Journal of Algebra and Its Applications

FREE AUGMENTED LD-SYSTEMS

Patrick DEHORNOY
Laboratoire de Mathématiques Nicolas Oresme UMR 6139
Université de Caen, 14032 Caen, France
dehornoy@math.unicaen.fr
URL: //www.math.unicaen.fr/∼dehornoy

Received (Day Month Year)
Revised (Day Month Year)
Accepted (Day Month Year)

Communicated by (xxxxxxxxx)

Define an augmented LD-system, or ALD-system, to be a set equipped with two binary operations, one satisfying the left self-distributivity law $x * (y * z) = (x * y) * (x * z)$ and the other satisfying the mixed laws $(x \circ y) * z = x * (y * z)$ and $x * (y \circ z) = (x * y) \circ (x * z)$. We solve the word problem of the ALD laws, and prove that every element in the parenthesized braid group $B_\bullet$ of [2,3,5,6] generates a free ALD-system of rank 1, *i.e.*, that $B_\bullet$ is a torsion-free ALD-system.

1. Introduction

Define an *LD-system* to be an algebraic system made of a set S equipped with a binary operation $*$ that satisfies the left self-distributivity law

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

Classical examples include groups equipped with their conjugacy operation $x * y = xyx^{-1}$, and lattices with their inf or sup operation. Less classical examples have appeared in Set Theory with the iterations of elementary embeddings [12], and in Low Dimensional Topology where (*LD*) provides an algebraic translation of Reidemeister move III [10,13,9]. A rich theory has been developed for LD-systems [4]. In particular, it is known that there exists on Artin's braid group B_∞ an LD-operation $*$ such that the $*$-closure of any braid is a free LD-system of rank 1—which provides a concrete realization of the latter structure.

Many examples of LD-systems turn out to be equipped with a second operation connected in various ways with the self-distributive operation. In the typical case of group conjugacy, using $\circ$ for the group product, the following mixed identities are satisfied

$$x * (y * z) = (x \circ y) * z, \tag{ALD_1}$$

$$x * (y \circ z) = (x * y) \circ (x * z). \tag{ALD_2}$$

When we add the identity $x \circ y = (x * y) \circ x$, the associativity of $\circ$ and the existence of a unit, one obtains the structure of an LD-monoid, which is investigated in Chapter XI of [4] (and in [7,8] under the name of LD-algebra).

It is easy to verify that all LD-systems cannot be enriched into LD-monoids. In particular, this is the case for the above mentioned LD-structure on B_∞, for which there can exist no second operation verifying (ALD_1). In [6], building on earlier approaches of [2,3,5], a new group $B_\bullet$ extending both Artin's braid group B_∞ and R.Thompson's group F is investigated. This group is called the parenthesized braid group, as its elements can be naturally interpreted using braid diagrams in which the strands come grouped into blocks that can be encoded in parenthesized words. It is shown that the LD-structure of B_∞ extends to $B_\bullet$ and that the latter can be completed with a second operation that satisfies the above identities (ALD_1) and (ALD_2)—but none of the further laws defining an LD-monoid. Such a structure is called an *augmented* LD-system, or *ALD-system.*

The aim of this note is to prove two new results about ALD-systems. The first one is that there exists an effective algorithm to recognize whether two abstracts are equal modulo (LD), (ALD_1) and (ALD_2), *i.e.*,

Proposition 1.1. *The word problem of the ALD laws is decidable.*

The second result is a counterpart for the ALD-structure of parenthesied braids of a result established in [4] for the LD-structure of ordinary braids, namely that every element of $B_\bullet$ generates a free ALD-subsystem of $B_\bullet$. In G is a group, the property that every element of G generates a free subgroup is known as G being a torsion-free group. Extending the notion to ALD-systems, we can assert the previous result as

Proposition 1.2. *When equipped with the operations of [6], parenthesized braids form a torsion-free ALD-system.*

Being quite similar to results holding for LD and B_∞, the above results are not surprising. However, their proofs require a few new specific arguments that are the subject of this paper.

2. Free augmented LD-systems

The aim of this section is to solve the word problem for the ALD laws, *i.e.*, to describe an algorithm that enables one to decide whether two terms are or not equivalent up to ALD.

