Braid Groups and Left Distributive Operations.

Patrick DEHORNOY

March 1992

ABSTRACT. An extension of the infinite braid group B_∞ exactly describes the left distributivity identities. These identities form a decidable family. The group B_∞ is closely connected with the free left distributive structure with one generator, and inherits some order properties with simple topological meaning. A quick comparison algorithm for braid words is also given.

The first aim of this paper is to construct 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 not a consequence of the left distributivity identity* $x(yz) = (xy)(xz)$.

The former status of this question was unusual. Two partial solutions have been proposed independently in [5] and [20] by reducing the decidability to a (unique) algebraic hypothesis known as the Irreflexivity Conjecture. This conjecture has been shown by Richard Laver to follow from a very strong (hence unprovable) set theoretical axiom. The question was whether this additional assumption is necessary or not. The opinions thereabout were divided: on one hand the connection between the existence of very large cardinals and a purely finitistic problem like the one above seemed strange, but on the other hand no metamathematical reason is known to forbid such a connection and some works on distributive structures ([9]) showed that intrinsically complex objects necessarily arise in their description.

In this paper we definitely eliminate all logical assumptions in this question and give a solution which is purely algebraic in methods and spirit. We first introduce an algebraic structure on left distributivity identities themselves. Definitions can be made in such a way that the structure C_{LD} thus constructed resembles a group. Then one replaces the study of C_{LD}, which has only a partial product and is incompletely

known at the beginning, by the study of a true group $\widetilde{B}_\infty$ whose presentation is suggested by the relations which are known to hold in C_{LD}. The main idea is that, if the relations used to define $\widetilde{B}_\infty$ reflect the core of left distributivity, then $\widetilde{B}_\infty$ should resemble C_{LD}, and, in particular, the results proved for C_{LD} using the geometry of left distributivity should have a purely algebraic counterpart in $\widetilde{B}_\infty$. This actually happens.

The group $\widetilde{B}_\infty$ is an extension of the infinite braid group B_∞, a property which reflects a deep connection between braids and distributive operations. Actually $\widetilde{B}_\infty$ is a kind of 'ramified' version of B_∞ where an infinite tree replaces the chain of integers. Though the kernel of the projection of $\widetilde{B}_\infty$ onto B_∞ is very large, both groups have very similar properties. For the study of $\widetilde{B}_\infty$, we use the special form of the relations in its presentation. The crucial points concern the decompositions of arbitrary words as quotients of positive words. The approach we develop for these questions projects to B_∞ immediately. As an application we obtain a new algorithm for comparing braid words which runs in quadratic time. Our method can be seen as a variant of the one described in [23]. Its particularity is to avoid any use of a specific normal form.

With the proof of the Irreflexivity Conjecture and the properties of $\widetilde{B}_\infty$, many questions about free distributive structures are settled. In particular one obtains *a posteriori* the complete description of the structure C_{LD}, a quotient of which identifies with a subset of $\widetilde{B}_\infty$. This shows that the relations defining $\widetilde{B}_\infty$ exactly reflect the geometry of left distributivity, and in particular some 'heptagonal identity' has a crucial importance. For the original problem of recognizing the consequences of left distributivity we obtain a primitive recursive bound.

It is known that the braid groups act on distributive structures where left translations are bijective ([2]). We observe that injectivity of left translations is actually sufficient for defining a partial action. This enables to use the free distributive structures for constructing distributive representations of B_∞. Actually, the connection between braids and distributive operations can be made complete: one constructs inside B_∞ a realisation $\mathfrak{f}$ of the free left distributive structure with one generator, and, conversely, every braid can be decomposed as a product of terms in $\mathfrak{f}$ and its translated copies. When the connection is used from braids to distribution, one obtains a simply exponential method for recognizing the consequences of left distributivity involving only one variable. When the connection is used from distribution to braids, one transfers the existence of a linear ordering.

Theorem.- *There exists a unique ordering on B_∞ which is compatible with product on the left and is such that every generator σ_i is infinitely large w. r. to all σ_k with $k > i$. This ordering is linear, it extends the divisibility partial ordering and there is an effective method for comparing braid words.*

The general orientation of the paper is from distributive operations to braids. It is organized as follows. The first six sections are devoted to the proof of the decidability result for the consequences of left distributivity. Section 1 constructs the structure C_{LD}, introduces the Irreflexivity Conjecture and revives some connected results used in the sequel. Section 2 introduces the abstract group $\widetilde{B}_\infty$ and translates the Irreflexivity Conjecture into an assumption about the decompositions of the elements of $\widetilde{B}_\infty$ into quotients of positive words. Section 3 establishes a general criterion for proving this assumption using the specific form of the presentation. Section 4 show that $\widetilde{B}_\infty$, as well as B_∞, satisfy the first part of the criterion. The algorithm for braid words comparison is described as a corollary. Section 5 introduces the geometrical notions which are needed in Section 6 for the proof of the second part of the criterion. Section 7 states the general results about distributive operations and the structure C_{LD}. Finally in Section 8 we investigate the distributive representations of braid groups, and deduce the order properties of B_∞ quoted above.

1. The algebraic structure of left distributivity identities.

Some algebraic structure on the set of all consequences of left distributivity reflects the geometry of this special identity. It is known that applying associativity or commutativity at various positions in a term gives rise to some geometrical relations, such as Maclane's pentagonal or hexagonal diagrams (see [22], [3]). We investigate similar relations in the case of distributivity. The construction itself is somewhat secondary here, the main point is the list of relations in Proposition 1 below.

Fix an infinite set Σ whose elements are called variables. The free magma generated by Σ using a single binary operation is denoted $\mathcal{T}_\Sigma$ and its elements are called terms. We write $P[Q]$ for the product of the terms P and Q. This notation gives the intuition that this product is the image of the term Q under some action of P, which is convenient in the left distributive framework (see [7]). With these notations, left distributivity is expressed as the following identity

$$(LD) \qquad \boldsymbol{x}[\boldsymbol{y}[\boldsymbol{z}]] = \boldsymbol{x}[\boldsymbol{y}][\boldsymbol{x}[\boldsymbol{z}]].$$

If $\approx_{LD}$ is the congruence on $\mathcal{T}_\Sigma$ generated by the pair $(\boldsymbol{x}[\boldsymbol{y}[\boldsymbol{z}]], \boldsymbol{x}[\boldsymbol{y}][\boldsymbol{x}[\boldsymbol{z}]])$, then the consequences of left distributivity (written with variables in Σ) are exactly the pairs (P, Q) in $\mathcal{T}_\Sigma^2$ which satisfy $P \approx_{LD} Q$. Thus the decision problem we investigate is the word problem for the equivalence relation $\approx_{LD}$ on $\mathcal{T}_\Sigma$.

The endomorphisms of the free magma $\mathcal{T}_\Sigma$ are *substitutions*: the image of any term P under such an endomorphism τ is the term P^τ obtained from P by replacing every occurrence of every variable $\boldsymbol{v}$ in P by the term $\boldsymbol{v}^\tau$. The set of all P^τ when τ ranges over $\mathrm{End}\mathcal{T}_\Sigma$ is denoted $\mathrm{Subst}(P)$. If (P, Q) and (P', Q') are pairs of terms and

there exists a substitution τ such that P' is P^τ and Q' is Q^τ, we say that (P', Q') is an *instance* of (P, Q) and write

$$(P, Q) \preceq (P', Q').$$

Denote by $\mathrm{Inst}(P, Q)$ the set of all instances of the pair (P, Q), and by $\bullet$ the opposite of composition for binary relations or mappings. It is natural to define the product of two identities in such a way that the mapping Inst becomes a morphism into the set of all binary relations on $\mathcal{T}_\Sigma$ equipped with $\bullet$. Results on terms unification (see *e.g.* [13]) make such a construction possible. Assume that (P_1, Q_1) and (P_2, Q_2) are arbitrary pairs. The relation $\mathrm{Inst}(P_1, Q_1) \bullet \mathrm{Inst}(P_2, Q_2)$ is nonempty if and only if the sets $\mathrm{Subst}(Q_1)$ and $\mathrm{Subst}(P_2)$ are not disjoint. In this case there exist substitutions τ_1 and τ_2 satisfying

$$\mathrm{Subst}(Q_1) \cap \mathrm{Subst}(P_2) = \mathrm{Subst}(Q_1^{\tau_1}) = \mathrm{Subst}(P_2^{\tau_2}), \tag{1}$$

and one has

$$\mathrm{Inst}(P_1, Q_1) \bullet \mathrm{Inst}(P_2, Q_2) = \mathrm{Inst}(P_1^{\tau_1}, Q_2^{\tau_2}).$$

We define the product of (P_1, Q_1) and (P_2, Q_2) as the pair $(P_1^{\tau_1}, Q_2^{\tau_2})$ above, thus obtaining a partial binary operation on pairs of terms which is associative when defined.

We consider the structure generated using this product by the translated copies of (LD), *i.e.* the identities which describe the application of left distributivity in a subterm of a given term. A convenient system of notations for such subterms is obtained by seeing terms in $\mathcal{T}_\Sigma$ as binary trees with leaves in Σ. We use finite sequences of 0's and 1's as addresses for nodes in such trees. An address describes the path in the tree from the root (whose address is the empty sequence denoted Λ) to the considered node, going to the left or to right at a branching point according to the fact that the next character in the address is 0 or 1. We denote by S the free monoid of all such finite sequences (which shall be called *points* in the sequel). The empty point is denoted by Λ, and the product on S by concatenation, so that 0^i denotes the product of i times 0. We fix some sequence $\langle \boldsymbol{x}_1, \boldsymbol{x}_2, \ldots \rangle$ in Σ.

Definition.- For every point w in S the *w-copy* of the pair (LD) is the pair $(LD)_w$ inductively defined by

$$(LD)_w = \begin{cases} (\boldsymbol{x}_1[\boldsymbol{x}_2[\boldsymbol{x}_3]], \boldsymbol{x}_1[\boldsymbol{x}_2][\boldsymbol{x}_1][\boldsymbol{x}_3]]) & \text{if } w \text{ is } \Lambda, \\ (P[\boldsymbol{x}_n], Q[\boldsymbol{x}_n]) & \text{if } w \text{ is } 0v, \ (LD)_v \text{ is } (P, Q) \text{ and } \boldsymbol{x}_n \text{ is the first variable which does not occur in } (P, Q) \\ (\boldsymbol{x}_1[P^\sigma], \boldsymbol{x}_1[Q^\sigma]) & \text{if } w \text{ is } 1v, \ (LD)_v \text{ is } (P, Q) \text{ and } \sigma \text{ is a substitution which maps every } \boldsymbol{x}_i \text{ to } \boldsymbol{x}_{i+1}. \end{cases}$$

The first and second components of the pair $(LD)_w$ coincide except the fact that their subterms in position w form a copy of (LD) (up to a renaming of the variables). For instance, we have

$$(LD)_0 = (\boldsymbol{x}_1[\boldsymbol{x}_2[\boldsymbol{x}_3]][\boldsymbol{x}_4], \boldsymbol{x}_1[\boldsymbol{x}_2][\boldsymbol{x}_1[\boldsymbol{x}_3]][\boldsymbol{x}_4]),$$
$$(LD)_1 = (\boldsymbol{x}_1[\boldsymbol{x}_2[\boldsymbol{x}_3[\boldsymbol{x}_4]]], \boldsymbol{x}_1[\boldsymbol{x}_2[\boldsymbol{x}_3]][\boldsymbol{x}_2[\boldsymbol{x}_4]]).$$

For w in S, $\overline{(LD)_w}$ denotes the symmetric pair of $(LD)_w$, and C_{LD} denotes the closure under product of the family of all $(LD)_w$ and $\overline{(LD)_w}$ where w ranges over S.

Proposition 1.- *i) The consequences of left distributivity are exactly the instances of the pairs in C_{LD}.*
ii) For every u, v, w in S, the relations

$$(LD)_u \bullet (LD)_{u1} \bullet (LD)_u = (LD)_{u1} \bullet (LD)_u \bullet (LD)_{u1} \bullet (LD)_{u0}$$
$$(LD)_u \bullet (LD)_{u11v} = (LD)_{u11v} \bullet (LD)_u$$
$$(LD)_u \bullet (LD)_{u10v} \bullet (LD)_{u00v} = (LD)_{u0v} \bullet (LD)_u$$
$$(LD)_u \bullet (LD)_{u01v} = (LD)_{u10v} \bullet (LD)_u$$
$$(LD)_{u0v} \bullet (LD)_{u1w} = (LD)_{u1w} \bullet (LD)_{u0v}$$

hold in C_{LD}.

Proof. For (i), the binary relation "(P, Q) is an instance of some pair in C_{LD}" is a congruence on $\mathcal{T}_\Sigma$ which includes and is included in $\approx_{LD}$. Point (ii) follows from a simple verification. The last four types follow from general geometric features similar to the ones used in the construction of critical pairs in Knuth-Bendix algorithm for rewrite systems (see [15]). The first one (the 'heptagonal identity') reflects a key property of left distributivity and is connected with the existence of an action of braid groups on distributive structures (see Section 8). ■

Let us now introduce the subset C^+_{LD} of C_{LD} generated by the identities $(LD)_w$ using product only (and no inverse). One verifies inductively that the first component of any element in C^+_{LD} is an *injective* term, *i.e.* a term where each variable occurs at most once. It follows that the product is always defined, and that C^+_{LD} equipped with product is a monoid. We say that a term Q is an *extension* of the term P if (P, Q) is an instance of a pair in C^+_{LD}. We revive without proof three earlier results. They have lead to a first approach to the word problem for $\approx_{LD}$ and will supply useful intuitions in the next sections. Assume that $\boldsymbol{x}$ is a fixed element in $\mathcal{T}_\Sigma$, and denote by $\mathcal{T}_{\boldsymbol{x}}$ the submagma of $\mathcal{T}_\Sigma$ generated by $\boldsymbol{x}$. Define inductively the terms $\boldsymbol{x}^{[n]}$ by $\boldsymbol{x}^{[1]} = \boldsymbol{x}$ and $\boldsymbol{x}^{[n]} = \boldsymbol{x}[\boldsymbol{x}^{[n-1]}]$ for $n > 1$.

Lemma 2.- ([5]) *If P is any term in $\mathcal{T}_{\boldsymbol{x}}$, then $\boldsymbol{x}^{[n]} \approx_{LD} P[\boldsymbol{x}^{[n-1]}]$ holds for n large enough.*

Lemma 3.- ([4])*Two terms in $\mathcal{T}_\Sigma$ are $\approx_{LD}$-equivalent if and only if they have a common extension.*

Let us write $\mathbf{S}_L(P)$ for the left subterm of the term P (which is defined if and only if P is not a variable), and $\mathbf{S}_L^i(P)$ for the i-th iterated left subterm of P (which is defined if and only if the leftmost branch of P viewed as a tree has length i at least).

Lemma 4.- ([4]) *Assume that the term Q is an extension of the term P, and P is not a variable. Then there exists an integer $j \geq 1$ such that $\mathbf{S}_L^j(Q)$ exists and is an extension of $\mathbf{S}_L(P)$.*

Putting these results together we obtain

Proposition 5.- (Comparison Property) *Assume that P, Q are any terms in $\mathcal{T}_{\boldsymbol{x}}$. Then there exists a term R and two integers i, j such that $\mathbf{S}_L^i(R)$ is an extension of P and $\mathbf{S}_L^j(R)$ is an extension of Q.*

Proof. By Lemma 2 we know that $\boldsymbol{x}^{[n]}$ is equivalent to $P[\boldsymbol{x}^{[n-1]}]$ and $Q[\boldsymbol{x}^{[n-1]}]$ for n large enough. By Lemma 3 the latter terms must have a common extension R, and by Lemma 4 some iterated left subterms of R are extensions respectively of the left subterm of $P[\boldsymbol{x}^{[n-1]}]$, which is P, and of the left subterm of $Q[\boldsymbol{x}^{[n-1]}]$, which is Q. ■

For P, Q in $\mathcal{T}_\Sigma$, write $P \sqsubset Q$ if P is $\mathbf{S}_L^k(Q)$ for some positive k, *i.e.* equivalently if the word P is a prefix of the word Q. Let $\sqsubset_{LD}$ be the relation obtained from $\sqsubset$ by $\approx_{LD}$-saturation: $P \sqsubset_{LD} Q$ holds if $P' \sqsubset Q'$ holds for some P', Q' which are $\approx_{LD}$-equivalent to P and Q respectively. Proposition 6 tells that two terms in $\mathcal{T}_{\boldsymbol{x}}$ which are not equivalent must be comparable with respect to $\sqsubset_{LD}$. Now for a given pair of terms (P, Q) there exists an effective enumeration of all pairs (P', Q') such that P' is an extension of P and Q' is an extension of Q, and the question of whether a term P' is a prefix of the term Q' is obviously decidable, so that the relation $\sqsubset_{LD}$ is certainly semi-decidable, as well as the relation $\approx_{LD}$. So a sufficient condition for the decidability of $\approx_{LD}$ (and $\sqsubset_{LD}$) is that the relations $\approx_{LD}$ and $\sqsubset_{LD}$ are disjoint, which can be expressed as the

Irreflexivity Conjecture.- *The relation $\sqsubset_{LD}$ is irreflexive.*

Another equivalent formulation is that no equivalence of the form

$$P \approx_{LD} P[Q_1]\ldots[Q_k]$$

may hold in $\mathcal{T}_{\boldsymbol{x}}$ for $k \geq 1$. This conjecture has been introduceded independently in [5] and [20], and was already used in [4]. The approach of [20] is completely different of the present one, but both of them finally butted against the same obstruction, which

was considered more and more puzzling as various attacks failed. The hypothesis that the intrinsic complexity of $\approx_{LD}$ could forbid an elementary proof of the irreflexivity property has been considered. We shall show that no such obstruction exists, and that the relation $\approx_{LD}$ is decidable within arithmetic.

What is missing in the above approach is some *effectivity*. Starting from terms P, Q we know that there exist a big term R such that P and Q are equivalent to some left subterms of R, but we have no control of the ranks of these left subterms. In particular no uniqueness is obtained, and the irreflexivity property is just an external trick to replace the lack of uniqueness. Now *if the irreflexivity property is true*, the involved left subterms must be unique, and it should be possible to make the whole construction effective. The problem is that the natural approach for developing this effective version requires the left cancellation property in the monoid C^+_{LD}, and that the only known proof of this property uses in turn the irreflexivity of $\sqsubset_{LD}$. We shall avoid this vicious circle by making the construction in an auxiliary structure where left cancellation is provable.

For the moment we observe that the natural way for proving the Irreflexivity Conjecture is to use models of left distributivity. Let us call a set equipped with a left distributive bracket an *LD-magma*. We say that an LD-magma $\mathfrak{g}$ is *irreflexive* if no equality

$$a = a[b_1]\dots[b_k]$$

holds in $\mathfrak{g}$ for any positive k. Because the projection of any identity $P \approx_{LD} P[Q_1]\dots[Q_k]$ would yield an equality as above, we have the following criterion.

Lemma 6.- ([20]) *Assume that $\mathfrak{g}$ is an irreflexive LD-magma. Then the Irreflexivity Conjecture is true. Moreover all sub-LD-magmas of $\mathfrak{g}$ with one generator are free.*

Proof. The freeness of the monogenic sub-LD-magmas of $\mathfrak{g}$ originates in the comparison property: if π is a projection of $\mathcal{T}_{\boldsymbol{x}}$ into $\mathfrak{g}$, the image of $\sqsubset_{LD}$ has to be a strict linear ordering, and π must be injective since it preserves this ordering. ■

Few of the usual examples of distributive structures are relevant for the present purpose (see [16], [24]). Most of them indeed, such as conjugacy in groups or barycentric means, are idempotent and therefore fail to be irreflexive since they satisfy equalities $a = a[a]$. Using a kind of skew conjugacy on the injections of the positive integers, we obtained in [6] an LD-magma $\mathfrak{d}$ where no equality $a = a[b]$ is possible. But some equality $a = a[b_1][b_2]$ holds in $\mathfrak{d}$. Now in [20], Richard Laver establishes that, if the set theoretical axiom "There exists an elementary embedding of a rank into itself" (EE), which is a very strong large cardinal assumption (*c.f.* [17], [19]), is true, then the algebra obtained by iterating the elementary embedding whose existence is a left distibutive irreflexive (and therefore free) LD-magma. So the Irreflexivity Conjecture follows from the (unprovable) axiom (EE) and set theory arises in the study of distributive operations.

Our proof will consist in constructing a new model of left distributivity by defining a bracket operation on (a variant of) G_{LD}. Thus the elements of the model will be distributivity identities. This method has some similarity with Henkin's proof of the completeness theorem for first order logic where one constructs a model for a set of sentences in such a way that the elements of the model are themselves sentences.

2. An extension of the braid group.

The structure C_{LD} is poor: the product is not everywhere defined, the pair (Q,P) is not exactly an inverse of the pair (P,Q), we do not know whether the relations in Proposition 1.1 make an exhaustive presentation. To avoid these disadvantages we shall consider the abstract group which admits the above relations as a presentation. This group will turn to be close enough to C_{LD} to still satisfy the main properties arising from the geometry of distributivity.

Definition.- The group $\widetilde{B}_\infty$ is the group admitting a family of generators $\widetilde{\sigma}_w$ indexed by the set S and presented by the relations

$$\begin{gathered}
\widetilde{\sigma}_u \bullet \widetilde{\sigma}_{u1} \bullet \widetilde{\sigma}_u = \widetilde{\sigma}_{u1} \bullet \widetilde{\sigma}_u \bullet \widetilde{\sigma}_{u1} \bullet \widetilde{\sigma}_{u0} \\
\widetilde{\sigma}_u \bullet \widetilde{\sigma}_{u11v} = \widetilde{\sigma}_{u11v} \bullet \widetilde{\sigma}_u \\
\widetilde{\sigma}_u \bullet \widetilde{\sigma}_{u10v} \bullet \widetilde{\sigma}_{u00v} = \widetilde{\sigma}_{u0v} \bullet \widetilde{\sigma}_u \\
\widetilde{\sigma}_u \bullet \widetilde{\sigma}_{u01v} = \widetilde{\sigma}_{u10v} \bullet \widetilde{\sigma}_u \\
\widetilde{\sigma}_{u0v} \bullet \widetilde{\sigma}_{u1w} = \widetilde{\sigma}_{u1w} \bullet \widetilde{\sigma}_{u0v}
\end{gathered}$$

where u, v, w range over S.

