algebraic properties of the shift mapping*, Proc. Amer. Math. Soc. **106** (1989), 617–623.
5. ——, *Free distributive groupoids*, J. Pure Appl. Algebra **61** (1989), 123–146.
6. ——, *Sur la structure des gerbes libres*, C. R. Acad. Sci. Paris Sér. I Math. **309** (1989), 143–148.
7. ——, *Problème de mots dans les gerbes libres*, Theoret. Comput. Sci. **94** (1992), 199–213.
8. ——, *Structural monoids associated to equational varieties*, Proc. Amer. Math. Soc. **117** (1993), 293–304.
9. ——, *A canonical ordering for free left distributive magmas*, Proc. Amer. Math. Soc. (to appear).
10. ——, *A normal form for the free left distributive law*, Internat. J. Algebra Comput. (to appear).
11. ——, *Reduction of braid words*, preprint, 1993.
12. R. Dougherty, *Critical points in an algebra of elementary embeddings*, preprint, 1992.
13. R. Dougherty and Th. Jech, *Finite left-distributive algebras and embedding algebras*, preprint, 1992.
14. E. A. Elrifai and H. R. Morton, *Algorithms for positive braids*, Quart. J. Math. Oxford (to appear).
15. D. B. Epstein et al., *Word processing in groups*, Jones and Barlett, 1992.
16. R. Fenn and C. Rourke, *Racks and links in codimension* 2, J. Knot Theory and its Ramifications (to appear).
17. F. A. Garside, *The braid group and other groups*, Quart J. Math. Oxford **20** (1969), 235–254.
19. T. Kepka, *Notes on left distributive groupoids*, Acta Univ. Carolin.—Math. Phys. **22** (1981), 23–37.
20. A. Kanamori, W. Reinhardt, and R. Solovay, *Strong axioms of infinity and elementary embeddings*, Ann. Math. Logic **13** (1978), 73–116.
21. D. Joyce, *A classifying invariant of knots: the knot quandle*, J. Pure Appl. Algebra **23** (1982), 37–65.
22. D. Larue, *On braid words and irreflexivity*, Algebra Univ. **31** (1994), 104-112.
23. R. Laver, *Elementary embeddings of a rank into itself*, Abstracts Amer. Math. Soc. **7** (1986), 6 .
24. ——, *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. **91** (1992), 209–231.
25. ——, *A division algorithm for the free left distributive algebra*, Proc. Helsinki 1990 ASL Meeting, Lecture Notes in Logic, Springer-Verlag, 1993, pp. 155–166.

26. ——, *Braid group actions on left distributive structures and well-orderings in the braid group*, preprint, 1993.

27. S. Mac Lane, *Natural associativity and commutativity*, Rice Univ. Studies **49** (1963), 28–46.

28. J. Paris and L. Harrington, *A mathematical incompleteness in Peano arithmetic*, Handbook of Mathematical Logic (J. Barwise, Ed.), North-Holland, 1977, pp. 1133–1142.

29. W. Thurston, *Finite state algorithms for the braid group*, preprint, 1988.

MATHÉMATIQUES, UNIVERSITÉ, 14 032 CAEN, FRANCE
E-mail address: dehornoy@geocub.greco-prog.fr