2.1. *ALD-systems*

The algebraic systems considered here are as follows:

Definition 2.1. An *ALD-system* is defined to be a set S equipped with two binary operations, $*$ and $\circ$ that satisfy the identities (LD), (ALD_1), and (ALD_2).

Example 2.1. We already observed that any group G equipped with the conjugation operation $*$ and the product is an ALD-system—and even an LD-monoid. Another easy example is obtained by starting with an arbitrary binary system $(S, \circ)$ and considering an $\circ$-endomorphism f. Then defining $x * y = f(y)$ turns $(S, *, \circ)$ into an ALD-system.

If L_x denotes the left $*$-translation $y \mapsto x * y$, then (LD) and (ALD_2) express that, for each x in the considered domain, L_x is an endomorphism with respect to $*$ and $\circ$, respectively, while (ALD_1) expresses that $\circ$ corresponds to a composition of translations: $L_{x\circ y} = L_x \circ L_y$. Thus, an ALD-system is an LD-system where the family of left translations is closed under composition—and in which (ALD_2) is satisfied. It may be noted that, in any case, the conjunction of (LD) and (ALD_1) implies some weak form of (ALD_2), as we can write

$$\begin{aligned}(x * (y \circ z)) * (x * u) &=_{LD} x * ((y \circ z) * u) =_{ALD_1} x * (y * (z * u))\\ &=_{LD} (x * y) * ((x * z) * (x * u))) =_{ALD_1} ((x * y) \circ (x * z)) * (x * u),\end{aligned}$$

which follows from (ALD_2) and actually implies it if we may cancel $x * u$ on the right.

2.2. *Terms and free ALD-systems*

We consider in the sequel free ALD-systems. As usual, the latter can be introduced as quotients of absolutely free algebras, *i.e.*, of algebras consisting of terms subject to no relation. Our notation will be as follows.

Definition 2.2. For $n \geqslant 1$, we denote by T^*_n (*resp.* T°_n, *resp.* $T^{*,\circ}_n$) the set of all terms constructed using the binary operator $*$ (*resp.* $\circ$, *resp.* $*$ and $\circ$) from n fixed variables $x_1, \ldots, x_n$. We write T^* for the union of all T^*_n, and similarly with T° and $T^{*,\circ}$—and x for x_1.

The *size* of a term t is defined to be the number of occurrences of variables in t, *i.e.*, it is defined to be 1 when t is a variable, and to be the sum of the sizes of the left and the right subterms of t otherwise. By construction, $T^{*,\circ}_n$ is an absolutely free algebra of rank n. The following is clear:

Lemma 2.1. *Let* $=_{ALD}$ *be the congruence on* $T^{*,\circ}_n$ *generated by all instances of the laws* (LD), (ALD_1), *and* (ALD_2)[a]. *Then, for each* n, *the system* $T^{*,\circ}_n/{=_{ALD}}$ *is a free ALD-system of rank* n.

We say that two terms t, t' are *ALD-equivalent* if $t =_{ALD} t'$ holds. Of course, there is a similar result for the free LD-system of rank n obtained as $T^*_n/{=_{LD}}$, where $=_{LD}$ is the congruence generated by the instances of the sole law (LD).

[a] *i.e.*, all pairs of terms of the form $(t_1 * (t_2 * t_3), (t_1 * t_2) * (t_1 * t_3))$, $(t_1 * (t_2 * t_3), (t_1 \circ t_2) * t_3)$, and $(t_1 * (t_2 \circ t_3), (t_1 * t_2) \circ (t_1 * t_3))$

It is helpful for intuition to associate with every term a finite binary rooted, labeled tree: the tree associated with a variable x consists of a single node labeled x; for $\square = *$ or $\circ$, the tree associated with $t_1 \square t_2$ consists of a root labeled $\square$ admitting as its left subtree the tree associated with t_1, and as its right subtree the tree associated with t_2.

As a preliminary remark, let us observe that the variety of ALD-systems is properly intermediate between LD-systems and LD-monoids.