Actually the family of all $\widetilde{\sigma}_{1^i}$ for $i \geq 0$ generates the group $\widetilde{B}_\infty$, but leads to an 'incomprehensible' presentation. For any set X, we write X^* for the free monoid generated by X, and $\mathsf{X}^{\mathbf{sym}}$ for the free monoid generated by the union of X and a disjoint copy $\overline{\mathsf{X}}$ of X. With these notations, the group $\widetilde{B}_\infty$ is a quotient of the monoid $\mathsf{S}^{\mathbf{sym}}$. We denote by $\widetilde{\sigma}$ the projection of $\mathsf{S}^{\mathbf{sym}}$ onto $\widetilde{B}_\infty$ which maps w to $\widetilde{\sigma}_w$, and by $\widetilde{\equiv}$ the associated congruence on $\mathsf{S}^{\mathbf{sym}}$. Similarly the braid group B_∞ is a quotient of $\mathsf{N}_+^{\mathbf{sym}}$ (where N_+ denotes the set of the positive integers). We denote by σ the projection of $\mathsf{N}_+^{\mathbf{sym}}$ onto B_∞ which maps i to the generator σ_i, and by $\equiv$ the congruence on $\mathsf{N}_+^{\mathbf{sym}}$ associated with the usual presentation of B_∞ from the generators σ_i. In this framework the elements of $\mathsf{N}_+^{\mathbf{sym}}$ will simply called braid words. A first justification for the name of the group $\widetilde{B}_\infty$ is the following

Lemma1.- *The braid group B_∞ is a quotient of the group $\widetilde{B}_\infty$.*

Proof. The morphism

$$\flat : w \mapsto \begin{cases} i+1 & \text{if } w \text{ is } 1^i, \\ \varepsilon & \text{if } w \text{ contains at least one } 0, \end{cases}$$

of $\mathrm{S}^{\mathbf{sym}}$ onto $\mathrm{N}_+^{\mathbf{sym}}$ induces a projection of $\widetilde{B}_\infty$ onto B_∞ as shows an easy examination of the defining relations of $\widetilde{\equiv}$ and $\equiv$. ■

The kernel of the projection of $\widetilde{B}_\infty$ onto B_∞ induced by $\flat$ will be described in Section 7. Presently we concentrate on translating the Irreflexivity Conjecture into a statement about the group $\widetilde{B}_\infty$.

By construction the structure C_{LD} is also related with the group $\widetilde{B}_\infty$. We extend the notation of Section 1 by defining $(LD)_\xi$ to be the image of the sequence ξ under the surjective partial morphism of a subset of $\mathrm{S}^{\mathbf{sym}}$ onto C_{LD} which maps w to $(LD)_w$ for w in S. An easy induction shows that exactly the same variables occur in both terms of each pair (P, Q) in C_{LD}, so that the relation $\mathrm{Inst}(P, Q)$ is a partial injective operator on $\mathcal{T}_\Sigma$. We shall in the sequel denote by $\Omega(\xi)$ the operator associated with the identity $(LD)_\xi$. For instance, the operator $\Omega(\Lambda)$ is the partial operator which maps every term $P[Q[R]]$ to the corresponding term $P[Q][P[R]]$. We observe that the correspondence between $(LD)_\xi$ and $\Omega(\xi)$ is a bijection. Let us write $(LD)_\xi \asymp (LD)_{\xi'}$ if the partial operators $\Omega(\xi)$ and $\Omega(\xi')$ coincide on the intersection of their domains. By 1.1 the implication

$$\xi \,\widetilde{\equiv}\, \xi' \Longrightarrow (LD)_\xi \asymp (LD)_{\xi'}$$

holds whenever $(LD)_\xi$ and $(LD)_{\xi'}$ are defined. It is not *a priori* obvious that $\asymp$ has to be an equivalence relation on C_{LD}, but we shall use as a guide the idea that the quotient $C_{LD}/\asymp$ should resemble $\widetilde{B}_\infty$, which will be established in Section 7.

The point is to define a distributive bracket on some quotient of $\widetilde{B}_\infty$. To this end we associate with every term P in $\mathcal{T}_{\boldsymbol{x}}$ a canonical sequence $\widetilde{\chi}_P$ in $\mathrm{S}^{\mathbf{sym}}$. We start from a proof of Lemma 1.2. Assume for an inductive argument that the term $\boldsymbol{x}^{[n+1]}$ is proved to be $\approx_{LD}$-equivalent both to $P[\boldsymbol{x}^{[n]}]$ and $Q[\boldsymbol{x}^{[n]}]$ for n large enough. Then (for n large enough) one obtains

$$\boldsymbol{x}^{[n]} \approx_{LD} P[\boldsymbol{x}^{[n-1]}] \approx_{LD} P[Q[\boldsymbol{x}^{[n-2]}]] \approx_{LD} P[Q][P[\boldsymbol{x}^{[n-2]}]] \approx_{LD} P[Q][\boldsymbol{x}^{[n-1]}],$$

and the same property holds for the term $P[Q]$. The induction starts since $\boldsymbol{x}^{[n]}$ is equal, hence equivalent, to $\boldsymbol{x}[\boldsymbol{x}^{[n-1]}]$ for every $n > 1$. By Proposition 1.1, this result implies that there must exist for every term P and every n large enough a sequence $\widetilde{\chi}_{P,n}$ in $\mathrm{S}^{\mathbf{sym}}$ such that the operator $\Omega(\widetilde{\chi}_{P,n}))$ maps the term $\boldsymbol{x}^{[n]}$ to the term $P[\boldsymbol{x}^{[n-1]}]$. The computation above gives for the sequences $\widetilde{\chi}_{P,n}$ the following induction clauses

$$\widetilde{\chi}_{\boldsymbol{x},n} = \varepsilon,$$
$$\widetilde{\chi}_{P[Q],n} = \widetilde{\chi}_{P,n} \bullet 1\widetilde{\chi}_{Q,n-1} \bullet \Lambda \bullet \overline{1\widetilde{\chi}_{P,n-1}},$$

where left concatenation is extended to sequences so that $u(w_1\bullet\ldots\bullet w_n)$ denotes $uw_1\bullet\ldots\bullet uw_n$, and $\overline{\xi}$ denotes the image of ξ under the involutory antiautomorphism of $\mathsf{S}^{\mathbf{sym}}$ which maps every element of S to its copy in $\overline{\mathsf{S}}$. This definition of $\widetilde{\chi}_{P,n}$ makes sense whenever n is greater than the height of the term P (viewed as a binary tree). A handy (but inessential) point is that the sequences $\widetilde{\chi}_{P,n}$ so constructed turn out to be independent of n. This invites to define a bracket on $\mathsf{S}^{\mathbf{sym}}$ by the formula

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

The computation above gives

Lemma 2.- *Let $\widetilde{\chi}_P$ be the image of the term P under the bracket preserving morphism of the free magma $\mathcal{T}_{\mathbf{x}}$ into $\mathsf{S}^{\mathbf{sym}}$ equipped with the bracket above which maps $\mathbf{x}$ to the empty sequence ε. Then the operator $\Omega(\widetilde{\chi}_P)$ maps $\mathbf{x}^{[n]}$ to $P[\mathbf{x}^{[n-1]}]$ whenever n is greater than the height of P.*

The bracket above on $\mathsf{S}^{\mathbf{sym}}$ has no reason to be left distributive, but we observe that, if the operator $\Omega(\xi)$ maps the term P to the term Q, then $\Omega(0\xi)$ maps $P[\mathbf{x}^{[n-1]}]$ to $Q[\mathbf{x}^{[n-1]}]$, so that the operators $\Omega(\widetilde{\chi}_P\bullet 0\xi)$ and $\Omega(\widetilde{\chi}_Q)$ take the same value on the term $\mathbf{x}^{[n]}$, suggesting that the lack of distributivity for the bracket on $\mathsf{S}^{\mathbf{sym}}$ is measured by the sequence 0ξ above. This is actually true.

Lemma 3.- *i) The following equivalences hold in $\mathsf{S}^{\mathbf{sym}}$*

$$\xi[\eta][\xi[\zeta]] \mathrel{\widetilde{\equiv}} \xi[\eta[\zeta]] \bullet 0$$
$$(\xi \bullet 0\xi')[\eta \bullet 0\eta'] \mathrel{\widetilde{\equiv}} \xi[\eta] \bullet 00\xi' \bullet 01\eta'.$$

ii) Assume that the term P is in $\mathcal{T}_{\mathbf{x}}$ and the operator $\Omega(\xi)$ maps P to Q. Then the equivalence

$$\widetilde{\chi}_P \bullet 0\xi \mathrel{\widetilde{\equiv}} \widetilde{\chi}_Q$$

holds.

Proof. For the first formulas apply the defining relations of $\widetilde{\equiv}$. For the second point it suffices to prove the result when the sequence ξ has length 1, *i.e.* is a point in S or its inverse. By symmetry we may assume that ξ is a point w in S. The result is proved inductively on the length of w. If w is Λ, the computation of $\widetilde{\chi}_P$ from $\widetilde{\chi}_{P_0}$, $\widetilde{\chi}_{P_{10}}$ and $\widetilde{\chi}_{P_{11}}$ where P is $P_0[P_{10}[P_{11}]]$ gives the result by applying the first relation of (i). If u is ev with $e = 0$ or $e = 1$, then the computation of $\widetilde{\chi}_P$ from $\widetilde{\chi}_{P_0}$ and $\widetilde{\chi}_{P_1}$ where P is $P_0[P_1]$ gives the result using the induction hypothesis and the second formula of (i). ■

Because the congruence $\widetilde{\equiv}$ is compatible with left concatenation and bar operation, the bracket on $\mathsf{S}^{\mathbf{sym}}$ induces a welldefined bracket on the group $\widetilde{B}_\infty$ (as well as on any further quotient of $\widetilde{B}_\infty$ whenever the compatibility with left concatenation holds).

Definition.- The subgroup of $\widetilde{B}_\infty$ generated by all $\widetilde{\sigma}_w$ where w begins with 0 (*resp.* with 1) will be denoted H_0 (*resp.* H_1).

By the previous lemma, the bracket on $\widetilde{B}_\infty$ induces a welldefined bracket on the set of right cosets $\widetilde{B}_\infty/H_0$, and this bracket is left distributive. One obtains an 'algebraic' translation of the Irreflexivity Conjecture in $\widetilde{B}_\infty$ as follows.

Proposition 4.- *Assume that for $k \geq 1$ the subgroup H_0 does not intersect the set $(H_1.\widetilde{\sigma}_\Lambda)^k.H_1$. Then the Irreflexivity Conjecture is true.*

Proof. By 1.6 it suffices to show that the closure of H_0 in $\widetilde{B}_\infty/H_0$ under bracket is an irreflexive LD-magma. This closure is the image of $\mathcal{T}_{\boldsymbol{x}}$ under the mapping

$$\varphi : P \mapsto \widetilde{\sigma}(\widetilde{\chi}_P)H_0,$$

so the point is to prove $\varphi(P) \neq \varphi(Q)$, *i.e.*

$$\widetilde{\sigma}(\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q) \notin H_0,$$

whenever Q is $P[Q_1]\ldots[Q_k]$. The explicit value of $\overline{\widetilde{\chi}_P}\bullet\widetilde{\chi}_Q$ in the latter case is

$$1\widetilde{\chi}_{Q_1} \bullet \Lambda \bullet \overline{1\widetilde{\chi}_P} \bullet 1\widetilde{\chi}_{Q_2} \bullet \Lambda \bullet \overline{1\widetilde{\chi}_{P[Q_1]}} \bullet \ldots \bullet 1\widetilde{\chi}_{Q_k} \bullet \Lambda \bullet \overline{1\widetilde{\chi}_{P[Q_1]\ldots[Q_{k-1}]}},$$

hence $\widetilde{\sigma}(\overline{\widetilde{\chi}_P}\bullet\widetilde{\chi}_Q)$ belongs to the set $(H_1.\widetilde{\sigma}_\Lambda)^k.H_1$. ■

In order to establish the condition above, we shall use more geometrical properties of left distributivity, namely the ones involved in Lemma 1.4. The idea is that the exponent of the iterated left subterm which appears in this lemma can be computed effectively using only the classes in $\widetilde{B}_\infty$. In the sequel we use the free submonoid S^* of $\mathsf{S}^{\mathbf{sym}}$ generated by S. The elements of S^* will be refered to as positive sequences. Let us call *LD-pairs* the pairs of the forms $\{u\bullet u1\bullet u, u1\bullet u\bullet u1\bullet u0\}$, $\{u\bullet u11v, u11v\bullet u\}$, $\{u\bullet u10v\bullet u00v, u0v\bullet u\}$, $\{u\bullet u01v, u10v\bullet u\}$, $\{u0v\bullet u1w, u1w\bullet u0v\}$. We denote by $\widetilde{\equiv}^+$ the congruence on S^* generated by all LD-pairs. Then $\widetilde{\equiv}$ is the congruence generated by $\widetilde{\equiv}^+$ together with all pairs $\{x\bullet\overline{x}, \varepsilon\}$ and $\{\overline{x}\bullet x, \varepsilon\}$ for x in S, but there is no *a priori* reason why $\widetilde{\equiv}^+$ should coincide with the restriction of $\widetilde{\equiv}$ to S^*.

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

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

$$\mathrm{Dil}(p,w)=\begin{cases} p+1 & \text{if } (\exists i<p)(w=0^i),\\ p & \text{otherwise;}\end{cases} \quad \mathrm{Tr}^p(w)=\begin{cases} v & \text{if } w=0^p v,\\ \varepsilon & \text{if } 0^p \text{ is not a prefix of } w;\end{cases}$$

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

An immediate induction shows that for every sequence X the successive values of $\mathrm{Dil}(p,X)$ make a strictly increasing sequence, and in particular $\mathrm{Dil}(p,X)$ is always at least p. Observe that $\mathrm{Tr}^0(X)$ is always X, and $\mathrm{Dil}(0,X)$ is always 0. The geometrical intuition for these notions are given by the following effective version of Lemma 1.4.

Lemma 5.- *Assume that X is a positive sequence and that $\Omega(X)$ maps P to Q. Assume moreover that $\mathbf{S}^p_L(P)$ exists, or that $\mathbf{S}^{\mathrm{Dil}(p,X)}_L(Q)$ exists, or that $\mathrm{Tr}^p(X)$ is nonempty. Then $\Omega(\mathrm{Tr}^p(X))$ maps $\mathbf{S}^p_L(P)$ to $\mathbf{S}^{\mathrm{Dil}(p,X)}_L(Q)$.*

Proof. Use induction on the length of X, and distinguish the various possible cases when X is just a point in 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 S^* the equalities

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

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

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

The main result about dilatation and trace is the following compatibility with the congruence $\widetilde{\equiv}^+$. This expresses a connection with the projection on $\widetilde{B}_\infty$, to be compared with the compatibility with the projection on G_{LD} claimed in Lemma 5.

Lemma 6.- *Assume that X, Y are positive sequences and $X\ \widetilde{\equiv}^+\ Y$ holds. Then the formulas*

$$\mathrm{Dil}(p,X)=\mathrm{Dil}(p,Y), \qquad \mathrm{Tr}^p(X)\ \widetilde{\equiv}^+\ \mathrm{Tr}^p(Y)$$

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. ■

In the sequel, we write $\mathrm{dil}(X)$ for $\mathrm{Dil}(1, X)$. We observed that, for any terms P, Q, the operator $\Omega(\overline{\widetilde{\chi}_P}\bullet\widetilde{\chi}_Q)$ maps the term $P[\mathbf{x}^{[n]}]$ to the term $Q[\mathbf{x}^{[n]}]$. By Lemma 1.3, we know that these terms have a common extension R, so that there must exist positive sequences X, Y in S^* such that the operators $\Omega(X)$ and $\Omega(Y)$ map $P[\mathbf{x}^{[n]}]$ and $Q[\mathbf{x}^{[n]}]$ respectively to R, and therefore the operator $\Omega(X\bullet\overline{Y})$ maps $P[\mathbf{x}^{[n]}]$ to $Q[\mathbf{x}^{[n]}]$. Assume that the sequences $\overline{\widetilde{\chi}_P}\bullet\widetilde{\chi}_Q$ and $X\bullet\overline{Y}$ are $\widetilde{\equiv}$-equivalent. Lemma 2 indicates that $\mathbf{S}_L^{\mathrm{dil}(X)}(R)$ is an extension of P, and $\mathbf{S}_L^{\mathrm{dil}(Y)}(R)$ is an extension of Q. So if the Irreflexivity Conjecture is true, the equality $\mathrm{dil}(X) = \mathrm{dil}(Y)$ holds exactly if and only if the terms P and Q are $\approx_{LD}$-equivalent. The previous argument is far from complete, but it suggests to compare terms P, Q by writing $\overline{\widetilde{\chi}_P}\bullet\widetilde{\chi}_Q$ as the quotient of two positive sequences and to compare the associated dilatations. The algebraic hypotheses which are needed for making this scheme correct are easily formulated.

Definition.- Assume that $\simeq$ and $\simeq^+$ are congruences respectively on $\mathrm{X}^{\mathbf{sym}}$ and X^*. We say that the pair $(\simeq, \simeq^+)$ has the *right quotient property* if every sequence ξ in $\mathrm{X}^{\mathbf{sym}}$ is $\simeq$-equivalent to a quotient $X\bullet\overline{Y}$ of positive sequences, and if moreover there exists positive sequences Z, Z' satisfying

$$X \bullet Z \simeq^+ X' \bullet Z' \ , \qquad Y \bullet Z \simeq^+ Y' \bullet Z'$$

whenever the positive sequences X, Y, X', Y' satisfy $X\bullet\overline{Y} \simeq X'\bullet\overline{Y'}$.

Proposition 7.- *Assume that the pair $(\widetilde{\equiv}, \widetilde{\equiv}^+)$ has the right quotient property. Then the Irreflexivity Conjecture is true.*

Proof. Define the sign of an element x of $\widetilde{B}_\infty$ as the sign (with value in $\{-1, 0, +1\}$) of the difference $\mathrm{dil}(X) - \mathrm{dil}(Y)$ where X, Y are positive sequences satisfying $x = \widetilde{\sigma}(X\bullet\overline{Y})$. This makes sense because such expressions are supposed to exist, and the right quotient property gives the independence from the choice of the decomposition. Indeed if $X\bullet\overline{Y}$ and $X'\bullet\overline{Y'}$ are $\widetilde{\equiv}$-equivalent, there exist Z, Z' satisfying

$$X \bullet Z \mathrel{\widetilde{\equiv}^+} X' \bullet Z' \ , \qquad Y \bullet Z \mathrel{\widetilde{\equiv}^+} Y' \bullet Z',$$

so one obtains

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

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

Now we observe that, for positive sequences X, Y, $X \mathrel{\widetilde{\equiv}} Y$ holds if and only if $X \bullet Z \mathrel{\widetilde{\equiv}}^+ Y \bullet Z$ holds for some positive sequence Z. Indeed $X \mathrel{\widetilde{\equiv}} Y$ implies $X \bullet \overline{Y} \mathrel{\widetilde{\equiv}} \varepsilon$, and there must exist Z, Z' satisfying $X \bullet Z \mathrel{\widetilde{\equiv}}^+ Z'$ and $Y \bullet Z \mathrel{\widetilde{\equiv}}^+ Z'$. It follows that, for any positive sequences Y, Z, there must exist (positive) sequences Y', Z' satisfying $Y \bullet Y' \mathrel{\widetilde{\equiv}}^+ Z \bullet Z'$. Indeed there exist Y'', Z'' satisfying $\overline{Y} \bullet X \mathrel{\widetilde{\equiv}} Y'' \bullet \overline{Z''}$, hence $Y \bullet Y'' \mathrel{\widetilde{\equiv}} Z \bullet Z''$, and, by the previous remark, one has $Y \bullet Y'' \bullet X \mathrel{\widetilde{\equiv}}^+ Z \bullet Z'' \bullet X$ for some positive sequence X.

Let ξ be an arbitrary sequence and w a point in S. We compare the signs of $\widetilde{\sigma}(\xi)$ and $\widetilde{\sigma}(\xi \bullet w)$. Choose positive sequences X, Y, Y', Z satisfying

$$\xi \mathrel{\widetilde{\equiv}} X \bullet \overline{Y} \quad \text{and} \quad Y \bullet Y' \mathrel{\widetilde{\equiv}}^+ w \bullet Z.$$

One has $\xi \bullet w \mathrel{\widetilde{\equiv}} X \bullet Y' \bullet \overline{Z}$, so the sign of $\widetilde{\sigma}(\xi \bullet w)$ is determined by the comparison of the integers $\mathrm{dil}(X \bullet Y')$ and $\mathrm{dil}(Z)$. One finds

$$\mathrm{dil}(Z) \begin{cases} = \mathrm{Dil}(1, Z) = \mathrm{dil}(w \bullet Z) = \mathrm{dil}(Y \bullet Y') & \text{if } w \neq \Lambda, \\ < \mathrm{Dil}(2, Z) = \mathrm{dil}(w \bullet Z) = \mathrm{dil}(Y \bullet Y') & \text{if } w = \Lambda. \end{cases}$$

If w is not Λ, the sign of $\widetilde{\sigma}(X \bullet Y' \bullet \overline{Z})$ is the sign of $\widetilde{\sigma}(X \bullet Y' \bullet \overline{Y'} \bullet \overline{Y})$, *i.e.* $\widetilde{\sigma}(\xi \bullet w)$ and $\widetilde{\sigma}(\xi)$ have the same sign. If w is Λ, the sign of $\widetilde{\sigma}(X \bullet Y' \bullet \overline{Z})$ is $+1$ whenever $\mathrm{dil}(X \bullet Y') \geq \mathrm{dil}(Y \bullet Y')$ holds. This means that $\widetilde{\sigma}(\xi \bullet w)$ has sign $+1$ whenever the sign of $\widetilde{\sigma}(\xi)$ is 0 or $+1$. It follows that the sign of any element in H_0 is 0, while the sign of any element in $(H_1 . \widetilde{\sigma}(\Lambda))^k . H_1$ is $+1$ whenever k is positive, and therefore these sets are disjoint. ■

The proof of right quotient property for the pair $(\mathrel{\widetilde{\equiv}}, \mathrel{\widetilde{\equiv}}^+)$ will be the task of the next sections.

3. Groups with complemented presentations.

The presentation used to define the group $\widetilde{B}_\infty$ has some specific syntactical properties. In particular the *LD*-pairs which generate it only involve positive sequences, and moreover for every u, v in S, positive sequences X, Y exist such that $\{u \bullet X, v \bullet Y\}$ is an *LD*-pair. We establish in this section a criterion for proving the right quotient property for such types of congruences. The method developed below is close to Garside's analysis of the braid broups [12], and turns out to be a variant of Thurston's approach in [23].

Throughout this section we assume that X is any set and that $\simeq$ is a congruence on $\mathrm{X}^{\mathbf{sym}}$ such that $\mathrm{X}^{\mathbf{sym}}/\simeq$ is a group.

Definition.- Assume that f is a mapping of X^2 to X^* such that $f(x,x)$ is ε for x in X. We say that f is a *right complement* for $\simeq$ if the pairs $\{x\bullet f(y,x), y\bullet f(x,y)\}$ with x, y in X generate $\simeq$ when completed with all pairs $\{x\bullet\overline{x},\varepsilon\}$ and $\{\overline{x}\bullet x,\varepsilon\}$.

Example. A typical example of a congruence admitting a right complement is the braid congruence $\equiv$ on the set of positive integers. The complement $\boldsymbol{c}_R$ is defined by

$$\boldsymbol{c}_R(i,j)=\begin{cases} i & \text{if } |i-j|\geq 2,\\ i\bullet j & \text{if } |i-j|=1,\\ \varepsilon & \text{if } i=j.\end{cases}$$

We assume in the sequel that the congruence $\simeq$ admits the mapping f as a right complement. We denote by $\simeq^+$ the congruence on X^* generated by the pairs $\{x\bullet f(y,x), y\bullet f(x,y)\}$. Clearly $\simeq^+$ is a refinement of the restriction of $\simeq$ to positive sequences. By definition the monoid $\mathrm{X}^*/\simeq^+$ admits the following weak form of right regularity

$$(\forall x,y\in \mathrm{X})(\exists X,Y\in \mathrm{X}^*)(x\bullet X\simeq^+ y\bullet Y).$$

We try to extend this property to arbitrary positive sequences. A simple iteration is not sufficient in general, for the termination of the process is problematic whenever the length of the complement $f(x,y)$ may be bigger than 1. Nevertheless the iteration, when it terminates, leads to a welldefined unique result.

Definition.- For ξ, η in $\mathrm{X}^{\mathbf{sym}}$, say that ξ is 1-*reducible to* η (on the right and w. r. to f) if there are two elements x, y of X and sequences ξ', ξ'' satisfying

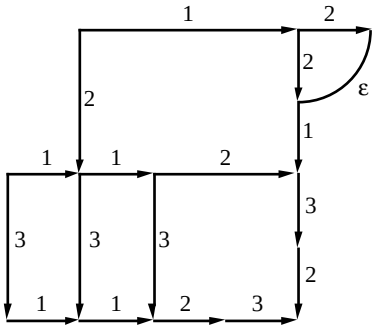
$$\xi=\xi'\bullet x\bullet\overline{y}\bullet\xi''\ ,\qquad \eta=\xi'\bullet\overline{f(y,x)}\bullet f(x,y)\bullet\xi''.$$

The sequence ξ is p-reducible to η if there is a length $p+1$ sequence from ξ to η such that each term is 1-reducible to the next one.

Lemma 1.- *Assume that the sequence ξ is p-reducible to η and q-reducible to $Y\bullet\overline{Z}$, where Y, Z are positive sequences. Then $p\leq q$ holds and η is $(q-p)$-reducible to $Y\bullet\overline{Z}$.*

Proof. First we observe that, if ξ is 1-reducible to η and ζ, there must exist a sequence ξ' and an integer $p'\leq 1$ such that both η and ζ are p'-reducible to ξ' (where 0-reducibility means equality). Then an induction on $p+q$ shows that, if ξ is p-reducible to η and q-reducible to ζ, then there exists a sequence ξ' and integers $p'\leq q$, $q'\leq p$ such that $p'+q'=p+q$ holds, η is p'-reducible to ξ' and ζ is q'-reducible to ξ'. Now assume the hypothesis of the lemma. There must exist a sequence ξ' and integers p', q' with $p+p'=q+q'$ such that η is p'-reducible to ξ' and $Y\bullet\overline{Z}$ is q'-reducible to ξ'. But a sequence $Y\bullet\overline{Z}$ is necessarily terminal with respect to reduction, so q' is 0, ξ' is equal to $Y\bullet\overline{Z}$ and p' is $q-p$. ■

Reduction can be illustrated using the Cayley diagram, an oriented graph where the edges wear labels in X. A sequence in $\mathrm{X}^{\mathbf{sym}}$ is associated with every (unoriented) path in the graph by concatening the successive labels of its edges, with the convention that the edge labelled x contributes x when gone over according to its orientation and $\overline{x}$ in the opposite case. If the sequence ξ reduces to η, the welldefined number p such that ξ is p-reducible to η holds is the number of connected domains in the associated Cayley diagram. The figure below illustrates the reduction of $\overline{3}\bullet 1\bullet\overline{2}\bullet 1\bullet 2$ to $1\bullet 1\bullet 2\bullet 3\bullet\overline{2}\bullet\overline{3}\bullet\overline{1}$ using the braid complement $\boldsymbol{c}_R$.



Reduction can be used to construct both $\simeq$-equivalent sequences in $\mathrm{X}^{\mathbf{sym}}$ and $\simeq^+$-equivalent sequences in X^*. The following lemma shows that two paths in the Cayley diagram with the same ends must be $\simeq$-equivalent, and even $\simeq^+$-equivalent if all edges are gone over positively.

Lemma 2.- If the sequence ξ reduces to η, then $\xi \simeq \eta$ holds. If X, Y, X', Y' are positive sequences and $\overline{X}\bullet Y$ reduces to $X'\bullet\overline{Y'}$, then $X\bullet X' \simeq^+ Y\bullet Y'$ holds.

Proof. The first point follows from an easy induction since $x\bullet\overline{y}$ is $\simeq$-equivalent to $\overline{f(y,x)}\bullet f(x,y)$ for every x, y in X. For the second point use induction on the length of the reduction. ■

Definition.- i) For ξ in $\mathrm{X}^{\mathbf{sym}}$, we say that ξ is *fully reducible* (on the right and with respect to f) if there exist positive sequences Y, Z such that ξ reduces to $Y\bullet\overline{Z}$. These (unique) positive sequences will be called respectively, if they exist, the *(right) numerator* and *(right) denominator* of ξ (with respect to f) and denoted by $\mathbf{N}_f(\xi)$ and $\mathbf{D}_f(\xi)$. The complement mapping f is *convergent* if every sequence is fully reducible with respect to f.
ii) For ξ, η in $\mathrm{X}^{\mathbf{sym}}$, the *(right) complement* of ξ in η, written $\mathbf{C}_f(\xi,\eta)$, is the numerator of $\overline{\eta}\bullet\xi$, and the *(right) join* of ξ and η, written $\mathbf{J}_f(\xi,\eta)$, is the sequence $\xi\bullet\mathbf{C}_f(\eta,\xi)$ (if they exist).

With these notations the equivalence

$$\xi \simeq \mathbf{N}_f(\xi) \bullet \overline{\mathbf{D}_f(\xi)}$$

holds for all fully reducible sequences ξ. Every positive sequence is fully reducible and its denominator is empty.

Lemma 3.- *i) For ξ in $\mathrm{X}^{\mathbf{sym}}$, ξ is fully reducible if and only if $\overline{\xi}$ is fully reducible if and only if $\mathbf{C}_f(\xi,\varepsilon)$ and $\mathbf{C}_f(\varepsilon,\xi)$ exist. In this case one has*

$$\mathbf{N}_f(\xi) = \mathbf{D}_f(\overline{\xi}) = \mathbf{C}_f(\xi,\varepsilon)\ , \qquad \mathbf{D}_f(\xi) = \mathbf{N}_f(\overline{\xi}) = \mathbf{C}_f(\varepsilon,\xi).$$

ii) For ξ, η in $\mathrm{X}^{\mathbf{sym}}$, $\mathbf{C}_f(\xi,\eta)$ exists if and only if ξ, η and $\overline{\mathbf{N}_f(\eta)}\bullet\mathbf{N}_f(\xi)$ are fully reducible. In this case $\mathbf{C}_f(\xi,\eta)$ exists and is equal to $\mathbf{D}_f(\eta)\bullet\mathbf{C}_f(\mathbf{N}_f(\xi),\mathbf{N}_f(\eta))$. Moreover one has

$$\mathbf{J}_f(\xi,\eta) \simeq \mathbf{J}_f(\eta,\xi),$$

and, in the case of positive sequences X, Y, even

$$\mathbf{J}_f(X,Y) \simeq^{+} \mathbf{J}_f(Y,X).$$

For x, y in X, $\mathbf{C}_f(x,y)$ exists and is equal to $f(x,y)$.
iii) For ξ, η, ζ in $\mathrm{X}^{\mathbf{sym}}$, $\mathbf{C}_f(\xi,\eta\bullet\zeta)$ exists if and only if $\mathbf{C}_f(\xi,\eta)$ and $\mathbf{C}_f(\mathbf{C}_f(\xi,\eta),\zeta)$ exist. In this case one has

$$\mathbf{C}_f(\xi,\eta\bullet\zeta) = \mathbf{C}_f(\mathbf{C}_f(\xi,\eta),\zeta)\ , \qquad \mathbf{C}_f(\eta\bullet\zeta,\xi) = \mathbf{C}_f(\eta,\xi)\bullet\mathbf{C}_f(\zeta,\mathbf{C}_f(\xi,\eta)).$$

Proof. Use induction on the lengths of the sequences and the fact that any subsequence of a fully reducible sequence must be fully reducible. ■

The full reducibility of a sequence in $\mathrm{X}^{\mathbf{sym}}$ expresses the existence of a decomposition as a quotient of positive sequences, which is the first part in the right quotient property of the pair $(\simeq,\simeq^{+})$. For the second part we need stronger assumptions. The existence of a complement mapping for the congruence $\simeq$ is a rather weak hypothesis which becomes interesting only when some compatibility is assumed between the congruence $\simeq^{+}$ and the complement mapping itself viewed as a binary operation on positive sequences. The nice point is that the most elementary occurrence of this compatibility turns out to be a sufficient condition in good cases.

Lemma 4.- *The following are equivalent*

i) for every positive sequence X, the lengths of the X' in X^* satisfying $X \simeq^{+} X'$ have a finite upper bound;

ii) there exists a $\simeq^{+}$-invariant mapping ν of X^* to the natural numbers such that $\nu(X\bullet Y) \geq \nu(X) + \nu(Y)$ holds for every X, Y and $\nu(x)$ is positive for every x in X.

The proof is immediate. A mapping as in (ii) above will be called a *norm* for $\simeq^+$.

Definition.- The mapping f is *coherent* (on the right) if for every x, y, z in X, the sequences

$$\mathbf{C}_f(f(x,y),f(z,y)) \text{ and } \mathbf{C}_f(f(x,z),f(y,z))$$

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

The following criterion is reminiscent of the one used in [12] to establish left cancellativity for the monoid of positive braids.

Lemma 5.- *Assume that f is coherent and the congruence $\simeq^+$ is normed. Then for every sequences X, Y, X', Y' in X^*, the following are equivalent*

i) $X\bullet X' \simeq^+ Y\bullet Y'$ holds,

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

$$X' \simeq^+ \mathbf{C}_f(Y,X)\bullet Z\ , \qquad Y' \simeq^+ \mathbf{C}_f(X,Y)\bullet Z$$

are satisfied.

Proof. By Lemma 3.ii, the second point implies the first one. Assume now that $\mathbf{C}_f$ is coherent and ν is a $\simeq^+$-norm on X^*. Write $X \simeq^+_1 Y$ if either X is equal to Y or Y is obtained from X by replacing exactly one subsequence $x\bullet f(y,x)$ by the corresponding pattern $y\bullet f(x,y)$. For $p \le \infty$ the p-th power of $\simeq^+_1$ is denoted by $\simeq^+_p$. For k, n, p in $\mathbf{N}\cup\{\infty\}$ let $\mathcal{S}^k_{n,p}$ be the following statement

"Assume $X\bullet X' \simeq^+_p Y\bullet Y'$, $\nu(X\bullet X') \le n$, $\nu(X) \le k$ and $\nu(Y) \le k$. Then $\mathbf{C}_f(X,Y)$ and $\mathbf{C}_f(Y,X)$ exist, and some Z in X^* satisfies $X' \simeq^+ \mathbf{C}_f(Y,X)\bullet Z$ and $Y' \simeq^+ \mathbf{C}_f(X,Y)\bullet Z$."

We observe that $\mathcal{S}^\infty_{0,\infty}$ is true since the empty sequence ε is the only positive sequence with norm 0. The statement $\mathcal{S}^1_{\infty,1}$ is a consequence of the definition of a complement mapping. Then one shows inductively on $p \ge 1$ that the conjunction of $\mathcal{S}^\infty_{n,\infty}$ and $\mathcal{S}^1_{n+1,1}$ implies $\mathcal{S}^1_{n+1,p}$ for every p, and therefore $\mathcal{S}^1_{n+1,\infty}$. The coherence of f is used in each step of this induction. Finally one shows inductively on $k \ge 1$ that the conjunction of $\mathcal{S}^\infty_{n,\infty}$ and $\mathcal{S}^1_{n+1,\infty}$ implies $\mathcal{S}^\infty_{n+1,k}$ for every k, and therefore $\mathcal{S}^\infty_{n+1,\infty}$. The existence of the norm and the formulas of Lemma 3.iii are used. Because $\mathcal{S}^1_{n+1,1}$ is true, $\mathcal{S}^\infty_{n,\infty}$ implies $\mathcal{S}^1_{n+1,\infty}$, and therefore $\mathcal{S}^\infty_{n+1,\infty}$. So since $\mathcal{S}^\infty_{1,\infty}$ is true, $\mathcal{S}^\infty_{\infty,\infty}$ certainly holds, which is the desired conclusion. ■

For positive sequences X, Y, say that X *divides* Y (on the right) if $X \simeq^+ Y\bullet Z$ holds for some (positive) sequence Z.

Lemma 6.- *Assume that f is coherent and the congruence $\simeq^+$ is normed.*
i) For every X, Y in X^*, $X \simeq^+ Y$ holds if and only if $\mathbf{C}_f(X,Y)$ and $\mathbf{C}_f(Y,X)$ both exist and are empty i.e. if and only if $\overline{X}\bullet Y$ reduces to ε.
ii) For every X, Y, Z in X^*, $Z\bullet X \simeq^+ Z\bullet Y$ implies $X \simeq^+ Y$.
iii) If X divides Y and Y divides X, then $X \simeq^+ Y$ holds. The join $\mathbf{J}_f(X,Y)$ is exactly a lower common multiple of X and Y.
iv) The congruence $\simeq^+$ is compatible with the binary operations $\mathbf{C}_f$ and $\mathbf{J}_f$.

Proof. (i) Assume $X \simeq^+ Y$. Then $X\bullet\varepsilon \simeq^+ Y\bullet\varepsilon$ holds as well, so by Lemma 5 the sequences $\mathbf{C}_f(X,Y)$ and $\mathbf{C}_f(Y,X)$ exist and some sequence Z satisfies $\varepsilon \simeq^+ \mathbf{C}_f(Y,X)\bullet Z \simeq^+ \mathbf{C}_f(X,Y)\bullet Z$. The only possibility is $\mathbf{C}_f(X,Y) = \mathbf{C}_f(Y,X) = Z = \varepsilon$. The converse is obvious.
(ii) Assume $Z\bullet X \simeq^+ Z\bullet Y$. Then for some Z', the sequences X and Y are $\simeq^+$-equivalent to $\mathbf{C}_f(Z,Z)\bullet Z'$ (*i.e.* to Z).
(iii) Assume $Y \simeq^+ X\bullet Z$ and $X \simeq^+ Y\bullet Z'$. One has $X \simeq^+ X\bullet Z'\bullet Z$, whence $\varepsilon \simeq^+ Z'\bullet Z$ by (ii). The existence of the norm implies $Z = Z' = \varepsilon$. Then the following version of Gauss' lemma holds: if X divides the product $Y\bullet Z$, then $\mathbf{C}_f(X,Y)$ exists and divides Z. Now assume that X and Y divide Z. Some X', Y' satisfy $Z \simeq^+ X\bullet X' \simeq^+ Y\bullet Y'$. By Lemma 5 some sequence Z' satisfies $X' \simeq^+ \mathbf{C}_f(Y,X)\bullet Z'$ and $Y' \simeq^+ \mathbf{C}_f(X,Y)\bullet Z'$, which implies

$$Z \simeq^+ X \bullet \mathbf{C}_f(Y,X) \bullet Z' = \mathbf{J}_f(X,Y) \bullet Z',$$

and $\mathbf{J}_f(X,Y)$ divides Z.
(iv) Assume that $X \simeq^+ X'$ holds and $\mathbf{C}_f(Y,X)$ exists. Then Y divides $X\bullet\mathbf{C}_f(Y,X)$, hence Y divides $X'\bullet\mathbf{C}_f(Y,X)$ as well. By 'Gauss' lemma' $\mathbf{C}_f(Y,X')$ exists and divides $\mathbf{C}_f(Y,X)$. By symmetry $\mathbf{C}_f(Y,X')$ must be $\simeq^+$-equivalent to $\mathbf{C}_f(Y,X)$. Similarly X divides $Y\bullet\mathbf{C}_f(X,Y)$. Hence so does X'. By Gauss' lemma again $\mathbf{C}_f(X',Y)$ exists, divides $\mathbf{C}_f(X,Y)$, and by symmetry, is $\simeq^+$-equivalent to $\mathbf{C}_f(X,Y)$. ■

Thus the operations $\mathbf{C}_f$ and $\mathbf{J}_f$ induce welldefined (partial) operations on the monoid $\mathrm{X}^*/\simeq^+$. If f is convergent one obtains using the projection of $\mathbf{J}_f$ a semilattice structure and $\mathbf{C}_f$ is distributive with respect to $\mathbf{J}_f$. It is now easy to express the algebraic properties we were looking for in terms of the complement mapping.

Proposition 7.- *i) Assume that the congruence $\simeq$ admits a coherent right complement mapping and that $\simeq^+$ is normed. Then the monoid $\mathrm{X}^*/\simeq^+$ admits left cancellation.*
ii) Assume moreover that the complement mapping is convergent. Then the monoid $\mathrm{X}^*/\simeq^+$ is right regular and the pair $(\simeq, \simeq^+)$ has the right quotient property.

Proof. Owing to Lemmas 5 and 6, only the last point remains to be proved. We use the above notations. We already observed that the existence assumption in the right quotient property is certainly satisfied whenever every sequence is fully reducible. In order to establish the uniqueness assumption write $(X,Y) \sim (X',Y')$ if some (positive) sequences Z, Z' satisfy

$$X \bullet Z \simeq^+ X' \bullet Z' \ , \qquad Y \bullet Z \simeq^+ Y' \bullet Z'.$$

Clearly $(X,Y) \sim (X',Y')$ implies $X \bullet \overline{Y} \simeq X' \bullet \overline{Y'}$. To establish the converse implication, we prove that $\xi \simeq \xi'$ implies

$$(\mathbf{N}_f(\xi), \mathbf{D}_f(\xi)) \sim (\mathbf{N}_f(\xi'), \mathbf{D}_f(\xi')).$$

This suffices to conclude since X and Y are respectively the numerator and denominator of $X \bullet \overline{Y}$. Now the relation $\sim$ is transitive because the monoid $\mathrm{X}^*/\simeq^+$ is right regular. So it suffices to establish the implication for a family of particular pairs $\{\xi, \xi'\}$ which generates $\simeq$ as an equivalence relation. We consider the pairs $\{\xi \bullet \eta \bullet \zeta, \xi \bullet \eta' \bullet \zeta\}$ where $\{\eta, \eta'\}$ is either a special pair, or a pair $\{\overline{y} \bullet y, \varepsilon\}$, or a pair $\{y \bullet \overline{y}, \varepsilon\}$ with y in X. In the first case, the compatibility of $\simeq^+$ with $\mathbf{C}_f$ and the formulas in Lemma 3 imply that the numerators of $\xi \bullet \eta \bullet \zeta$ and $\xi \bullet \eta' \bullet \zeta$ are $\simeq^+$-equivalent, and so are the denominators. In the second case, the sequence $\xi \bullet \eta' \bullet \zeta$ is 1-reducible to $\xi \bullet \eta \bullet \zeta$, so their numerators and denominators are respectively equal. For the third case, set $X = \mathbf{N}_f(\xi)$, $X' = \mathbf{D}_f(\xi)$, $Z = \mathbf{N}_f(\zeta)$, $Z' = \mathbf{D}_f(\zeta)$. By applying the formulas of Lemma 3 and the coherence of $\mathbf{C}_f$ one obtains

$$\begin{aligned}
\mathbf{N}_f(\xi \bullet y \bullet \overline{y} \bullet \zeta) &= X \bullet \mathbf{C}_f(y, X') \bullet (\mathbf{C}_f(\mathbf{C}_f(Z, y), \mathbf{C}_f(X', y)) \\
&\simeq^+ X \bullet \mathbf{C}_f(y, X') \bullet \mathbf{C}_f(\mathbf{C}_f(Z, X'), \mathbf{C}_f(y, X')) \\
&\simeq^+ X \bullet \mathbf{C}_f(Z, X') \bullet \mathbf{C}_f(\mathbf{C}_f(y, X'), \mathbf{C}_f(Z, X')) \\
&\simeq^+ \mathbf{N}_f(\xi \bullet \zeta) \bullet \mathbf{C}_f(\mathbf{C}_f(y, Z), \mathbf{C}_f(X', Z)) \\
\mathbf{D}_f(\xi \bullet y \bullet \overline{y} \bullet \zeta) &= Z' \bullet \mathbf{C}_f(y, Z) \bullet (\mathbf{C}_f(\mathbf{C}_f(X', y), \mathbf{C}_f(Z, y)) \\
&\simeq^+ Z' \bullet \mathbf{C}_f(y, Z) \bullet \mathbf{C}_f(\mathbf{C}_f(X', Z), \mathbf{C}_f(y, Z)) \\
&\simeq^+ Z' \bullet \mathbf{C}_f(X', Z) \bullet \mathbf{C}_f(\mathbf{C}_f(y, Z), \mathbf{C}_f(X', Z)) \\
&\simeq^+ \mathbf{D}_f(\xi \bullet \zeta) \bullet \mathbf{C}_f(\mathbf{C}_f(y, Z), \mathbf{C}_f(X', Z))
\end{aligned}$$

In the three cases one obtains

$$(\mathbf{N}_f(\xi \bullet \eta \bullet \zeta), \mathbf{D}_f(\xi \bullet \eta \bullet \zeta)) \sim (\mathbf{N}_f(\xi \bullet \eta' \bullet \zeta), \mathbf{D}_f(\xi \bullet \eta' \bullet \zeta)),$$

which completes the proof. ■

Further properties of the congruence $\simeq^+$ can be expressed in terms of the right complement when it exists. The following criterion for the embeddability of the monoid $\mathrm{X}^*/\simeq^+$ into a group follows the classical Ore's theorem.

Proposition 8.- *Assume that the congruence $\simeq$ admits a coherent and convergent right complement mapping f and that $\simeq^+$ is normed. Then the following are equivalent*

i) the monoid $\mathrm{X}^*/\simeq^+$ admits right cancellation;

ii) the congruence $\simeq^+$ is the restriction of $\simeq$ to X^*, and the monoid $\mathrm{X}^*/\simeq^+$ is (isomorphic to) the submonoid of $\mathrm{X}^{\mathbf{sym}}/\simeq$ generated by X;

iii) $\mathbf{C}_f(X,Y) \simeq^+ \mathbf{C}_f(Y,X)$ implies $\mathbf{C}_f(X,Y) = \mathbf{C}_f(Y,X) = \varepsilon$.

Moreover, if these conditions are satisfied, the word problem for $(\mathrm{X}^{\mathbf{sym}}, \simeq)$ is decidable.

Proof. The right quotient property for the pair $(\simeq, \simeq^+)$ immediately implies the equivalence of (i) and (ii). Now assume that X, Y are positive sequence and $\mathbf{C}_f(X,Y) \simeq^+ \mathbf{C}_f(Y,X)$ holds. Then one has

$$X \bullet \mathbf{C}_f(Y,X) \simeq^+ Y \bullet \mathbf{C}_f(X,Y) \simeq^+ Y \bullet \mathbf{C}_f(X,Y),$$

which implies $X \simeq^+ Y$ if right cancellation is allowed, and therefore $\mathbf{C}_f(X,Y) = \varepsilon$. Conversely assume $X \bullet Z \simeq^+ Y \bullet Z$. Define sequences X_n, Y_n by

$$X_0 = X, \quad Y_0 = Y, \quad X_{n+1} = \mathbf{C}_f(X_n, Y_n), \quad Y_{n+1} = \mathbf{C}_f(Y_n, X_n).$$

Starting from $Z_{-1} = X \bullet Z$, one obtains inductively by Lemma 5 positive sequences Z_n satisfying $Z_{n-1} \simeq^+ X_n \bullet Z_n \simeq^+ Y_n \bullet Z_n$. By the existence of a norm the sequences X_n and Y_n have to be empty for n large enough. Now if condition (iii) holds, then the equalities $X_{n+1} = Y_{n+1} = \varepsilon$ imply $X_n = Y_n = \varepsilon$ for $n \geq 1$. So one deduces $X_1 = Y_1 = \varepsilon$, which gives $X_0 \simeq^+ Y_0$, and right cancellation is allowed in $\mathrm{X}^*/\simeq^+$.

For the word problem of $(\mathrm{X}^{\mathbf{sym}}, \simeq)$, observe that, for any sequence ξ in $\mathrm{X}^{\mathbf{sym}}$, $\xi \simeq \varepsilon$ is equivalent to $\mathbf{N}_f(\xi) \simeq \mathbf{D}_f(\xi)$. If $\simeq^+$ is the restriction of $\simeq$ to positive sequences, the latter relation is equivalent to the fact that $\overline{\mathbf{D}_f(\xi)} \bullet \mathbf{N}_f(\xi)$ is reducible to ε. This gives an algorithmic method for deciding $\xi \simeq \varepsilon$ by means of a double reduction. ■

4. The complement mapping for $\widetilde{B}_\infty$.

We apply the method developed in the previous section to the case of the congruence $\widetilde{\equiv}$ which presents the group $\widetilde{B}_\infty$ as a quotient of $\mathrm{S}^{\mathbf{sym}}$. We say that a point x in S is a *prefix* of the point y if $y = xz$ holds for some z, and consider the mapping $\widetilde{\boldsymbol{c}}$ of S^2 to S^* defined by

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

Lemma 1.- *The mapping $\widetilde{\boldsymbol{c}}$ is a right complement for the congruence $\widetilde{\equiv}$, and is compatible with left concatenation in* S*: $\widetilde{\boldsymbol{c}}(wu, wv)$ is always equal to $w\widetilde{\boldsymbol{c}}(u, v)$.*

Proof. Easy from the examination of the LD-pairs. ■

In the sequel, we use the notations $\widetilde{\mathbf{N}}$, $\widetilde{\mathbf{D}}$, $\widetilde{\mathbf{C}}$, $\widetilde{\mathbf{J}}$ to refer to the right numerator, denominator, complement, join associated with the complement mapping $\widetilde{\boldsymbol{c}}$ on $\mathrm{S}^{\mathbf{sym}}$. In order to prove that the pair $(\widetilde{\equiv}, \widetilde{\equiv}^+)$ has the right quotient property, we have have to establish the three criteria of Proposition 3.7.

Lemma 2.- *The congruence $\widetilde{\equiv}^+$ is normed.*

Proof. We use the action of Ω on terms. Define the *size* of a term P as the number of nodes in P when viewed as a tree. If Z is any positive sequence in S^*, the transformation $\Omega(Z)$ strictly increases the size of each term in its domain. We know that $X \,\widetilde{\equiv}^+\, X'$ implies $\Omega(X) = \Omega(X')$, so for any X the lengths of the sequences X' which are $\widetilde{\equiv}^+$-equivalent to X are bounded by the difference between the sizes of the terms Q and P where (P, Q) is any pair of terms such that $\Omega(X)$ maps P to Q. ■

Proposition 3.- *The complement mapping $\widetilde{\boldsymbol{c}}$ is coherent.*

Proof. This is a brute force verification. For all possible mutual positions of the points u, v, w in S, we have to verify the existence and $\widetilde{\equiv}^+$-equivalence of the sequences $\widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(u, v), \widetilde{\boldsymbol{c}}(w, v))$ and $\widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(u, w), \widetilde{\boldsymbol{c}}(v, w))$ by reducing the corresponding sequences. The number of different cases is very large, but many cases are easy (for instance if at least two points are equal) and some symmetry can be used to remove some patterns. If one point is prefix-incomparable with the greatest common prefix of the other two ones, the sequences above are quickly shown to be equal. The serious case is when one point is a prefix of the greatest common prefix of the other ones. Owing to the compatibility of $\widetilde{\boldsymbol{c}}$ (and therefore of $\widetilde{\mathbf{C}}$) with left concatenation, one can assume that the first point is Λ. We shall not give the details. It turns out that the critical case is (not surprinsingly) the case of the triple $(\Lambda, 1, 11)$ and its permutations. The explicit values are

$$\begin{cases} \widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(\Lambda, 1), \widetilde{\boldsymbol{c}}(11, 1)) = \widetilde{\mathbf{C}}(\Lambda \bullet 1 \bullet 0, 11 \bullet 1) = \Lambda \bullet 1 \bullet 0 \bullet 11 \bullet 01 \bullet 10 \bullet 00 \\ \widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(\Lambda, 11), \widetilde{\boldsymbol{c}}(1, 11)) = \widetilde{\mathbf{C}}(\Lambda, 1 \bullet 11 \bullet 10) = \Lambda \bullet 1 \bullet 11 \bullet 10 \bullet 0 \bullet 01 \bullet 00 \end{cases}$$

are the equivalence is easy. Similarly one obtains

$$\begin{cases} \widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(1, 11), \widetilde{\boldsymbol{c}}(\Lambda, 11)) = \widetilde{\mathbf{C}}(1 \bullet 11 \bullet 10, \Lambda) = 1 \bullet \Lambda \bullet 11 \bullet 1 \bullet 01 \bullet 0 \\ \widetilde{\mathbf{C}}(\widetilde{\boldsymbol{c}}(1, \Lambda), \widetilde{\boldsymbol{c}}(11, \Lambda)) = \widetilde{\mathbf{C}}(1 \bullet \Lambda, 11) = 1 \bullet 11 \bullet 10 \bullet \Lambda \bullet 1 \bullet 0 \end{cases}$$

with the same conclusion. ■

It follows that Proposition 3.7 applies to the monoid $\mathrm{S}^*/\widetilde{\equiv}^+$, which therefore admits left cancellation (a property which was quoted as the missing part in the 'natural' attempts to prove the Irreflexivity Conjecture using the monoid C^+_{LD}).

We observed that the braid group B_∞ is a quotient of the group $\widetilde{B}_\infty$ by comparing their presentations using the congruences $\equiv$ and $\widetilde{\equiv}$. This compatibility extends to the complement mappings.

Lemma 4.- *The projection $\flat$ is an homomorphism with respect to $\widetilde{\boldsymbol{c}}$ and $\boldsymbol{c}_R$.*

Proof. A simple verification. ■

It follows that the complement $\boldsymbol{c}_R$ is coherent, and that the pair $(\equiv^+, \equiv)$ has the right quotient property (the equivalence $\equiv^+$ on positive braid words is certainly normed since it merely preserves the lengths of the sequences). This corresponds to the proof of left cancellability in the monoid B^+_∞ of positive braids given in [12]. For every sequence ξ in $\mathrm{S}^{\mathbf{sym}}$, the $\boldsymbol{c}_R$-reduction of $\xi^\flat$ is the projection of the $\widetilde{\boldsymbol{c}}$-reduction of ξ. So using the notations $\mathbf{N}_R$, $\mathbf{D}_R$, $\mathbf{C}_R$, $\mathbf{J}_R$ for the (right) numerator, denominator, complement, join associated with $\boldsymbol{c}_R$, we have the following formulas (when the sequences are fully reducible for $\widetilde{\boldsymbol{c}}$, which will be proved to always happen in Section 6)

$$(\widetilde{\mathbf{N}}(\xi))^\flat = \mathbf{N}_R(\xi^\flat) \qquad (\widetilde{\mathbf{D}}(\xi))^\flat = \mathbf{D}_R(\xi^\flat),$$
$$(\widetilde{\mathbf{C}}(\xi,\eta))^\flat = \mathbf{C}_R(\xi^\flat,\eta^\flat) \qquad (\widetilde{\mathbf{J}}(\xi,\eta))^\flat = \mathbf{J}_R(\xi^\flat,\eta^\flat).$$

The braids relations are reversible. So, if we introduce the symmetric notion of a left complement by using the pairs $\{f(y,x)\bullet x, f(x,y)\bullet x\}$ instead of the pairs $\{x\bullet f(y,x), y\bullet f(x,y)\}$ in the definition, the congruence $\equiv$ must admit a left complement $\boldsymbol{c}_L$ as well. This left complement is defined by

$$\boldsymbol{c}_L(i,j) = \begin{cases} i & \text{if } |i-j| \geq 2, \\ j \bullet i & \text{if } |i-j| = 1, \\ \varepsilon & \text{if } i = j. \end{cases}$$

We shall denote by $\mathbf{N}_L$, $\mathbf{D}_L$, $\mathbf{C}_L$, $\mathbf{J}_L$ the operations associated with left reductions using $\boldsymbol{c}_L$. By [12] (or anticipating the results of Section 6), the monoid B^+_∞ is regular, hence every braid word α is fully reducible (on the left and on the right). The pair $(\equiv, \equiv^+)$ has both the right and the left quotient properties (with the obvious definition of the latter notion), and the following formulas are satisfied

$$\alpha \equiv \mathbf{N}_R(\alpha) \bullet \overline{\mathbf{D}_R(\alpha)} \equiv \overline{\mathbf{D}_L(\alpha)} \bullet \mathbf{N}_L(\alpha),$$
$$\mathbf{N}_L(\alpha^{\mathbf{rev}}) = (\mathbf{N}_R(\alpha))^{\mathbf{rev}}, \qquad \mathbf{D}_L(\alpha^{\mathbf{rev}}) = (\mathbf{D}_R(\alpha))^{\mathbf{rev}},$$

where $\gamma^{\mathbf{rev}}$ denotes the sequence obtained from γ by reversing the order of all factors. The above decompositions of braid words as quotients of positive sequences need not be unique: $\equiv$-equivalent sequences need not to have $\equiv^+$-equivalent numerators and denominators. But when both reductions are combined, one obtains an intrinsic decomposition. For α in $\mathrm{N}_+^{\mathbf{sym}}$ set

$$\begin{cases} \mathbf{N}_{LR}(\alpha) = \mathbf{N}_L(\mathbf{N}_R(\alpha)\overline{\mathbf{D}_R(\alpha)}), \\ \mathbf{D}_{LR}(\alpha) = \mathbf{D}_L(\mathbf{N}_R(\alpha)\overline{\mathbf{D}_R(\alpha)}). \end{cases}$$

Proposition 5.- *Every braid word α satisfies $\alpha \equiv \overline{\mathbf{D}_{LR}(\alpha)}\bullet\mathbf{N}_{LR}(\alpha)$, and the classes of $\mathbf{N}_{LR}(\alpha)$ and $\mathbf{D}_{LR}(\alpha)$ in B_∞^+ only depend on the class of α in B_∞.*

Proof. Because the pair $(\equiv, \equiv^+)$ has the right quotient property, we know that, if α and α' are $\simeq$-equivalent, there exist positive sequences Z, Z' satisfying

$$\mathbf{N}_R(\alpha) \bullet Z \equiv^+ \mathbf{N}_R(\alpha') \bullet Z' \quad \text{and} \quad \mathbf{D}_R(\alpha) \bullet Z \equiv^+ \mathbf{D}_R(\alpha') \bullet Z'.$$

By definition of the left reduction, one has

$$\begin{aligned} \mathbf{N}_L(\mathbf{N}_R(\alpha) \bullet \overline{\mathbf{D}_R(\alpha)}) &= \mathbf{N}_L(\mathbf{N}_R(\alpha) \bullet Z \bullet \overline{Z} \bullet \overline{\mathbf{D}_R(\alpha)}) \\ &\equiv^+ \mathbf{N}_L(\mathbf{N}_R(\alpha') \bullet Z' \bullet \overline{Z'} \bullet \overline{\mathbf{D}_R(\alpha')}) \\ &= \mathbf{N}_L(\mathbf{N}_R(\alpha') \bullet \overline{\mathbf{D}_R(\alpha')}), \end{aligned}$$

and a similar relation holds for denominators. ■

The previous result can be applied to extend to arbitrary braid words any normal form defined for positive braid words (such as the ones described in [10] or [23]). But alternatively it can be used to describe an algorithm for comparing braid words without using any type of normal form (this suggests that the method could be proved to be optimal in some sense).

Proposition 6.- *The braid word α is $\equiv$-equivalent to the trivial word if and only if the words $\mathbf{N}_{LR}(\alpha)$ and $\mathbf{D}_{LR}(\alpha)$ are empty.*

Proof. The empty sequence is the only *positive* sequence which is equivalent to ε. ■

The algorithmic complexity of the determination of the LR-numerator and denominator will be computed at the end of Section 6. Observe that (owing to the formulas above expressing the L-operations in terms of the R-operations) the comparison method above coincides with the one deduced from Proposition 3.8.

By examining again the generating relations of $\widetilde{\equiv}$, one easily defines a left complement for $\widetilde{\equiv}$. But this complement has no interest because it heavily fails to be coherent and convergent. Actually most of the properties of B_∞ can be lifted to B_∞^+ 'on the right', but not 'on the left'. In particular the question of the right cancellability in the monoid $\mathrm{S}^*/\widetilde{\equiv}^+$ remains open for the moment.

5. Simple sequences.

It remains to prove that the complement mapping $\widetilde{\boldsymbol{c}}$ for $\widetilde{\equiv}$ is convergent, *i.e.* that every reduction using $\widetilde{\boldsymbol{c}}$ must terminate. By Proposition 3.7 this property is equivalent to the right regularity of the monoid $\mathrm{S}^*/\widetilde{\equiv}^+$. Now Lemma 1.3 nearly claims that the monoid C_{LD}^+, which is a quotient of $\mathrm{S}^*/\widetilde{\equiv}^+$ and is supposed to resemble it, is right regular. Unfortunately the proof of Lemma 1.3 given in [4] uses the action on terms and distribution in an essential way so that there is no obvious way for simply lifting the regularity result from C_{LD}^+ to $\mathrm{S}^*/\widetilde{\equiv}^+$. On the other hand a direct proof that every sequence in $\mathrm{S}^{\mathbf{sym}}$ is fully reducible is quite problematic for the lengths of the sequences may increase in the reduction process. Garside's solution for the similar question in the case of braid groups B_n uses the fundamental words Δ_n. Such a global tool can be used only in finitely generated groups. This solution cannot be extended to the case of G_{LD}, which, in contradistinction to B_∞, has no natural finitely generated approximations. We shall see at the end of Section 6 that the method developed below is a kind of local version of Garside's method.

The only situation where f-reduction in $\mathrm{X}^{\mathbf{sym}}$ clearly has to terminate is the case where for every x, y in X the sequence $f(x,y)$ has length 0 or 1. This hypothesis is not satisfied in the present case since *e.g.* $\widetilde{\boldsymbol{c}}(\Lambda,1)$ is $\Lambda\bullet 1\bullet 0$. In order to fall nevertheless in the case above, we shall determine the closure $\widehat{\mathrm{S}}$ of S under the complement $\widetilde{\mathbf{C}}$ and replace S by this extended set. The correct definition will come once again from the interpretation on terms given by the operator Ω. This section is devoted to a description of the needed geometrical notions.

We use the following notations. For any sequence ξ in $\mathrm{S}^{\mathbf{sym}}$ such that the identity $(LD)_\xi$ is defined, the first and the second components of the pair $(LD)_\xi$ will be called the *initial* and *final* terms of ξ respectively, and denoted by $\mathbf{T}_I(\xi)$ and $\mathbf{T}_F(\xi)$. Thus the domain and images of the operator $\Omega(\xi)$ are respectively the sets $\mathrm{Subst}(\mathbf{T}_I(\xi))$ and $\mathrm{Subst}(\mathbf{T}_F(\xi))$. We already observed that, if X is a positive sequence, then the term $\mathbf{T}_I(X)$ is an injective term (this follows inductively from the fact that $\mathbf{T}_I(\Lambda)$, which is $\boldsymbol{x}_1[\boldsymbol{x}_2[\boldsymbol{x}_3]]$, is injective). The term $\mathbf{T}_F(X)$ is certainly not injective whenever the sequence X is not the empty sequence.

Definition.- The term P is *subinjective* if, for every subterm Q of P, the rightmost variable of Q (*i.e.* the last variable in the word Q) occurs only once in Q.

An injective term is subinjective, but the converse is not necessarily true. For instance the term $\mathbf{T}_F(\Lambda)$, which is $\boldsymbol{x}_1[\boldsymbol{x}_2][\boldsymbol{x}_1[\boldsymbol{x}_3]]$, and more generally all terms $\mathbf{T}_F(w)$ for w in S, are subinjective but not injective. Injective terms are useful in order to follow the geometrical evolution of occurrences when distribution transformations are operated. A close examination of the extensions of injective terms, and in particular of the derived terms ∂P introduced in [4] suggests the following

Definition.- A positive sequence X is Ω-*simple* if the term $\mathbf{T}_F(X)$ is a subinjective term.

The idea is that the transformation associated with an Ω-simple sequence may not distribute a subterm of a term inside itself. For instance the sequence $\Lambda\bullet\Lambda$ is not Ω-simple because in the term $\mathbf{T}_F(\Lambda\bullet\Lambda)$, which is $\boldsymbol{x}_1[\boldsymbol{x}_2][\boldsymbol{x}_1][\boldsymbol{x}_1[\boldsymbol{x}_2][\boldsymbol{x}_3]]$, the subterm $\boldsymbol{x}_1[\boldsymbol{x}_2]$ is distributed to its own subterm $\boldsymbol{x}_1$. In the sequel we denote by $\mathrm{var}_R(P)$ the rightmost variable of the term P.

Lemma 1.- *Let X be a positive sequence. Then the following are equivalent:*
i) the sequence X is Ω-simple;
ii) the image of every injective term under the operator $\Omega(X)$ is subinjective;
iii) the image of some injective term under the operator $\Omega(X)$ is subinjective.

Proof. In order to prove that (i) implies (ii), assume that P is any injective term in the domain of $\Omega(X)$. There exists a substitution σ such that P is $\mathbf{T}_I(X)^\sigma$ and the image Q of P under $\Omega(X)$ is $\mathbf{T}_F(X)^\sigma$. If R is any subterm of Q, then either R is a subterm of some $\boldsymbol{v}^\sigma$ for $\boldsymbol{v}$ a variable occurring in $\mathbf{T}_F(X)$, and R must be injective since $\boldsymbol{v}^\sigma$ is a subterm of the injective term P, or there exists a subterm R' of $\mathbf{T}_F(X)$ such that R is R'^σ. In this case $\mathrm{var}_R(R)$ is $\mathrm{var}_R(\mathrm{var}_R(R')^\sigma)$, which occurs only once in $\mathrm{var}_R(R')^\sigma$ because the latter term is a subterm of P, and therefore only once in R because R' is subinjective. So Q is subinjective.

In order to prove that (iii) implies (i), assume that P is an injective term and that $\Omega(X)$ maps P to a subinjective term Q. Assume that the term $\mathbf{T}_F(X)$ is not subinjective. There exists a subterm R of $\mathbf{T}_F(X)$ such that $\mathrm{var}_R(R)$ occurs at least twice in R. But for some substitution σ the term Q is $\mathbf{T}_F(X)^\sigma$, and the variable $\mathrm{var}_R(R^\sigma)$, which is $(\mathrm{var}_R(R))^\sigma$, occurs at least twice in R^σ, and therefore the term Q is not subinjective, a contradiction. ■

For P in $\mathcal{T}_\Sigma$ and w in S short enough, we denote by $\mathbf{S}_w(P)$ the subterm of the term P with address w. The set of all w in S such that $\mathbf{S}_w(P)$ exists is called the *support* of the term P and denoted by $\mathrm{Supp}(P)$. Then the size of P is the cardinality of $\mathrm{Supp}(P)$.

Lemma 2.- *If the term Q is an extension of the term P and Q is subinjective, then P must be subinjective.*

Proof. Assume that Q is an extension of P, and that P is not subinjective. We show that Q is not subinjective. Clearly it suffices to show the result for the case when some $\Omega(w)$ maps P to Q. Assume that the subterm $\mathbf{S}_u(P)$ witnesses for P being not subinjective. We have to exhibit some point v such that the subterm $\mathbf{S}_v(Q)$ witnesses for the similar property in Q. One considers the various possible mutual positions of u and w. If u and w are prefix-incomparable, then $\mathbf{S}_u(Q)$ is equal to $\mathbf{S}_u(P)$, and u is convenient. If either $w0$ or $w10$ or $w11$ is a prefix of u, then Q includes at least one copy of $\mathbf{S}_u(P)$, this copy is not subinjective, and Q having a nonsubinjective subterm cannot be subinjective. If u is $w1$, then $\mathrm{var}_R(\mathbf{S}_u(P))$ is $\mathrm{var}_R(\mathbf{S}_w(P))$, and by definition it occurs at least once in $\mathbf{S}_{u10}(P)$ or twice in $\mathbf{S}_{u11}(P)$ So it occurs certainly twice in $\mathbf{S}_w(Q)$. The argument is similar if u is w. Finally if u is a strict prefix of w, applying $\Omega(w)$ to P cannot duplicate the variable $\mathrm{var}_R(\mathbf{S}_v(P))$ and therefore P cannot be subinjective. ■

Proposition 3.- *Any subsequence of an Ω-simple sequence is Ω-simple.*

Proof. Assume that X, Y, Z are positive sequences and Y is not Ω-simple. Let P be any injective term in the domain of $\Omega(X\bullet Y\bullet Z)$, and let Q, R respectively be the images of P under $\Omega(X\bullet Y)$ and $\Omega(X\bullet Y\bullet Z)$. Because Y is not Ω-simple, Q cannot be subinjective, and therefore by Lemma 2 the term R cannot be subinjective. By Lemma 1 this proves that the sequence $X\bullet Y\bullet Z$ is not Ω-simple. ■

For the moment we have no syntactical characterization of the Ω-simple sequences. But it is easy to define on a purely syntactical way a family of Ω-simple sequences. So exactly as in Section 2 where we substituted the study of the group $\widetilde{B}_\infty$ to the study of G_{LD}, we shall replace the study of Ω-simple sequences by the study of the special sequences mentioned above. At the end both notions will coincide.

Definition.- i) For w in S and k in N, $w_{(k)}$ denotes the empty sequence if k is 0 and the sequence $w1^{k-1}\bullet w1^{k-2}\bullet\ldots\bullet w1\bullet w$ otherwise.

ii) The set $\widehat{\mathrm{S}}$ is the least subset of S^* which contains the empty sequence and is closed for every integer k under the operation

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

A positive sequence is said to be *simple* if is $\widetilde{\equiv}^+$-equivalent to a sequence in $\widehat{\mathrm{S}}$.

An easy induction shows that any sequence in $\widehat{\mathrm{S}}$ has a unique decomposition as

$$\prod_{w\in\mathrm{S}}^{\triangleright} w_{(k_w)}$$

where $\langle k_w; w\in\mathrm{S}\rangle$ is a sequence of integers with only finitely many positive values and $\triangleright$ is the linear ordering on 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 first factor $\Lambda_{(k_\Lambda)}$. To this end observe that Λ occurs at most once in any element of $\widehat{\mathsf{S}}$, 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 $\mathrm{ind}(w, X)$. Notice that S is included in $\widehat{\mathsf{S}}$, for Λ is clearly simple, and for every w in S the sequence wX is in $\widehat{\mathsf{S}}$ if (and only if) X is in $\widehat{\mathsf{S}}$.

Lemma 4.- *A simple sequence is Ω-simple.*

Proof. Since $X \mathrel{\widetilde{\equiv}}^+ X'$ implies $\Omega(X) = \Omega(X')$, it suffices to show that, if X is in $\widehat{\mathsf{S}}$, and $\Omega(X)$ maps some injective term P to Q, then Q is subinjective. We do it inductively on the size of the term P. The result is obvious if P is a variable. So assume that P is not in Σ. By definition of $\widehat{\mathsf{S}}$, there exists an integer k and sequences X_0, X_1 in $\widehat{\mathsf{S}}$ such that X is $\Lambda_{(k)} \bullet 1 X_1 \bullet 0 X_0$. Let $R_0[R_1]$ be the image of P under $\Omega(\Lambda_{(k)})$. An easy computation shows that for $e = 0, 1$ the term R_e is injective and that its size is strictly below the size of P. So the induction hypothesis implies that the image R'_e of R_e under $\Omega(X_e)$ is subinjective. Now Q is $R'_0[R'_1]$, and clearly $\mathrm{var}_R(R'_1)$, which is $\mathrm{var}_R(P)$, does not occur in R'_0. So Q is subinjective. ■

The notion of a simple sequence in S^* can be projected to the positive integers using the braid projection. The geometrical meaning of the sequences so obtained is easily described. With obvious notations, a positive braid word A is simple if and only if it has a decomposition

$$A \equiv^+ \sigma_{1(k_1)} \bullet \sigma_{2(k_2)} \bullet \ldots.$$

Simple braids are characterized algebraically as the divisors of the fundamental words Δ_n (see the end of Section 6), and geometrically by the property that they can be arranged so that any string crosses at most once any other string (this is obvious from the above definition). For the moment we observe that the projection of braids onto permutations is a bjection on simple braids. Let $\mathfrak{S}_{(\mathrm{N})}$ be the group of all permutations of the nonnegative integers which eventually coincide with identity. Denote by Φ the product of the canonical projections of $\mathsf{S}^{\mathbf{sym}}$ onto $\widetilde{B}_\infty$, of $\widetilde{B}_\infty$ onto B_∞ and of B_∞ onto $\mathfrak{S}_{(\mathrm{N})}$.

Lemma 5.- *The restriction of Φ to $\widehat{\mathsf{S}}$ is surjective. Two sequences X, X' in $\widehat{\mathsf{S}}$ have the same image under Φ if and only if the indices of the points 1^i in X and X' are equal for every $i \geq 0$.*

Proof. Easy induction starting from the fact that the index of Λ in X determines the image of 0 under $\Phi(X)$. ■

In terms of $\widehat{\mathrm{S}}$ one deduces the following uniqueness property. This is the first result where a geometrical property implies a syntactical one.

Proposition 6.- *Assume that X is a simple sequence. Then there exists exactly one element X' of $\widehat{\mathrm{S}}$ satisfying $\Omega(X) = \Omega(X')$.*

Proof. First let us denote for P in $\mathcal{T}_\Sigma$ by $f(P,i)$ the rightmost variable of the subterm $\mathbf{S}_{1^i0}(P)$, if it exists. An easy induction shows that, if X is a positive sequence and $\Omega(X)$ maps the term P to the term Q, then

$$f(Q,i) = f(P, \Phi(X)(i))$$

holds whenever $f(P,i)$ exists. This gives a criterion for reconstructing the sequence X from the pair (P,Q) if X is assumed to be Ω-simple and the mapping $i \mapsto f(P,i)$ is injective (which certainly happens if P is an injective term). We claim that, if X, Y are two elements of $\widehat{\mathrm{S}}$ such that $\Omega(X)$ and $\Omega(Y)$ take the same value on some injective term P, then X and Y are equal. This is proved inductively on the size of the term P. If $\Omega(X)$ and $\Omega(Y)$ map P to Q, the formula above shows that the permutations $\Phi(X)$ and $\Phi(Y)$ give equal values to all integers i such that the point 1^i0 lies in the support of P. The other integers must be fixed points of $\Phi(X)$ and $\Phi(Y)$. By Lemma 5 this implies that the indices of Λ (and more generally of any 1^i) in X and Y are equal. Now write $X = \Lambda_{(k)} \bullet 1 X_1 \bullet 0 X_0$, $Y = \Lambda_{(k)} \bullet 1 Y_1 \bullet 0 Y_0$, and let $P_0[P_1]$ be the image of P under $\Omega(\Lambda_{(k)})$. Then for $e = 0$ and $e = 1$ the term P_e is injective, has the same image under $\Omega(X_e)$ and $\Omega(Y_e)$ and its size is strictly less than the size of P. By induction hypothesis, this implies $X_e = Y_e$ for $e = 0, 1$, and we are done. ■

By this result, there is no ambiguity to define in the sequel the *normal form* of a simple sequence X as the unique element X' in $\widehat{\mathrm{S}}$ satisfying $X \mathrel{\widetilde{\equiv}^+} X'$. Also we shall speak of the indices of a simple sequence as the indices in its normal form.

6. Complementation of simple sequences.

The main result of this section is the convergence of the complement mapping associated with the congruence $\mathrel{\widetilde{\equiv}}$ on $\mathrm{S}^{\mathbf{sym}}$. This result will be proved by directly establishing that the complement of two simple sequences exist and is still simple, so that reduction does not increase the degree of a sequence defined as the length of its decomposition into a product of simple sequences, and therefore must eventually terminate.

Our main task will be to compute the product of two simple sequences and in particular to control the fact that this product is simple or not. The process will be inductive so that the key point is to compute the product of an arbitrary simple sequence X and a single factor of the form $1^q{}_{(i)}$. The following lemma determines the two possible types of elementary products appearing in this process.

Lemma 1.- *For p, k, i in* N *and Y in* S^**, the following formulas hold*

$$1^p{}_{(k)} \bullet \Lambda_{(i)} \begin{cases} \widetilde{\equiv}^+ \Lambda_{(i)} \bullet 1^p{}_{(k)} & \text{if } i < p, \\ = \Lambda_{(k+i)} & \text{if } i = p, \\ \text{is not } \Omega\text{-simple} & \text{if } p < i \leq p+k, \\ \widetilde{\equiv}^+ \Lambda_{(i)} \bullet 1^{p+1}{}_{(k)} \bullet 01^p{}_{(k)} & \text{if } i > p+k. \end{cases}$$

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

Proof. The first two cases in the first formula are easy, as well as the particular case $k = 0$. For the third case, assume $i = p + \ell$ with $1 \leq \ell \leq k$. Let P be the term $\mathbf{x}_1[\mathbf{x}_2[\ldots[\mathbf{x}_{p+k+1}[\mathbf{x}_{p+k+2}]]\ldots]]$. One verifies that, if Q is the image of P under $\Omega(1^p{}_{(k)} \bullet 1^p{}_{(\ell)})$, then the variable $\mathbf{x}_{p+\ell}$ occurs both at $1^p 0^2 1^{\ell-1} 0$ and $1^p 01^\ell$ in Q. So Q is not subinjective, the sequence $1^p{}_{(k)} \bullet 1^p{}_{(\ell)}$ is not Ω-simple, and by Proposition 5.3 this implies that $1^p{}_{(k)} \bullet \Lambda_{(i)}$, which has a non-$\Omega$-simple subsequence, is not Ω-simple either. For the last case, denote by $\mathcal{F}(p,k,i)$ the formula

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

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 is the heptagonal identity. The details are not difficult. The second formula is proved similarly using induction on $i \geq 0$. ■

Definition.- Assume that X is a simple sequence. Denote by $\widehat{X}$ the mapping on nonnegative integers defined by

$$\widehat{X}(i) = i + \mathrm{ind}(1^i, X).$$

The integer i is *admissible for X* if the inequality $\widehat{X}(x) < \widehat{X}(i)$ holds for every $x < i$. The integer k is *accessible to X* if k is $\widehat{X}(i)$ for some i which is admissible for X.

Lemma 2.- *Assume that X is a simple sequence and i is any integer. Then either i is admissible for X, the sequence $X \bullet \Lambda_{(i)}$ is simple and $\widehat{X}(i)$ is the index of Λ in this sequence, or i is not admissible for X and the sequence $X \bullet \Lambda_{(i)}$ is not Ω-simple.*

Proof. We may assume that X is in $\widehat{\mathrm{S}}$ and write

$$X = \prod_{p=0}^{\infty} 1^p{}_{(k_p)} \bullet \prod_{p=\infty}^{0} 1^p 0 X_p$$

(where each X_p belongs to $\widehat{\mathrm{S}}$). By Lemma 1, we obtain

$$X \bullet \Lambda_{(i)} \mathrel{\widetilde{\equiv}^+} \prod_{p=0}^{\infty} 1^p{}_{(k_p)} \bullet \Lambda_{(i)} \bullet \prod_{p=\infty}^{i+1} 1^p 0 X_p \bullet \prod_{p=i-1}^{0} 1^{p+1} 0 X_p \bullet 01^i X_i \bullet \prod_{p=i-1}^{0} 01^p 0 X_p.$$

Now one has

$$\prod_{p=i}^{\infty} 1^p{}_{(k_p)} \bullet \Lambda_{(i)} \mathrel{\widetilde{\equiv}^+} \Lambda_{(m)} \bullet \prod_{p=i+1}^{\infty} 1^p{}_{(k_p)},$$

where m is $i + k_i$, *i.e.* $\widehat{X}(i)$. In order to compute the product $\prod_0^{i-1} 1^p{}_{(k_p)} \bullet \Lambda_{(m)}$, we successively consider the products $1^p{}_{(k_p)} \bullet \Lambda_{(m)}$ for $p = i-1, \ldots, p = 0$ and obtain a formula

$$1^p{}_{(k_p)} \bullet \Lambda_{(m)} \mathrel{\widetilde{\equiv}^+} \Lambda_{(m)} \bullet Y_p$$

for some (simple) Y_p whenever the condition $\widehat{X}(p) < m$ holds. So if i admissible for X we successfully commute $\Lambda_{(m)}$ with each of $1^{i-1}{}_{(k_{i-1})}$, ..., $\Lambda_{(k_0)}$, and the resulting factors form a simple sequence (up to some commutations). The value for the index of Λ in $X \bullet \Lambda_{(i)}$ follows from the explicit value in Lemma 1. Now if one of the inequalities fails, let r be the maximal index such that $\widehat{X}(r) \geq m$ holds. Then

$$1^{r+1}{}_{(k_{r+1})} \bullet \ldots \bullet 1^{i-1}{}_{(k_{j-1})} \bullet \Lambda_{(m)}$$

is $\widetilde{\equiv}^+$-equivalent to $\Lambda_{(m)} \bullet Y'$ for some Y'. By Lemma 1 (translated using left concatenation of 1^r in each factor), $1^r{}_{(k_r)} \bullet 1^r{}_{(m-r)}$ is not Ω-simple, and therefore by 5.3 the sequences $1^r{}_{(k_r)} \bullet \Lambda_{(m)}$ and $X \bullet \Lambda_{(i)}$ are not Ω-simple. ■

As a first application, we obtain the converse implication of Lemma 5.4.

Proposition 3.- *A positive sequence in* S^* *is simple if and only if it is* Ω*-simple.*

Proof. It remains to prove that X is simple whenever it is Ω-simple. We use induction on the size of the term $\mathbf{T}_I(X)$, and, for a given cardinality, induction on the length of X. The result is obvious if $\mathbf{T}_I(X)$ has size 1 (then X must be the empty sequence), or if X has length 1 (then X is simple). Assume that X is Ω-simple, and has length $n \geq 2$. Write $X = Y \bullet v$. By 5.3 the sequence Y is Ω-simple. The term $\mathbf{T}_I(X)$ belongs to $\mathrm{Subst}(\mathbf{T}_I(Y))$ so the size of $\mathbf{T}_I(Y)$ is at most the size of $\mathbf{T}_I(X)$, and Y has length $n-1$. So by induction hypothesis Y is simple. If v is Λ, we apply Lemma 2 to conclude that either $Y \bullet v$ is simple, or it is not Ω-simple. In the second case X

could not be Ω-simple, a contradiction. So $Y{\bullet}v$ and X are simple. If v is not Λ, say $v = ev'$ with $e = 0$ or $e = 1$, we write Y as $\Lambda_{(k)}{\bullet}1Y_1{\bullet}0Y_0$ for some simple sequences Y_1, Y_0. If the term P lies in the domain of $\Omega(X)$, it lies in the domain of $\Omega(\Lambda_{(k)})$, and, if $Q_0[Q_1]$ is the image of P under $\Omega(\Lambda_{(k)})$, then Q_e lies in the domain of $Y_e{\bullet}v'$ and its size is strictly smaller than the size of P. By applying this fact to the case of $P = \mathbf{T}_I(X)$, we see that the induction hypothesis holds for the sequence $Y_e{\bullet}v'$, which has to be simple, as well as X itself. ■

By Proposition 5.3, the previous result implies that any subsequence of a simple sequence is simple. No syntactical proof of this result is known, and therefore the detour through Ω-simple sequences seems unavoidable at the present time.

If X, Y are positive sequences, there exists a unique canonical term R such that the intersection of $\mathrm{Subst}(\mathbf{T}_I(X))$ and $\mathrm{Subst}(\mathbf{T}_I(Y))$, *i.e.* of the domains of $\Omega(X)$ and $\Omega(Y)$, is exactly $\mathrm{Subst}(R)$. This term R will be denoted $\mathbf{T}_I(X, Y)$.

Proposition 4.- *Assume that X, Y are simple sequences. Then the sequences $\widetilde{\mathbf{C}}(X, Y)$ and $\widetilde{\mathbf{J}}(X, Y)$ exist and are simple. The term $\mathbf{T}_I(\widetilde{\mathbf{J}}(X, Y))$ is exactly $\mathbf{T}_I(X, Y)$. Moreover the index k of Λ in $\widetilde{\mathbf{J}}(X, Y)$ is the least number which is accessible both to X and Y, and the index i of Λ in $\widetilde{\mathbf{C}}(X, Y)$ is the (unique) integer i which is admissible for X and mapped to k by $\widehat{X}$.*

Proof. We use induction on the size of $\mathbf{T}_I(X, Y)$. The result is clearly true if $\mathbf{T}_I(X, Y)$ has size 1, for in this case X and Y must to be empty. Let X, Y be arbitrary positive sequences. Let k be the minimal number which is accessible both to X and Y. Because the functions $\widehat{X}$ and $\widehat{Y}$ eventually coincide with the identity mapping, every integer which is large enough is accessible to X and Y, and the number k must exist. Let i and j be the least preimages of k with respect to $\widehat{X}$ and $\widehat{Y}$ respectively. By Lemma 2 the integers i and j are admissible for X and Y respectively, the sequences $X{\bullet}\Lambda_{(i)}$ and $Y{\bullet}\Lambda_{(j)}$ are simple and k is the index of Λ in both of them. So there exist simple sequences X_e, Y_e, for $e = 0, 1$ satisfying

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

In order to apply the induction hypothesis we have to verify that the size of $\mathbf{T}_I(X_e, Y_e)$ is strictly below the size of $\mathbf{T}_I(X, Y)$ for $e = 1$ and $e = 0$. To obtain this result it suffices to prove

$$\mathbf{T}_I(X, Y) = \mathbf{T}_I(X \bullet \Lambda_{(i)}, Y \bullet \Lambda_{(j)}).$$

Indeed this condition implies that $\mathbf{T}_I(X, Y)$ lies in the domains of $\Omega(\Lambda_{(k)}{\bullet}1X_1{\bullet}0X_0)$ and $\Omega(\Lambda_{(k)}{\bullet}1Y_1{\bullet}0Y_0)$, and then, if $Q_0[Q_1]$ is the image of $\mathbf{T}_I(X, Y)$ under $\Omega(\Lambda_{(k)})$, the term Q_e lies in the domains of X_e and Y_e. This shows that the size of $\mathbf{T}_I(X_e, Y_e)$, which is at most the size of Q_e, is strictly below the size of $\mathbf{T}_I(X, Y)$.

The condition above is trivial if k is 0. Assume $k \geq 1$. We claim that at least one of i, j is strictly smaller than k. Assume that i is equal to k. By definition of an admissible number, we must have

$$\widehat{X}(k-1) < k$$

and therefore the index of 1^{k-1} in X is 0. Let i' be the least preimage of $k-1$ under $\widehat{X}$. For x smaller than i', $\widehat{X}(x)$ cannot be greater than k since k is admissible, and cannot be $k-1$ by definition of i'. So i' is admissible for X, and $k-1$ is 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. 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 $\Omega(\xi)$. So assume that P lies in the domain of $\Omega(X)$: because of the factor $1^i{}_{(k-i)}$ in the normal form of 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. So the claim is proved.

At this point we may apply the induction hypothesis to X_e and Y_e for $e = 0$ and $e = 1$. So the sequences $\widetilde{\mathbf{C}}(X_e, Y_e)$ exist and are simple, and one has

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

This proves that X, Y have a common multiple which is moreover simple.

The inductive argument preserves the hypothesis that $\mathbf{T}_I(\widetilde{\mathbf{J}}(X,Y))$ is $\mathbf{T}_I(X,Y)$. So it only remains to prove that the common multiple constructed above is the least such common multiple. Write i', j', k' for the indices of Λ in the simple sequences $\widetilde{\mathbf{C}}(Y,X)$, $\widetilde{\mathbf{C}}(X,Y)$, $\widetilde{\mathbf{J}}(X,Y)$ respectively. The formulas of Lemma 1 show that the index of Λ never decreases when a product is operated on the right. Since the sequence $\widetilde{\mathbf{J}}(X,Y)$ has to divide the sequence $\Lambda_{(k)} \bullet 1\widetilde{\mathbf{J}}(X_1,Y_1) \bullet 0\widetilde{\mathbf{J}}(X_0,Y_0)$, we must have $k' \leq k$. But on the other hand $\widetilde{\mathbf{J}}(X,Y)$ is a common multiple of X and Y, and this implies that k' is accessible both to X and Y and therefore $k \leq k'$ holds by minimality of k. Hence k' and k are equal. Now $X \bullet \Lambda_{(i')}$ is a simple sequence and the index of Λ in this sequence is k. By Lemma 2 the only possibility is $i' = i$, and similarly $j' = j$. This completes the proof of Proposition 4. ■

Definition.- The *degree* $\mathrm{d}^\circ(\xi)$ of the sequence ξ in $\mathrm{S}^{\mathbf{sym}}$ is the least number d such that ξ can be factorized as the product of d sequences, each of which is either a simple sequence or the inverse of a simple sequence.

Proposition 5.- *The complement $\widetilde{\boldsymbol{c}}$ is convergent, and for every sequence ξ one has*

$$\mathrm{d}^o(\widetilde{\mathbf{N}}(\xi)) \leq \mathrm{d}^o(\xi)\ , \qquad \mathrm{d}^o(\widetilde{\mathbf{D}}(\xi)) \leq \mathrm{d}^o(\xi).$$

If X, Y are positive sequences one has

$$\mathrm{d}^o(\widetilde{\mathbf{C}}(X,Y)) \leq \mathrm{d}^o(X)\ , \qquad \mathrm{d}^o(\widetilde{\mathbf{J}}(X,Y)) \leq \sup(\mathrm{d}^o(X), \mathrm{d}^o(Y)).$$

Proof. Immediate induction from Proposition 4. ■

Let us define, for X, Y in $\widehat{\mathrm{S}}$, the sequences $\widehat{\mathbf{C}}(X,Y)$ and $\widehat{\mathbf{J}}(X,Y)$ as the respective normal forms (in $\widehat{\mathrm{S}}$) of the simple sequences $\widetilde{\mathbf{C}}(X,Y)$ and $\widetilde{\mathbf{J}}(X,Y)$. The proof of Proposition 4 gives an inductive way for directly determining the values of $\widehat{\mathbf{C}}(X,Y)$ and $\widehat{\mathbf{J}}(X,Y)$, *i.e.* computing the corresponding lists of indices. Having determined the minimal number k which is accessible to X and Y, and their minimal preimages i and j under $\widehat{X}$ and $\widehat{Y}$, one computes (using the formulas of Lemma 1) the normal forms of $X{\bullet}\Lambda_{(i)}$ and $Y{\bullet}\Lambda_{(j)}$, and apply inductively the process to the '1-component' and the '0-component' of these sequences. Observe that the relations

$$\widetilde{\sigma}_X \bullet \widetilde{\sigma}_{\widehat{\mathbf{C}}(Y,X)} = \widetilde{\sigma}_{\widehat{\mathbf{J}}(X,Y)}$$

form a presentation of the group $\widetilde{B}_\infty$ from the generators $\widetilde{\sigma}_X$ with X in $\widehat{\mathrm{S}}$. The mapping $\widehat{\mathbf{C}}$ is a (right) complement for this presentation, which is trivially coherent because $\widetilde{\boldsymbol{c}}$ is coherent, and convergent because it does not increase length (w. r. to the new generators). Remark that reduction using $\widehat{\mathbf{C}}$ instead of $\widetilde{\boldsymbol{c}}$ leads to equivalent, but not necessarily identical numerator and denominator.

When projected to braids, the previous results give the convergence of the braid complement $\boldsymbol{c}_R$ and thus a new proof of the right regularity of the monoid B_∞^+ which is local and makes no use of the universal words Δ_n. With obvious notations, one obtains a presentation of B_∞ by the relations

$$\sigma_A \bullet \sigma_{\widehat{\mathbf{C}}_R(B,A)} = \sigma_{\widehat{\mathbf{J}}_R(A,B)}$$

where A, B range over simple braid words (or, equivalently, over the permutations in $\mathfrak{S}_{(\mathrm{N})}$).

The reduction of a sequence $\overline{X}{\bullet}Y$ with X, Y (positive) simple sequences in $\mathrm{S}^{\mathbf{sym}}$ or $\mathrm{N}_+^{\mathbf{sym}}$ will be called a *simple reduction*.

Proposition 6.- *i) If ξ is a sequence in $\mathrm{S}^{\mathbf{sym}}$ with degree m, the determination of $\widetilde{\mathbf{N}}(\xi)$ and $\widetilde{\mathbf{D}}(\xi)$ requires at most $m^2/4$ simple reductions.*

ii) If α is a braid word with degree m, the determination of $\mathbf{N}_{R}(\alpha)$ and $\mathbf{D}_{R}(\alpha)$ requires at most $m^2/4$ simple reductions, and the determination of $\mathbf{N}_{LR}(\alpha)$ and $\mathbf{D}_{LR}(\alpha)$ requires at most $m^2/2$ simple reductions.

Proof. Obvious from Proposition 5. ■

This results in a quadratic upper bound for the comparison of braid words when one restricts to a fixed set of generators σ_1, ..., σ_n. Indeed it suffices to determine once for all a table of complements for the $n!$ simple braids involving σ_1, ..., σ_n (or, better, for the corresponding lists of indices, *i.e.* for the permutations of $\{1, \ldots, n\}$). For an unbounded set of generators, one has to include the cost of simple reductions. But at this point one meets with the study already made by Thurston, and we refer to [23].

When one restricts to the case of $n-1$ generators, simple braid words as defined here are easily characterized as the divisors of the halftwist Δ_n (see *e.g.* [10]). We observed that Garside's approach cannot extend to $\widetilde{B}_\infty$ since $\widetilde{B}_\infty$ has no such finitely generated approximations. Nevertheless we can define a local notion of maximal simple sequences using the action on terms via Ω and the derivation of terms introduced in [4].

Definition.- For P in $\mathcal{T}_\Sigma$, the *deriving sequence of P* is the sequence $\widetilde{\Delta}_P$ inductively defined as follows. If P is a variable, then $\widetilde{\Delta}_P$ is the empty sequence. Otherwise $\widetilde{\Delta}_P$ is $\Lambda_{(h-2)} \bullet 1 \widetilde{\Delta}_{Q_1} \bullet 0 \widetilde{\Delta}_{Q_0}$ where h is the right height of P and $Q_0[Q_1]$ is the image of P under $\Omega(\Lambda_{(h-2)})$. The image of the term P under the mapping $\Omega(\widetilde{\Delta}_P)$ is denoted by ∂P and called the *derived term* of P.

By construction the sequence $\widetilde{\Delta}_P$ is in $\widehat{\mathrm{S}}$. One could show that the present definition of derivation is equivalent to the one used in [4].

Lemma 7.- *No strict extension of a derived term ∂P may be a subinjective term.*

Proof. By 5.2 it suffices to prove that R is not a subinjective term when R is the image of ∂P under some transformation $\Omega(w)$ with w in S. Assume first that w is Λ. By construction of the derived term, every variable occurring in P except the rightmost one occurs both in the left and right subterms of ∂P, because the index of Λ in $\widetilde{\Delta}_P$ has the maximal possible value. Let $\boldsymbol{v}$ be the rightmost variable in $\mathbf{S}_{10}(\partial P)$. Certainly $\boldsymbol{v}$ also occurs in $\mathbf{S}_0(\partial P)$, and it follows that $\boldsymbol{v}$, which is the rightmost variable of $\mathbf{S}_0(R)$, occurs at least twice in this term. Hence R cannot be subinjective. Now assume that w is ew' for some w' in S and e in $\{0, 1\}$. Write ∂P as $\partial P_0[\partial P_1]$ where h is the right height of P and $P_0[P_1]$ is the image of P under $\Omega(\Lambda_{(h-2)})$. Then

the subterm $\mathbf{S}_e(R)$ is a strict extension of ∂P_e. Because the size of P_e is strictly less than the size of P, we may apply the induction hypothesis and conclude that R is not subinjective. ■

Lemma 8.- *Let P be any term in $\mathcal{T}_\Sigma$. Then the positive sequences which divide $\widetilde{\Delta}_P$ are exactly the simple sequences X such that the domain of $\Omega(X)$ contains P.*

Proof. The term P belongs by construction to the domain of $\Omega(\widetilde{\Delta}_P)$. The domain of any operator $\Omega(X \bullet Y)$ is included in the domain of the operator $\Omega(X)$, and any subsequence of a simple sequence is simple, hence the first condition implies the second one. Conversely assume that X is a simple sequence and that the term P is in the domain of $\Omega(X)$. Since the sequence $\widetilde{\Delta}_P$ only depends on the support of the term P we may assume that P is an injective term. Now X and $\widetilde{\Delta}_P$ are simple sequences, so by Proposition 4 the sequence $\widetilde{\mathbf{J}}(\widetilde{\Delta}_P, X)$ is simple. By Proposition 4 again, the term P lies in the domain of $\Omega(\widetilde{\mathbf{J}}(\widetilde{\Delta}_P, X))$, and the image of P under $\Omega(\widetilde{\mathbf{J}}(\widetilde{\Delta}_P, X))$, which is the image of ∂P under $\Omega(\widetilde{\mathbf{C}}(X, \widetilde{\Delta}_P)$, is subinjective. By Lemma 7 this implies that $\widetilde{\mathbf{C}}(X, \widetilde{\Delta}_P)$ is empty, *i.e.* that X divides $\widetilde{\Delta}_P$. ■

For every term P, the simple sequences X such that P lies in the domain of $\Omega(X)$ form a finite semilattice $\widehat{\mathrm{S}}_P$, and the sequence $\widetilde{\Delta}_P$ is the maximum of $\widehat{\mathrm{S}}_P$. The projection of $\widehat{\mathrm{S}}_P$ using $\flat$ is the set of the simple sequences on σ_1, ..., σ_{h-1}, where h is the right height of the term P. In particular the projection of $\widetilde{\Delta}_P$ is the fundamental word Δ_{h-1}. Several properties of the braids Δ_n extend to the sequences $\widetilde{\Delta}_P$, and one can develop a complete theory for the semilattice of all simple extensions of a term P, defined as the images of P under all $\Omega(X)$ where X divides $\widetilde{\Delta}_P$. Generalizations involving iterated derivation lead to interesting features which are geometric counterparts for some properties of the words Δ_n^k such as the ones established in [10].

In this paper, we shall only observe that the above results give an effective upper bound for the complexity of reduction.

Lemma 9.- *Let ξ be a degree d sequence in $\mathrm{S}^{\mathbf{sym}}$. Assume that the term R lies in the domain of $\Omega(\xi)$. Then the lengths of all positive sequences involved in the reduction of ξ are bounded by $\exp_d(\mathrm{size}(R))$ where $\exp_1(n)$ is n and $\exp_{k+1}(n)$ is $2^{\exp_k(n)}$.*

Proof. Let us say that the reduction of ξ lies below the term P if P lies in the image of any operator $\Omega(X)$ such that there is a path in the Cayley diagram associated with the reduction of ξ which is labelled X and ends at the terminal point of the diagram. If the reduction of ξ lies below P, then the length of any positive sequence involved in this reduction is bounded by the size of P since every factor in the sequence strictly increases the size of any term it is applied to. Now we observe that, if ξ has the form $\overline{X} \bullet Y$ with X, Y simple positive sequences, and if R belongs to the domain of $\Omega(X)$

and $\Omega(Y)$, or to the domain of $\Omega(\xi)$, then the reduction of ξ is below ∂R. Iterating this result using Proposition 4 shows that the reduction of any degree d sequence lies below $\partial^d R$ whenever R belongs to the domain of $\Omega(\xi)$. The bound follows, since the size of ∂R is at most $2^{\mathrm{size}(R)}$. ■

The previous bound is certainly not optimal.

7. The presentation of left distributivity identities.

We are now ready to state the main results of the paper.

Theorem 1.- *The Irreflexivity Conjecture is true.*

Proof. The congruence $\widetilde{\equiv}$ for $\widetilde{B}_\infty$ admits $\widetilde{\boldsymbol{c}}$ as a complement. By 4.3 and 6.5, $\widetilde{\boldsymbol{c}}$ is coherent and convergent. So by 3.8, the pair of congruences $(\widetilde{\equiv}, \widetilde{\equiv}^+)$ has the right quotient property. By 2.9 this implies the irreflexivity of relation $\sqsubset_{LD}$. ■

This result settles a large number of technical questions about (free) LD-magmas. We gather the most important ones below.

Theorem 2.- *i) The word problem for $(\mathcal{T}_\Sigma, \approx_{LD})$ is decidable and has a primitive recursive complexity, as well as the relation $\sqsubset_{LD}$.*

ii) Every free LD-magma admits a linear ordering $<$ which is compatible with left translations and satisfies $x < x[y]$ for all x, y. In particular every free LD-magma is left cancellative.

iii) No consequence of (LD) has the form (P, Q) where P and Q are distinct terms with the same support.

iv) The normal forms for the elements of $\mathcal{T}_{\boldsymbol{x}}$ defined in [20] and [21] always exist.

v) The algorithm described in [8] for the word problem of $(\mathcal{T}_\Sigma, \approx_{LD})$ is correct when it terminates.

Proof. i) We have seen in Section 1 that the irreflexivity of the relation $\sqsubset_{LD}$ implies the decidability of the word problem when only one variable is involved. Observe that the results in Section 2 give a better method for term comparison than the brute enumeration used in Section 1: for P, Q in $\mathcal{T}_{\boldsymbol{x}}$, $P \approx_{LD} Q$ holds if and only if the equality

$$\mathrm{dil}(\widetilde{\mathbf{N}}(\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q)) = \mathrm{dil}(\widetilde{\mathbf{D}}(\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q))$$

is true. In order to extend the comparison to more than one variable, one uses point (iii), which is established in [4] from the Irreflexivity Conjecture. So assume that P, Q are terms in $\mathcal{T}_{\boldsymbol{x}}$ and let τ be the substitution which maps every variable to $\boldsymbol{x}$. First compare P^τ and Q^τ as above. If they are not equivalent, P and Q are not equivalent. Otherwise denote by X and Y the numerator and denominator of

$\overline{\widetilde{\chi}_{P^\tau}} \bullet \widetilde{\chi}_{Q^\tau}$. The images of P^τ and Q^τ under respectively $\Omega(X)$ and $\Omega(Y)$ are equal, so the images of P and Q under respectively $\Omega(X)$ and $\Omega(Y)$ have identical supports. By point (iii), they are equivalent if and only if they are equal, which gives a decision method. The only expensive step in the above algorithm is the reduction of the sequence $\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q$. An easy induction shows that the length (and therefore the degree) of the sequence $\widetilde{\chi}_P$ is bounded by an exponential in the size of P. By applying 6.9, one obtains that, for terms P, Q with size less than n, the (space) complexity of the reduction of $\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q$ is bounded by a tower of exponentials whose height is itself an exponential w. r. to n (with some care one can obtain 2^n). The same bound holds for the relation $\sqsubset_{LD}$, since $P \sqsubset_{LD} Q$ is equivalent to

$$\mathrm{dil}(\widetilde{\mathbf{N}}(\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q)) > \mathrm{dil}(\widetilde{\mathbf{D}}(\overline{\widetilde{\chi}_P} \bullet \widetilde{\chi}_Q)).$$

For point (ii) we know that the projection of $\sqsubset_{LD}$ onto the free LD-magma $\mathcal{T}_\Sigma / \approx_{LD}$ is a strict ordering, which is linear in the case of one generator. For the general case, one extends the projection of $\sqsubset_{LD}$ to a linear ordering by using the lexicographical extension of an arbitrary linear ordering on the generators. The details use Lemma 1.3. ■

Other corollaries such as the resolution of equations in free LD-magmas, or the lattice structure of the simple extensions of a given term involve new tools and will be developed in forthcoming papers. For the moment we come back to the original question of determining the consequences of left distributivity, *i.e.* completely describing the partial group G_{LD}.

Lemma 3.- *Assume that $(LD)_\xi$ and $(LD)_{\xi'}$ are are defined. The following are equivalent:*

i) $\xi \mathrel{\widetilde{\equiv}} \xi'$ holds;

ii) there exist terms P, Q in $\mathcal{T}_{\mathbf{x}}$ such that both $\Omega(\xi)$ and $\Omega(\xi')$ map P to Q;

iii) $(LD)_\xi \asymp (LD)_{\xi'}$ holds.

Proof. We already observed that (i) implies (iii), so we just have to verify that (ii) implies (i). Assume (ii). By Lemma 2.3, we have

$$\widetilde{\chi}_Q \mathrel{\widetilde{\equiv}} \widetilde{\chi}_P \bullet 0\xi \mathrel{\widetilde{\equiv}} \widetilde{\chi}_P \bullet 0\xi',$$

and therefore $0\xi \mathrel{\widetilde{\equiv}} 0\xi'$ holds. We claim that this equivalence implies (and therefore is equivalent to) $\xi \mathrel{\widetilde{\equiv}} \xi'$. For reduce ξ and ξ' as

$$\xi \mathrel{\widetilde{\equiv}} X \bullet \overline{Y}\ , \qquad \xi' \mathrel{\widetilde{\equiv}} X' \bullet \overline{Y'}.$$

This implies

$$0\xi \mathrel{\widetilde{\equiv}} 0X \bullet \overline{0Y}\ , \qquad 0\xi' \mathrel{\widetilde{\equiv}} 0X' \bullet \overline{0Y'}.$$

By the right quotient property there must exist (positive) sequences Z, Z' satisfying

$$0X \bullet Z \mathrel{\widetilde{\equiv}^+} 0X' \bullet Z' \ , \qquad 0Y \bullet Z \mathrel{\widetilde{\equiv}^+} 0Y' \bullet Z'.$$

By Lemma 2.6 this implies

$$\mathrm{Tr}(0X \bullet Z) \mathrel{\widetilde{\equiv}^+} \mathrm{Tr}(0X' \bullet Z') \ , \qquad \mathrm{Tr}(0Y \bullet Z) \mathrel{\widetilde{\equiv}^+} \mathrm{Tr}(0Y' \bullet Z'),$$

hence

$$X \bullet \mathrm{Tr}(Z) \mathrel{\widetilde{\equiv}^+} X' \bullet \mathrm{Tr}(Z') \ , \qquad Y \bullet \mathrm{Tr}(Z) \mathrel{\widetilde{\equiv}^+} Y' \bullet \mathrm{Tr}(Z').$$

Finally one obtains $X \bullet \overline{Y} \mathrel{\widetilde{\equiv}} X' \bullet \overline{Y'}$, *i.e.* $\xi \mathrel{\widetilde{\equiv}} \xi'$. ■

Theorem 4.- *The relation $\asymp$ is an equivalence relation on C_{LD} which is compatible with the (partial) product, and the mapping $\xi \mapsto (LD)_\xi$ induces an isomorphism of some subset of $\widetilde{B}_\infty$ onto $C_{LD}/\asymp$.*

The proof is immediate from Lemma 3.

Write G_{LD} for the quotient structure $C_{LD}/\asymp$. Then G_{LD} is a 'partial group', and the realisation of G_{LD} as a subset of $\widetilde{B}_\infty$ means that the relations listed in Proposition 1.1 form (in a somehow vague sense) an exhaustive presentation for the distributivity identities.

Remark. Define an LD-category as a category equipped with a bifunctor which is left distributive up to natural isomorphisms. Then the above presentation of $C_{LD}/\asymp$ gives a full solution to the coherence problem associated with LD-categories. The analogue of Mac Lanes's pentagon in the case of associativity ([22]) is here an heptagon.

Denote by $\imath(G_{LD})$ the image of G_{LD} in $\widetilde{B}_\infty$. Then $\imath(G_{LD})$ is determined as the set of the elements which can be written as $\widetilde{\sigma}(X \bullet \overline{Y})$ where X, Y are positive sequences such that the images of $\Omega(X)$ and $\Omega(Y)$ are not disjoint. Observe that any element of $\widetilde{B}_\infty$ is a conjugate of some element in $\imath(G_{LD})$: indeed any element of $\widetilde{B}_\infty$ can be written as $\widetilde{\sigma}(X \bullet \overline{Y})$ where X, Y are positive sequences, and $\widetilde{\sigma}(\overline{Y} \bullet X)$ certainly lies in the image of $\imath$. This image can also be defined in terms of the 'characteristic sequences' $\widetilde{\chi}_P$.

Proposition 5.- *An element of $\widetilde{B}_\infty$ lies in $\imath(G_{LD})$ if and only if it can be represented by a sequence*

$$\prod_{k=\infty}^{1} \overline{1^{k-1}\xi_k} \bullet \prod_{k=1}^{\infty} 1^{k-1}\eta_k$$

where ξ_1, ξ_2, ..., η_1, η_2, ... belong to the image of $\widetilde{\chi}$.

Proof. Assume that $\Omega(\xi)$ maps the term P (of $\mathcal{T}_{\mathbf{x}}$) to Q. We may assume that the right height h of P is Q is large enough so that the rightmost branch in P and Q is the longest branch. Write

$$P = P_1[\dots[P_h]\dots] \ , \qquad Q = Q_1[\dots[Q_h]\dots].$$

By construction $\Omega(\widetilde{\chi}_{P_k})$ maps $\mathbf{x}^{[h-k+1]}$ to $P_k[\mathbf{x}^{[h-k]}]$ for every k between 1 and $h-1$. We deduce

$$\Omega(\widetilde{\chi}_{P_1}) : \mathbf{x}^{[h]} \longmapsto P_1[\mathbf{x}^{[h-1]}]$$
$$\Omega(\widetilde{\chi}_{P_1} \bullet 1\widetilde{\chi}_{P_2}) : \mathbf{x}^{[h]} \longmapsto P_1[P_2[\mathbf{x}^{[h-2]}]]$$
$$\dots$$
$$\Omega(\prod_1^{h-1} 1^{k-1}\widetilde{\chi}_{P_k}) : \mathbf{x}^{[h]} \longmapsto P_1[P_2[\dots[\mathbf{x}]\dots]] = P.$$

Similarly $\Omega(\prod_1^{h-1} 1^{k-1}\widetilde{\chi}_{Q_k})$ maps $\mathbf{x}^{[h]}$ to Q, and the operator associated to the quotient of the latter products map P to Q, as $\Omega(\xi)$ does. By Lemma 3 we conclude that ξ is equivalent to this quotient. ■

Proposition 3.8 invites to study the word problem for the presentation of $\widetilde{B}_\infty$ by means of the right cancellation property for the relation $\widetilde{\equiv}^+$. Although partial results are known (in particular one can show that any generator 1^i is right cancellable for $\widetilde{\equiv}^+$ by lifting the cancellability for $\equiv^+$), no complete proof is known. But the action on terms gives a direct solution.

Proposition 6.- *The word problem for* $(\mathrm{S}^{\mathbf{sym}}, \widetilde{\equiv})$ *is decidable.*

Proof. For ξ in $\mathbf{S}^{\mathbf{sym}}$ the relation $\xi \ \widetilde{\equiv} \ \varepsilon$ is equivalent to $\widetilde{\mathbf{N}}(\xi) \ \widetilde{\equiv} \ \widetilde{\mathbf{D}}(\xi)$, and therefore to $\Omega(\widetilde{\mathbf{N}}(\xi)) = \Omega(\widetilde{\mathbf{D}}(\xi))$. Now for positive sequences X, Y, the equality of $\Omega(X)$ and $\Omega(Y)$ is decided by finding a term P whose support is large enough to guarantee that P belongs to the domains of $\Omega(X)$ and $\Omega(Y)$, and comparing the images of P under these transformations: by Lemma 3, if the operators coincide somewhere, they must coincide everywhere. ■

We finish this section with the description of the kernel of the projection of $\widetilde{B}_\infty$ onto B_∞. We denote by $\sharp$ the section of $\flat$ which maps $i+1$ to 1^i.

Lemma 7.- *i) If X is a positive sequence, there exist positive sequences X_i satisfying*

$$X \ \widetilde{\equiv}^+ \ X^{\flat\sharp} \bullet \prod_i 1^i 0 X_i.$$

ii) If A, B are equivalent positive braid words, there exist positive sequences X_i, Y_i satisfying

$$A^\sharp \bullet \prod_i 1^i 0 X_i \ \widetilde{\equiv}^+ \ B^\sharp \bullet \prod_i 1^i 0 Y_i.$$

The proof is omitted. Let us denote by N_0 the normal subgroup of $\widetilde{B}_\infty$ generated by all $\widetilde{\sigma}_w$ where w begins with 0.

Proposition 8.- *The kernel of the projection of $\widetilde{B}_\infty$ onto B_∞ induced by $\flat$ is N_0.*

Proof. Use Lemma 7 and the fact that N_0 is also the normal subgroup of $\widetilde{B}_\infty$ generated by all $\widetilde{\sigma}_w$ where w contains at least one 0 (and also the normal subgroup generated by the $\widetilde{\sigma}_w$ such that w ends with 0). ■

The structure of N_0 can be described more precisely. Every element of N_0 can be written as a conjugate $ax\overline{a}$ where a lies in the sub*monoid* M of $\widetilde{B}_\infty$ generated by all $\widetilde{\sigma}_{1^i}$ with $i \geq 0$, and x lies in the subgroup K generated by the $\widetilde{\sigma}_w$ where w contains at least one 0. The structures of M and K are exactly known. The monoid M is (isomorphic to) the quotient of N^* under the congruence generated by all pairs $\{i\bullet j, j\bullet i\}$ with $|i-j| \geq 2$. The group K is the direct sum of N copies of $\widetilde{B}_\infty$. Finally one can describe the operation on N_0 in terms of the operations on M and K. Because the product of $ax\overline{a}$ and $ay\overline{a}$ is clearly $axy\overline{a}$, it suffices to explain how $ax\overline{a}$ can be rewritten as $by\overline{b}$. Such a rewriting is possible whenever the projection of a to B_∞^+ divides the projection of b and can be expressed using the operation $\mathbf{J}_R$.

8. Distributive representations of braid groups.

In this section we apply the previous results about free distributive structures to obtain new properties of braid groups using what may be called distributive representations of these groups. This study results in a close connection between the braid group B_∞ and the free LD-magma with one generator.

The braid groups act on distributive structures (see *e.g.* [2]). Assume first that $\mathfrak{g}$ is any set equipped with a bracket, and define a right action $\Theta_\mathfrak{g}$ of positive braid words (*i.e.* elements of N_+) on sequences from $\mathfrak{g}$ by

$$\Theta_\mathfrak{g}(i) : \langle a_1, a_2, \ldots\rangle \longmapsto \langle a_1, a_2, \ldots, \alpha_i[a_{i+1}], a_i, a_{i+2}, \ldots\rangle.$$

The congruence $\equiv^+$ is compatible with this action if and only if the bracket on $\mathfrak{g}$ is left distributive. Indeed the first component of the images of $\langle a_1, a_2, \ldots\rangle$ under $2\bullet1\bullet2$ and $1\bullet2\bullet1$ are respectively $a_1[a_2[a_3]]$ and $a_1[a_2][a_1[a_3]]$.

Remark. The heptagonal identity is another expression of the existence of the action above. Denote by F the mapping of $\mathcal{T}_\Sigma$ to $\mathcal{T}_\Sigma^{\mathrm{N}}$ defined by

$$F : P \mapsto \langle \mathbf{S}_0(P), \mathbf{S}_{10}(P), \mathbf{S}_{110}(P), \ldots \rangle$$

(take $\boldsymbol{x}$ when $\mathbf{S}_{1^i0}(P)$ is no longer defined). Then $\Theta_{\mathcal{T}_\Sigma}(i)$ is the image of $\Omega(1^{i-1})$ under F: if $\Omega(1^{i-1})$ maps P to Q, then $\Theta_{\mathcal{T}_\Sigma}(i)$ maps $F(P)$ to $F(Q)$. Because the bracket on $\mathcal{T}_\Sigma$ is not left distributive, the operators $\Theta_{\mathcal{T}_\Sigma}(i \bullet i{-}1 \bullet i)$ and $\Theta_{\mathcal{T}_\Sigma}(i{-}1 \bullet i \bullet i{-}1)$ do not coincide, but, if $\langle Q_1, Q_2, \ldots \rangle$ and $\langle Q'_1, Q'_2, \ldots \rangle$ are the respective images of some sequence $\langle P_1, P_2, \ldots \rangle$, the existence of the action on LD-magmas means that there must exist, for every $k \geq 1$, a sequence ξ_k (possibly depending on P) such that $\Omega(\xi_k)$ maps Q_k to Q'_k. The choice

$$\xi_j = \begin{cases} \Lambda & \text{if } j = i \ , \\ \varepsilon & \text{otherwise} \ , \end{cases}$$

is convenient and gives rise to the relation

$$\Omega(1^{i-1} \bullet 1^i \bullet 1^{i-1}) = \Omega(1^i \bullet 1^{i-1} \bullet 1^i \bullet 1^{i-1}0)$$

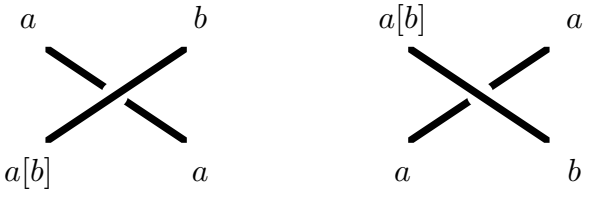
(and more generally to the formula of Lemma 7.7).

The natural hypothesis for extending the action to arbitrary braids is to assume that left translations in the LD-magma $\mathfrak{g}$ are bijective, so that $\mathfrak{g}$ is an *automorphic set* (in [2]) or a *rack* (in [11]). Actually, if we only assume that left translations in $\mathfrak{g}$ are injective, *i.e.* that $\mathfrak{g}$ is a left cancellative LD-magma, we obtain a partial but welldefined action of arbitrary sequences by

$$\Theta_{\mathfrak{g}}(\bar{\imath}) : \langle a_1, a_2, \ldots \rangle \longmapsto \langle a_1, a_2, \ldots, a_{i+1}, c, a_{i+2}, \ldots \rangle$$

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

The geometrical meaning of the action $\Theta_{\mathfrak{g}}$ is clear. We associate with the strings of the braids labels which belong to $\mathfrak{g}$, and these labels change at each crossing according to the rules



In the sequel the sequences in $\mathfrak{g}^{\mathrm{N}}$ are called $\mathfrak{g}$-labellings, and we say that a $\mathfrak{g}$-labelling $\vec{\boldsymbol{a}}$ is *admissible* for the braid word α if $\vec{\boldsymbol{a}}$ belongs to the domain of $\Theta_{\mathfrak{g}}(\alpha)$. The corresponding image is denoted by $(\vec{\boldsymbol{a}})^\alpha$.

Lemma 1.- *Assume that $\mathfrak{g}$ is a left cancellative LD-magma. For every finite family of braid words α_1, ..., α_p, there exists a $\mathfrak{g}$-labelling which is admissible for α_1, ..., α_p. Moreover $\alpha \equiv \alpha'$ implies $(\vec{\boldsymbol{c}})^{\alpha} = (\vec{\boldsymbol{c}})^{\alpha'}$ for every $\mathfrak{g}$-labelling $\vec{\boldsymbol{c}}$ which is both α- and α'-admissible.*

Proof. If A, B are positive words, then $\Theta_{\mathfrak{g}}(A)$ and $\Theta_{\mathfrak{g}}(B)$ are defined everywhere on $\mathfrak{g}^{\mathrm{N}}$. 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 $((\vec{\boldsymbol{a}})^{A})^{\bar{A}}$ is $\vec{\boldsymbol{a}}$. We claim that, if α is L-reducible (= reducible on the left) to β, then $\Theta_{\mathfrak{g}}(\alpha)$ includes $\Theta_{\mathfrak{g}}(\beta)$ (as a set of pairs). This will show that $\Theta_{\mathfrak{g}}(\alpha)$ includes $\Theta_{\mathfrak{g}}(\overline{\mathbf{D}_{L}(\alpha)}{\bullet}\mathbf{N}_{L}(\alpha))$, and therefore that the domain of $\Theta_{\mathfrak{g}}(\alpha)$ includes the image of $\Theta_{\mathfrak{g}}(\mathbf{D}_{L}(\alpha))$. To prove the claim, we may assume that α is 1-reducible to β, and even that α is $i{\bullet}\overline{j}$ for some nonnegative integers i, j. The critical case is for $|i-j|=1$. Assume *e.g.* $\alpha = 1{\bullet}\overline{2}$, so that β is $\overline{2}{\bullet}\overline{1}{\bullet}2{\bullet}1$. The hypothesis that $\langle a_1, a_2, \ldots\rangle$ is admissible for $\overline{2}{\bullet}\overline{1}$ implies that there exist c_1 and c_2 in $\mathfrak{g}$ satisfying $a_2 = a_3[c_2]$ and $a_1 = a_3[c_1]$. It follows that $\langle a_1[a_2], a_1, a_3, \ldots\rangle$ is admissible for $\overline{2}$, and one has

$$(\langle a_1, a_2, a_3, a_4, \ldots\rangle)^{1{\bullet}\overline{2}} = \langle a_1[a_2], a_3, c_1, a_4, \ldots) = (\langle a_1, a_2, a_3, a_4, \ldots\rangle)^{\overline{2}{\bullet}\overline{1}{\bullet}2{\bullet}1}.$$

For the extension to several words α_1, ..., α_p, we just have to verify that the images of $\Theta_{\mathfrak{g}}(\mathbf{D}_{L}(\alpha_1))$, ..., $\Theta_{\mathfrak{g}}(\mathbf{D}_{L}(\alpha_p))$ cannot be disjoint. But the intersection of these images include the image of $\Theta_{\mathfrak{g}}(A)$, where A is the left lowest common multiple of $\mathbf{D}_{L}(\alpha_1))$, ..., $\mathbf{D}_{L}(\alpha_p))$ (*i.e.* their product w. r. to $\mathbf{J}_{L}$).

A similar argument shows that, if α is R-reducible (= reducible on the right) to β, then $\Theta_{\mathfrak{g}}(\alpha)$ is included in $\Theta_{\mathfrak{g}}(\beta)$. Now assume that α and α' are $\equiv$-equivalent and $\vec{\boldsymbol{a}}$ is admissible for α and α'. There exist positive sequences A, B, A', B' such that α is R-reducible to $A{\bullet}\overline{B}$ and α' is R-reducible to $A'{\bullet}\overline{B'}$. By the right quotient property there exist positive sequences C, C' satisfying $A{\bullet}C \equiv A'{\bullet}C'$ and $B{\bullet}C \equiv B'{\bullet}C'$. Now $\vec{\boldsymbol{a}}$ is admissible for $A{\bullet}\overline{B}$ and $A'{\bullet}\overline{B'}$. Using the invariance of $\Theta_{\mathfrak{g}}$ with respect to equivalence of positive sequences we have

$$(\vec{\boldsymbol{a}})^{\alpha} = (\vec{\boldsymbol{a}})^{A{\bullet}\overline{B}} = ((\vec{\boldsymbol{a}})^{A{\bullet}C})^{\overline{C}{\bullet}\overline{B}} = ((\vec{\boldsymbol{a}})^{A'{\bullet}C'})^{\overline{C'}{\bullet}\overline{B'}} = (\vec{\boldsymbol{a}})^{A'{\bullet}\overline{B'}} = (\vec{\boldsymbol{a}})^{\alpha'}.$$

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 $\vec{\boldsymbol{a}}$ is admissible for all intermediate terms. ■

Thus the image of a $\mathfrak{g}$-labelling under a braid is welldefined when it exists. The Burau representation and therefore the Alexander polynomial of a braid can be constructed using the labellings associated with the barycentric LD-magma whose bracket is defined by

$$a[b] = (1-t)a + tb,$$

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

The specific properties of the free LD-magmas (which are now known to be left cancellative), in particular the existence of linear orderings, lead to new applications. In the sequel $\mathfrak{f}$ denotes the free LD-magma with one generator, and $<_{\mathfrak{f}}$ denotes its canonical linear ordering (*c.f.* Theorem 7.2). The class of the term P in $\mathfrak{f}$ is denoted by $\dot{P}$.

Definition.- A braid is *σ_i-positive* if it has a decomposition (w. r. 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. Let $\langle a_1^0, a_2^0, \ldots\rangle$ be an α-admissible $\mathfrak{f}$-labelling. Define inductively sequences $\langle a_1^p, a_2^p, \ldots\rangle$ by

$$\langle a_1^{p+1}, a_2^{p+1}, \ldots\rangle = \langle a_1^p, a_2^p, \ldots\rangle^{x_p},$$

where $x_1,\ldots,x_n$ are the successive elements of α (in $\mathbf{N}_+ \cup \overline{\mathbf{N}}_+$). By applying the distributivity one obtains

$$a_1^{p+1}[\ldots[a_i^{p+1}[\dot{\boldsymbol{x}}]]\ldots] = \begin{cases} a_1^p[\ldots[a_i^p[\dot{\boldsymbol{x}}]]\ldots] & \text{if } x_p \neq i, \overline{i}, \\ a_1^p[\ldots[a_i^p[a_{i+1}^p][\dot{\boldsymbol{x}}]]\ldots] & \text{if } x_p = i. \end{cases}$$

Now for any a_1, …, a_{i+1} in $\mathfrak{f}$, one has

$$a_i <_{\mathfrak{f}} a_i[a_{i+1}]$$

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

$$a_i[\dot{\boldsymbol{x}}] <_{\mathfrak{f}} a_i[a_{i+1}][\dot{\boldsymbol{x}}]$$

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

$$a_1[\ldots[a_i[\dot{\boldsymbol{x}}]]\ldots] <_{\mathfrak{f}} a_1[\ldots[a_i[a_{i+1}][\dot{\boldsymbol{x}}]]\ldots]$$

because $<_{\mathfrak{f}}$ is compatible with bracket on the left. If i occurs in α but $\overline{i}$ does not, we deduce

$$a_1^0[a_2^0[\ldots[a_i^0[\dot{\boldsymbol{x}}]]\ldots]] <_{\mathfrak{f}} a_1^n[a_2^n[\ldots[a_i^n[\dot{\boldsymbol{x}}]]\ldots]],$$

while $\alpha \equiv \varepsilon$ would imply $a_k^0 = a_k^n$ for every k, and therefore

$$a_1^0[a_2^0[\ldots[a_i^0[\dot{\boldsymbol{x}}]]\ldots]] = a_1^n[a_2^n[\ldots[a_i^n[\dot{\boldsymbol{x}}]]\ldots]],$$

a contradiction. ■

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.)

So far we introduced a representation of B_∞ using $\mathfrak{f}$. Conversely we can apply the previous result to represent $\mathfrak{f}$ in B_∞. In the sequel, we denote by s the 'shift' endomorphism of B_∞ which maps every σ_i to the corresponding σ_{i+1}.

Proposition 3.- *The bracket on B_∞ defined by*

$$x[y] = x.s(y).\sigma_1.\overline{s(x)}$$

is left distributive and irreflexive. Thus the closure of any braid under this bracket is free.

Proof. The bracket on B_∞ is the projection under (the morphism induced by) $\flat$ of the bracket defined in Section 2 on $\widetilde{B}_\infty$. Because the kernel of this morphism, which is N_0, includes the subgroup H_0, the bracket must be left distributive. For irreflexivity, we obtain as in 2.5

$$\overline{x}.(x[y_1]\ldots[y_k]) = s(y_1).\sigma_1.s(\overline{x}.y_2).\sigma_1.s(x[y_1])\ldots s(y_k).\sigma_1.s(\overline{x[y_1]\ldots[y_{k-1}]}).$$

The second member is σ_1-positive for $k \geq 1$, so by Proposition 2 the equality

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

is impossible. One concludes using Lemma 1.6. ■

The property of braids stated as Proposition 2 is a topological version of the Irreflexivity Conjecture. Indeed it implies the above construction of an irreflexive LD-magma, and therefore by 1.6 the conjecture itself. Thus a direct argument for Proposition 2 could replace the construction of Sections 2 to 6 for the Irreflexivity Conjecture (but not for the more precise results of 7.2.ii and 7.4). No such proof is known up to now. Observe that we cannot replace the subgroup H_0 by the normal subgroup N_0 in 2.4 in order to complete the proof of irreflexivity inside B_∞: some elements of N_0 have sign $+1$, and thus N_0 cannot be directly separated from $(H_1.\widetilde{\sigma}_\Lambda)^k.H_1$ using the argument of Proposition 2.7.

Remark. The quotients of B_∞ inherit the left distributive structure when 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 [6]. It is known that the corresponding monogenic LD-magmas $\mathfrak{d}$ 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 $a[b] = b + 1$.

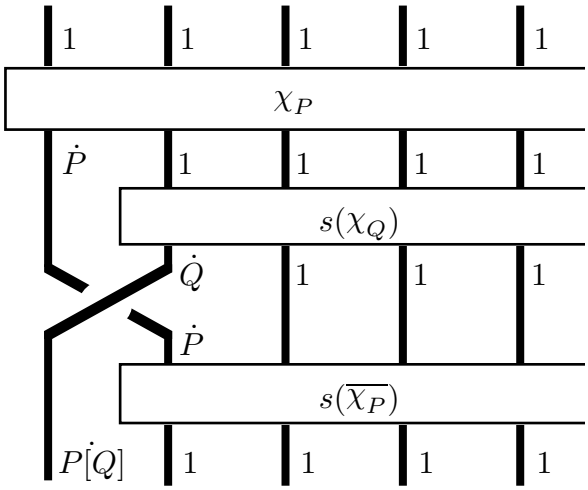
For P in $\mathcal{T}_{\mathbf{x}}$, we denote by χ_P the braid word inductively defined by

$$\chi_{\mathbf{x}} = \varepsilon,$$
$$\chi_{P[Q]} = \chi_P \bullet s(\chi_Q) \bullet 1 \bullet \overline{s(\chi_P)}$$

(using s for words with the obvious meaning). Proposition 3 tells that the terms P, Q are $\approx_{LD}$-equivalent terms if and only if the braid words χ_P and χ_Q are $\equiv$-equivalent. The image of χ is the free sub-LD-magma of B_∞ generated by 1. It will be simply denoted $\mathfrak{f}$, so that $\dot{P}$ is exactly $\sigma(\chi_P)$ for every term P. Observe that χ_P is the projection of $\widetilde{\chi}_P$ under $\flat$, and that this projection is but a copy since all factors in $\widetilde{\chi}_P$ have the form 1^i or $\overline{1^i}$. The figure below illustrates the inductive definition of the words χ_P and the formula

$$\langle 1, 1, 1, \ldots \rangle^{\chi_P} = \langle \dot{P}, 1, 1, \ldots \rangle$$

which immediately follows.



The above results give an immediate solution to the problem of defining canonical representatives with respect to the congruence $\approx_{LD}$: use any normal form of the braid word χ_P as a representative for the class of the term P. This however is only a partial solution which does not diminish the interest of the results in [20] and [21] since it does not select a distinguished term in each class (the usual normal forms of a χ_P braid word need not be χ_P words themselves).

Theorem 4.- *The relation $\approx_{LD}$ on $\mathcal{T}_{\mathbf{x}}$ lies in the complexity class $EXPTIME$.*

Proof. The length of $\chi(P)$ is bounded by an exponential w. r. to the size of P, since the inductive definition gives

$$\text{length}(\chi_{P[Q]}) = 2.\text{length}(\chi_P) + \text{length}(\chi_Q) + 1.$$

Braid comparison has a polynomial complexity. ■

Extension to the multivariate case would require a similar realization for free LD-magmas with several generators. No such realization is known, so that the only presently known upper bound for comparison of arbitrary terms remains the primitive recursive bound stated in Theorem 7.2.

Definition.- An ɟ-labelling is *finite* if it has only finitely many components not equal to 1. The constant labelling $\langle 1, 1, \ldots\rangle$ is denoted $\vec{\boldsymbol{1}}$. For $\langle a_1, a_2, \ldots\rangle$ a finite ɟ-labelling, one sets

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

Lemma 5.- *i) For every finite ɟ-labelling $\vec{\boldsymbol{c}}$, there exists a braid word γ such that $\sigma(\gamma) = \Pi(\vec{\boldsymbol{c}})$ and $(\vec{\boldsymbol{1}})^{\gamma} = \vec{\boldsymbol{c}}$.*
ii) The equality

$$\Pi((\vec{\boldsymbol{c}})^{\alpha}) = \Pi(\vec{\boldsymbol{c}}).\sigma(\alpha)$$

holds for every braid word α and every α-admissible finite ɟ-labelling $\vec{\boldsymbol{c}}$.

Proof. i) Assume that $\vec{\boldsymbol{c}}$ is $\langle c_1, c_2, \ldots\rangle$ and choose terms R_1, R_2,... such that c_k is $\sigma(\chi_{R_k})$ for $k \geq 1$. We observed that the labelling $\vec{\boldsymbol{1}}$ is admissible for χ_{R_k} and that $(\vec{\boldsymbol{1}})^{\chi_{R_k}}$ is $\langle c_k, 1, 1, \ldots\rangle$. So we have we obtain

$$(\vec{\boldsymbol{1}})^{\chi_{R_1} \bullet s(\chi_{R_2})} = \langle c_1, c_2, 1, \ldots\rangle,$$

and the formula with $\gamma = \prod_k s^{k-1}(\chi_{R_k})$ follows using an easy induction.
ii) It suffices to prove the formula for the case of a single factor say i. Now

$$\begin{aligned}
\Pi(\langle c_1, c_2, \ldots\rangle^i) &= \Pi(\langle c_1, c_2, \ldots, c_i[c_{i+1}], c_i, c_{i+2}, \ldots\rangle \\
&= c_1.s(c_2)\ldots s^{i-1}(c_i[c_{i+1}]).s^i(c_i).s^{i+1}(c_{i+2})\ldots \\
&= c_1.s(c_2)\ldots s^{i-1}(c_i).s^i(c_{i+1}).\sigma_i.s^i(\overline{c_i}).s^i(c_i).s^{i+1}(c_{i+2})\ldots \\
&= c_1.s(c_2)\ldots s^{i-1}(c_i).s^i(c_{i+1}).\sigma_i.s^{i+1}(c_{i+2})\ldots \\
&= \Pi(\langle c_1, c_2, \ldots\rangle).\sigma_i,
\end{aligned}$$

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

Proposition 6.- *i) The partial action $\Theta_{\mathfrak{f}}$ is strongly faithful in the following sense: if there exists at least one finite ɟ-labbeling $\vec{\boldsymbol{c}}$ which is both α- and α'-admissible and $(\vec{\boldsymbol{c}})^{\alpha}$ is equal to $(\vec{\boldsymbol{c}})^{\alpha'}$, then $\alpha \equiv \alpha'$ holds.*

ii) The mapping Π is injective, and every positive braid has a unique expression as $\Pi(\vec{\boldsymbol{a}})$ where $\vec{\boldsymbol{a}}$ is a finite ɟ-labelling which is $\vec{\boldsymbol{1}}$-admissible.

Proof. The first point follows from the formula in Lemma 5.ii, which also shows that any braid $\sigma(\alpha)$ can be expressed as the quotient of two braids in the image of Π. In particular, if A is a positive word, $\sigma(A) = (\vec{\boldsymbol{1}})^A$ holds. The injectivity of Π follows from the formula of Lemma 5.i. ■.

Using RL-numerator and denominator, one obtains a canonical decomposition for an arbitrary braid as the quotient of two braids in the image of Π, *i.e.* as the quotient of two finite sequences in $\mathfrak{f}$. Observe that the decomposition so described corresponds to some combing of the braids, and is very easily obtained: for a positive word A, apply $\Theta_{\mathfrak{f}}(A)$ to the sequence $\vec{\boldsymbol{1}}$ (*i.e.* apply $\Omega(A^\sharp)$ to $\boldsymbol{x}^{[n]}$ for n large enough), and determine the corresponding χ-sequences. Actually we do not obtain in this way normal forms in B_∞ or B_∞^+ since a normal decomposition for the elements of $\mathfrak{f}$ presupposes a normal decomposition of braids (or alternatively a direct normal form for terms w. r. to $\approx_{LD}$, like in [20] or [21]). Observe also that B_∞^+ is included in the image of Π, but that the converse inclusion is false: for instance $1[1][1]$ is $\sigma_1^2\sigma_2^{-1}$, which cannot be expressed by a positive word.

In Section 4 we proved that the divisibility relation induces a (semi)lattice structure on B_∞^+. The extension of this partial ordering to B_∞ is also introduced and intensively used in [23] and [10]. The distributive representations of B_∞ enable to extend this partial ordering to a *linear* ordering. We begin with two lemmas about positive braids.

Definition.- Two terms P, Q in $\mathcal{T}_\Sigma$ are *strongly inequivalent* if they have the form

$$P = R_1[\ldots[R_p[\boldsymbol{y}]]\ldots] \ , \qquad Q = R_1[\ldots[R_p[\boldsymbol{z}]]\ldots]$$

where $\boldsymbol{y}$ and $\boldsymbol{z}$ are distinct variables.

Because the rightmost variable in a term is $\approx_{LD}$-invariant, strongly inequivalent terms must be inequivalent.

Lemma 7.- *Assume that P', Q' are strongly inequivalent and satisfy $P' \sqsubset_{LD} P$ and $Q' \sqsubset_{LD} Q$. Then P and Q are not equivalent.*

Proof. Assume $P \approx_{LD} Q$. By three calls to Lemma 1.3 there exists a common extension R of P and Q such that some iterated left subterms of R say P'' and Q'' are extensions of P' and Q' respectively. Let $\boldsymbol{y}$ (*resp.* $\boldsymbol{z}$) be the rightmost variable of P' and P'' (*resp.* Q' and Q''). The terms P'' and Q'' cannot coincide since they dont have the same rightmost variable. Assume $P'' \sqsubset Q''$. Let $\widehat{Q''}$ be the term obtained from Q'' by replacing the rightmost occurrence of $\boldsymbol{z}$ by $\boldsymbol{y}$. Now $\widehat{Q''}$ is equivalent to the term obtained from Q' by replacing the rightmost occurrence of $\boldsymbol{z}$ by $\boldsymbol{y}$, which is P' by hypothesis. So $\widehat{Q''}$ must be equivalent to its (strict) prefix P'', contradicting the irreflexivity of $\sqsubset_{LD}$. ■

If $\prec$ is any relation on a set X, $\prec^*$ denotes the lexicographical extension of $\prec$ to X^{N}: $\langle x_1, x_2, \ldots\rangle \prec^* \langle y_1, y_2, \ldots\rangle$ holds if $x_i \prec y_i$ holds for the minimal i such that x_i and y_i are not equal.

Lemma 8.- *For every positive braid words A, B, the inequality $(\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B$ holds if and only if the inequality $(\vec{\boldsymbol{c}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^B$ holds for at least one finite $\mathfrak{f}$-labelling $\vec{\boldsymbol{c}}$ if and only if this inequality holds for every finite $\mathfrak{f}$-labelling $\vec{\boldsymbol{c}}$.*

Proof. Assume $(\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B$. We denote by $\mathfrak{f}_\Sigma$ the free LD-magma $\mathcal{T}_\Sigma/\approx_{LD}$. The relation $\sqsubset_{LD}$ induces a (strict) partial ordering denoted $<_{\mathfrak{f}_\Sigma}$ on $\mathfrak{f}_\Sigma$. We claim that

$$\langle \dot{\boldsymbol{x}}_1, \dot{\boldsymbol{x}}_2, \ldots\rangle^A <_{\mathfrak{f}_\Sigma}^* \langle \dot{\boldsymbol{x}}_1, \dot{\boldsymbol{x}}_2, \ldots\rangle^B$$

holds, where $\dot{P}$ denotes the class P in $\mathfrak{f}_\Sigma$. Any mapping of Σ into $\mathfrak{f}$ extends to a morphism of $\mathfrak{f}_\Sigma$ into $\mathfrak{f}$ which is compatible with the orderings $<_{\mathfrak{f}_\Sigma}$ and $<_{\mathfrak{f}}$, so for every $\mathfrak{f}$-labelling $\langle c_1, c_2, \ldots\rangle$ we deduce

$$(\langle c_1, c_2, \ldots\rangle)^A <_{\mathfrak{f}}^* (\langle c_1, c_2, \ldots\rangle)^B$$

from the inequality above by mapping $\boldsymbol{x}_i$ to c_i.

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 $\boldsymbol{x}_1[\boldsymbol{x}_2[\ldots[\boldsymbol{x}_n]\ldots]]$ under $\Omega(A^\sharp)$ and $\Omega(B^\sharp)$, and write P_k (*resp.* Q_k) for the subterm $\mathbf{S}_{1^{k-1}0}(P)$ (*resp.* $\mathbf{S}_{1^{k-1}0}(Q)$). The substitution which maps every variable to $\boldsymbol{x}$ is denoted τ. The hypothesis implies (and actually is equivalent to) $P^\tau \ {\sqsubset_{LD}}^* \ Q^\tau$, and we have to prove $P \ {\sqsubset_{LD}}^* \ Q$.

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

$$(\langle \dot{\boldsymbol{x}}_1, \dot{\boldsymbol{x}}_2, \ldots\rangle)^A = (\langle \dot{\boldsymbol{x}}_1, \dot{\boldsymbol{x}}_2, \ldots\rangle)^B$$

which projects onto $P^\tau \approx_{LD} Q^\tau$, contradicting the hypothesis. For $k < i$ the equivalence $P_k \approx_{LD} Q_k$ projects onto ${P_k}^\tau \approx_{LD} {Q_k}^\tau$. Because of the comparison property for $\sqsubset_{LD}$, three cases may occur.

If ${Q_i}^\tau \ \sqsubset_{LD} \ {P_i}^\tau$ holds, we obtain $Q^\tau \ {\sqsubset_{LD}}^* \ P^\tau$, which contradicts the hypothesis.

If ${P_i}^\tau \approx_{LD} {Q_i}^\tau$ holds, choose positive sequences Z, Z' such that $\Omega(Z)$ and $\Omega(Z')$ maps ${P_i}^\tau$ and ${Q_i}^\tau$ respectively to a common extension R. Assume that $\Omega(Z)$ maps P_i to P', and $\Omega(Z')$ maps Q_i to Q'. The terms R, P', Q' have the same support, so because P' and Q' are not equivalent, they must have a 'variable disagreeement', *i.e.* there exist terms R_1,...,R_p and distinct variables $\boldsymbol{y}$, $\boldsymbol{z}$ such that the patterns $R_1[\ldots[R_p[\boldsymbol{y}$ and $R_1[\ldots[R_p[\boldsymbol{z}$ are prefixes of the *words* P' and Q'. This easily implies

$$R_1[\ldots[R_p[\boldsymbol{y}]]\ldots] \ \sqsubset_{LD} \ P' \text{ and } R_1[\ldots[R_p[\boldsymbol{z}]]\ldots] \ \sqsubset_{LD} \ Q',$$

whence

$$R_1[\ldots[R_p[\boldsymbol{y}]]\ldots] \sqsubset_{LD} P_i \text{ and } R_1[\ldots[R_p[\boldsymbol{z}]]\ldots] \sqsubset_{LD} Q_i.$$

Therefore one has

$$P_1[\ldots[P_{i-1}[R_1[\ldots[R_p[\boldsymbol{y}]]\ldots]]]\ldots] \sqsubset_{LD} P$$

and

$$P_1[\ldots[P_{i-1}[R_1[\ldots[R_p[\boldsymbol{z}]]\ldots]]]\ldots] \sqsubset_{LD} Q.$$

By Lemma 7, this contradicts the equivalence $P \approx_{LD} Q$ which holds by construction.

So necessarily the only remaining possibility, which is ${P_i}^\tau \sqsubset_{LD} {Q_i}^\tau$, holds. As above, choose positive sequences Z, Z' such that $\Omega(Z)$ and $\Omega(Z')$ maps ${P_i}^\tau$ and ${Q_i}^\tau$ respectively to terms R, S such that one is a strict prefix of the other one. Assume $R \sqsubset S$. Assume that $\Omega(Z)$ 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 disagreeement'. As above the latter case is impossible. So $P_i \sqsubset_{LD} Q_i$ holds, which implies $P \sqsubset_{LD}{}^* Q$, and proves the claim.

It follows that, for any pair of positive sequences A, B, either $(\vec{\boldsymbol{c}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^B$ holds for every $\vec{\boldsymbol{c}}$, or $(\vec{\boldsymbol{c}})^A = (\vec{\boldsymbol{c}})^B$ holds for every $\vec{\boldsymbol{c}}$, or $(\vec{\boldsymbol{c}})^B <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^A$ holds for every $\vec{\boldsymbol{c}}$. So if $(\vec{\boldsymbol{c}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^B$ holds for at least one $\vec{\boldsymbol{c}}$, necessarily it holds for every $\vec{\boldsymbol{c}}$, and in particular for $\vec{\boldsymbol{1}}$. The proof of Lemma 8 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* w. r. to X if $x \prec yay^{-1}$ holds for every x, y in the subgroup generated by X.

Theorem 9.- *i) There exists a unique ordering $<$ on the braid group B_∞ which is compatible with the left translations and such that, for every i, the generator σ_i is infinitely large w. r. 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 $\mathfrak{f}$. There exists a primitive recursive algorithm for comparing braid words w. r. to $<$.
iii) For any braid words α, β, the inequality $\sigma(\alpha) < \sigma(\beta)$ holds if and only if $(\vec{\boldsymbol{c}})^\alpha <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^\beta$ holds for every $\mathfrak{f}$-labelling $\vec{\boldsymbol{c}}$ which is admissible for α and β if and only if this inequality holds for at least one such $\mathfrak{f}$-labelling.

Proof. Denote by B_∞^{++} the set of all $\sigma(\overline{A}\bullet B)$ where A, B are positive words satisfying $(\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B$. Clearly B_∞^+ is included in B_∞^{++}, and, because $<_{\mathfrak{f}}^*$ is irreflexive, 1 does not belong to B_∞^{++}. We observe that x lies in B_∞^{++} if and only if $(\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B$ holds for *every* expression of x as $\sigma(\overline{A}\bullet B)$ with A, B positive braid words. For if $\overline{A}\bullet B$ and $\overline{A'}\bullet B'$ are equivalent, there exist positive words C, C' satisfying

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

and by Lemma 8 we have the equivalences

$$\begin{aligned}(\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B \iff ((\vec{\boldsymbol{1}})^C)^A <_{\mathfrak{f}}^* ((\vec{\boldsymbol{1}})^C)^B \\ \iff ((\vec{\boldsymbol{1}})^{C'})^{A'} <_{\mathfrak{f}}^* ((\vec{\boldsymbol{1}})^{C'})^{B'} \iff (\vec{\boldsymbol{1}})^A <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^B.\end{aligned}$$

Now 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 8 again, we have

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

and this shows that B_∞^{++} is stable under product. Therefore the relation $<$ defined on B_∞ by

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

is a strict ordering which is compatible with left translations and extends the left divisibility partial ordering (defined similarly by $x^{-1}y \in B_\infty^+$). Moreover the ordering $<$ is linear on B_∞ because $<_{\mathfrak{f}}^*$ is a linear ordering and every braid can be written as $\sigma(\overline{A}\bullet B)$ for some positive words A, B. And because $(\vec{\boldsymbol{1}})^\alpha = \langle a_1, a_2, \ldots\rangle$ implies $\langle\vec{\boldsymbol{1}}\rangle^{s(\alpha)} = \langle 1, a_1, a_2, \ldots\rangle$, the set B_∞^{++} is stable under s and $x < y$ is equivalent to $s(x) < s(y)$.

We claim that the inequality $s(x) < s(y)\sigma_1 s(z)$ holds for every x, y, z. It suffices to show that any σ_1-positive word belongs to B_∞^{++}. Now if $\sigma(\gamma)$ is σ_1-positive and if $\vec{\boldsymbol{a}}$ is any γ-admissible $\mathfrak{f}$-labelling, the proof of Proposition 2 shows the inequality $\vec{\boldsymbol{a}} <_{\mathfrak{f}}^* (\vec{\boldsymbol{a}})^\gamma$. Since $<$ is a linear ordering, we can deduce $1 < \gamma$ provided that $\alpha \in B_\infty^{++}$ implies the existence of at least one α-admissible labelling $\vec{\boldsymbol{c}}$ satisfying $\vec{\boldsymbol{c}} <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^\alpha$. Let $\vec{\boldsymbol{c}}$ be $(\vec{\boldsymbol{1}})^{\mathbf{D}_L(\alpha)}$: $\vec{\boldsymbol{c}}$ is $(\overline{\mathbf{D}_L(\alpha)}\bullet\mathbf{N}_L(\alpha))$-admissible, and one has

$$\vec{\boldsymbol{c}} = (\vec{\boldsymbol{1}})^{\mathbf{D}_L(\alpha)} <_{\mathfrak{f}}^* (\vec{\boldsymbol{1}})^{\mathbf{N}_L(\alpha)} = (\vec{\boldsymbol{c}})^{\overline{\mathbf{D}_L(\alpha)}\bullet\mathbf{N}_L(\alpha)}.$$

But α is L-reducible to $\overline{\mathbf{D}_L(\alpha)}\bullet\mathbf{N}_L(\alpha)$, so by the proof of Lemma 1 we know that $\vec{\boldsymbol{c}}$ is α-admissible and that $(\vec{\boldsymbol{c}})^\alpha$ is equal to $(\vec{\boldsymbol{c}})^{\overline{\mathbf{D}_L(\alpha)}\bullet\mathbf{N}_L(\alpha)}$. Thus σ_1 is infinitely large w. r. to the image of s, and therefore w. r. 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.

According to the definition of B_∞^{++}, the comparison of $\sigma(\alpha)$ to 1 consists in reducing α on the left, applying $\Theta_{\mathfrak{f}}(\mathbf{D}_L(\alpha))$ and $\Theta_{\mathfrak{f}}(\mathbf{N}_L(\alpha))$ to $\vec{\boldsymbol{1}}$ and comparing the results w. r. to $<_{\mathfrak{f}}^*$. The last two steps respectively correspond to applying the transformations $\Omega(\mathbf{D}_L(\alpha)^\sharp)$ and $\Omega(\mathbf{N}_L(\alpha)^\sharp)$ to a term $\boldsymbol{x}^{[n]}$ with n large enough, and comparing the successive right subterms of the images w. r. to $\sqsubset_{LD}$ using the reduction in $\widetilde{B}_\infty$ of the associated $\widetilde{\chi}$-sequences. By Theorem 7.2 the complexity of this method is bounded by a tower of exponentials.

In order to prove the uniqueness, assume that $<'$ is any ordering on B_∞ which is compatible with left translations and such that σ_i is infinitely large w. r. to the family of all σ_k with $k > i$. We claim that $1 <' x$ holds for every σ_1-positive braid x. This is proved using induction on the number k of σ_1 in a decomposition of x. For $k = 1$, $s(z'^{-1}z^{-1}) <' s(z'^{-1}\sigma_1 s(z')$ implies $1 <' s(z)\sigma_1 s(z')$. For the induction, $1 <' y$ implies $s(z)\sigma_1 <' s(z)\sigma_1 y$ and therefore $1 <' s(z)\sigma_1 y$ since $1 <' s(z)\sigma_1$ holds.

Assume now that a, b belong to $\mathfrak{f}$ and $\alpha <_{\mathfrak{f}} b$ holds. We can choose terms P, Q such that a is $\sigma(\chi_P)$, b is $\sigma(\chi_Q)$ and $P \sqsubset Q$ holds. By the computation of Proposition 3, we know that $a^{-1}b$ (which is $\sigma(\overline{\chi_P}\bullet\chi_Q)$) is σ_1-positive. By the previous claim, $1 <' a^{-1}b$, and therefore $a <' b$, hold. So $<_{\mathfrak{f}}$ is the restriction of $<'$ to $\mathfrak{f}$. Moreover we observe that, under the same hypotheses, $as(x) <' bs(y)$ holds for every x, y, since $s(x^{-1})a^{-1}bs(y)$ is σ_1-positive as well. We deduce the implication

$$\langle a_1, a_2, \ldots\rangle <_{\mathfrak{f}}^* \langle b_1, b_2, \ldots\rangle \Longrightarrow \Pi(\langle a_1, a_2, \ldots\rangle) <' \Pi(\langle b_1, b_2, \ldots\rangle)$$

for all finite $\mathfrak{f}$-labellings $\langle a_1, a_2, \ldots\rangle$, $\langle b_1, b_2, \ldots\rangle$. Indeed the case of $a_1 <_{\mathfrak{f}} b_1$ has been settled above. Assume $a_1 = b_1$ and $a_2 <_{\mathfrak{f}} b_2$. By applying s everywhere in the preceeding proof, we obtain similarly

$$s(\Pi(\langle a_2, a_3, \ldots\rangle)) <' s(\Pi(\langle b_2, b_3, \ldots\rangle)),$$

which implies

$$a_1 s(\Pi(\langle a_2, a_3, \ldots\rangle)) <' a_1 s(\Pi(\langle b_2, b_3, \ldots\rangle)),$$

i.e.

$$\Pi(\langle a_1, a_2, \ldots\rangle) <' \Pi(\langle b_1, b_2, \ldots\rangle).$$

This argument can clearly be iterated. Finally, because $<_{\mathfrak{f}}^*$ is a linear ordering, we obtain the equivalence of $\vec{\boldsymbol{a}} <_{\mathfrak{f}}^* \vec{\boldsymbol{b}}$ and $\Pi(\vec{\boldsymbol{a}}) <' \Pi(\vec{\boldsymbol{b}})$ for every $\vec{\boldsymbol{a}}$, $\vec{\boldsymbol{b}}$ in $\mathfrak{f}^{(\mathbb{N})}$.

Now assume that $\vec{\boldsymbol{c}}$ is any finite $\mathfrak{f}$-labelling which is admissible for both α and β. By applying the formula of Lemma 5.ii and the equivalence above we have

$$\begin{aligned}(\vec{\boldsymbol{c}})^\alpha <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^\beta &\Longleftrightarrow \Pi((\vec{\boldsymbol{c}})^\alpha) <' \Pi((\vec{\boldsymbol{c}})^\beta)\\ &\Longleftrightarrow \Pi(\vec{\boldsymbol{c}}).\sigma(\alpha) <' \Pi(\vec{\boldsymbol{c}}).\sigma(\beta) \Longleftrightarrow \sigma(\alpha) <' \sigma(\beta).\end{aligned}$$

It follows that $<'$ and $<$ coincide since we have seen that $\sigma(\alpha) < \sigma(\beta)$ implies the existence of at least one $\mathfrak{f}$-labelling $\vec{\boldsymbol{c}}$ satisfying $(\vec{\boldsymbol{c}})^\alpha <_{\mathfrak{f}}^* (\vec{\boldsymbol{c}})^\beta$. This completes the proof of Theorem 9. ■

As for Proposition 2, the detour through distributive structures and the extended group $\widetilde{B}_\infty$ is the only way presently known for proving the existence of the ordering $<$ on B_∞. In particular, the irreflexivity of $<$ on B_∞ is another form of the irreflexivity property for $\sqsubset_{LD}$.

Denoting by ω, ω^* and η the order types of the natural numbers, of the negative integers and of the rationals, one easily shows that the order type of $<_{\mathfrak{f}}$ is $\omega(1+\eta)$, so that the order type of B_∞^+ equipped with $<$ is $(\omega(1+\eta))^{\omega^*}$. The order type of B_∞ equipped with $<$ is η. We hope that new comparison algorithms for $\sqsubset_{LD}$ will soon improve the rough complexity bound established for braid words comparison.

As a final remark, observe that the LD-magma B_∞ is certainly left cancellative, so that we can use braids themselves to label braids. The extension of 6.i and 9.iii (replacing $<_{\mathfrak{f}}$ by $<$) to finite B_∞-labellings is immediate since the formula of 5.ii holds for B_∞-labellings as well as for $\mathfrak{f}$-labellings.

References.

[1] J. Birman, *Braids, links, and mapping class groups*, Annals of Math. Studies **82** Princeton Univ. Press (1975).

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

[3] P. Cartier, *Développements récents sur les groupes de tresses, applications à la topologie et à l'algèbre*, Séminaire Bourbaki, exposé 716 (1989).

[4] P. Dehornoy, *Free distributive groupoids*, Journal of Pure and Applied Algebra, **61** (1989) 123–146.

[5] —, *Sur la structure des gerbes libres*, Comptes-rendus de l'Acad. des Sciences de Paris, **309-I** (1989) 143–148.

[6] —, *Algebraic properties of the shift mapping*, Proc. AMS, **106-3** (1989) 617–623.

[7] —, *The Adjoint Representation of Left Distributive Structures*, Comm. in Algebra, *to appear*.

[8] —, *Problème de mots dans les gerbes libres*, Theor. Comp. Sc., *to appear*.

[9] R. Dougherty, *Critical points of elementary embeddings*, preprint (1989).

[10] E. A. Elrifai & H. R. Morton, *Algorithms for positive braids*, preprint (1990).

[11] R. Fenn & C. Rourke, *Preliminary announcement of results: racks, links and 3-manifolds*, preprint (1990).

[12] F. A. Garside, *The Braid Group and other Groups*, Quart. J. Math. Oxford **20** No 78 (1969) 235–254.

[13] G. Huet & D. Oppen, *Equations and Rewrite Rules: a survey*, .in R. Book, ed., Formal Languages: Perspectives and Open Problems, Academic Press (1980).

[14] A. Jacquemard, *About the effective classification of conjugacy classes of braids*, Journal of Pure and Applied Algebra, **63** (1990) 161–169.

[15] D. Knuth & P. Bendix, *Simple word problems in universal algebras*, in J. Leech, ed., Computational Problems in Abstract Algebra, Pergamon Press (1970) 263–297.
[16] P. Kepka, *Notes on left distributive groupoids*, Acta universitatis Carolinae, Mathematica et physica, **22-2** (1981) 23–37.
[17] A. Kanamori, W. Reinhardt, R. Solovay, *Strong axioms of infinity and elementary embeddings*, Ann. Math. Logic, **13** (1978) 73–116.
[18] D. Joyce, *A classifying invariant of knots: the knot quandle*, Journal of Pure and Applied Algebra, **23** (1982) 37–65.
[19] R. Laver, *Elementary embeddings of a rank into itself*, AMS Abstracts, **7** (1986) 6.
[20] —, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Mathematics, **91-2** (1992) 209–231.
[21] —, *A division algorithm for the free left distributive algebra*, Proc. Helsinki 1990 ASL Meeting *to appear*.
[22] S. Mac Lane, *Natural associativity and commutativity*, Rice Univ. Studies, **49** (1963), 28–46.
[23] W. Thurston, *Finite state algorithms for the braid group*, Preprint (1988).
[24] F. Wehrung, *Gerbes primitives*, C. R. Acad. Sci. Paris **313-I** (1991) 357–362.

Mathématiques, Université, 14 032 Caen, France
dehornoy@geocub.greco-prog.fr