Proposition 2.1. (*i*) *A free LD-system cannot be enriched into an ALD-system.*

(*ii*) *A free ALD-system does not obey the law $x \circ y = (x * y) \circ x$, and therefore is not an LD-monoid.*

Proof. (*i*) For t a term, let $\mathrm{ht}_R(t)$ be the length of the rightmost branch in the associated tree, *i.e.*, define $\mathrm{ht}_R(t)$ by $\mathrm{ht}_R(x) = 0$ and $\mathrm{ht}_R(t_1 \square t_2) = \mathrm{ht}_R(t_2) + 1$ for $\square = *$ or $\circ$. Then the law (*LD*) preserves ht_R, and, therefore, ht_R induces a well defined parameter on each free LD-system. On the other hand, (ALD_1) changes ht_R, so there may exist no operation $\circ$ satisfying (ALD_1) on a free LD-system.

(*ii*) The terms $x_1 \circ x_2$ and $(x_1 * x_2) \circ x_1$ are not ALD-equivalent, as none of the identities (*LD*), (ALD_1), (ALD_2) may apply to a term with only two occurrences of variables. $\square$

2.3. *Two ALD-invariants*

In order to subsequently solve the word problem of ALD, we shall associate with every term in $T^{*,\circ}$ two ALD-invariants, *i.e.*, two objects that depend only on the ALD-class of the term. The first invariant is a term in T_1°; the second one is a finite sequence of LD-classes of terms in T^*. To introduce the latter, we first fix some notation for sequences.

Definition 2.3. Assume that $(S, *)$ is a binary system. The set of all finite, nonempty sequences of elements of S is denoted by $\widehat{S}$. An element of $\widehat{S}$ is typically denoted $\vec{s}$; its length is then denoted $\ell(\vec{s})$, and its successive elements $s_1, \dots, s_{\ell(\vec{s})}$. The concatenation of two sequences $\vec{s}$, $\vec{t}$, *i.e.*, the sequence of length $\ell(\vec{s}) + \ell(\vec{t})$ obtained by writing $\vec{t}$ after $\vec{s}$, is denoted $\vec{s}^\frown\vec{t}$. Next, we denote by $\vec{*}$ the binary operation on $\widehat{S}$ defined by

$$\vec{s} \,\vec{*}\, \vec{t} = (s_1 * \dots * s_{\ell(\vec{s})} * t_1, \dots, s_1 * \dots * s_{\ell(\vec{s})} * t_{\ell(\vec{t})}), \tag{2.1}$$

where missing parentheses are to be added on the right: $x * y * z$ stands for $x * (y * z)$.

Lemma 2.2. *Assume that $(S, *)$ is an LD-system. Then $(\widehat{S}, \vec{*}, ^\frown)$ is an ALD-system.*

Proof. The only point that is not absolutely obvious is that (*LD*) holds. Now, for all s, t, u in $\widehat{S}$, the kth entry in $\vec{s} \,\vec{*}\, (\vec{t} \,\vec{*}\, \vec{u})$ is $s_1 * \dots * s_p * t_1 * \dots * t_q * u_k$, while that of $(\vec{s} \vec{*} \vec{t}) \vec{*} (\vec{s} \vec{*} \vec{u})$ is

$$(s_1 * ... * s_p * t_1) * ... * (s_1 * ... * s_p * t_q) * s_1 * ... * ... * u_k.$$

Repeated applications of the LD law show that the expressions are equal. □

We can now introduce the two mappings that give rise to ALD-invariants.

Definition 2.4. For each term t in $T^{*,\circ}$, we define a term $I(t)$ in T_1° and a finite sequence of terms $J(t)$ in $\widehat{T^*}$ using the inductive clauses

$$(I(t), J(t)) = \begin{cases} (x, t) & \text{if } t \text{ is a variable,} \\ (I(t_2), J(t_1) \vec{*} J(t_2)) & \text{for } t = t_1 * t_2, \\ (I(t_1) \circ I(t_2), J(t_1)^\frown J(t_2)) & \text{for } t = t_1 \circ t_2, \end{cases} \tag{2.2}$$

For instance, for $t = x_1 * ((x_2 * x_3) \circ x_4)$, the reader can check the values $I(t) = x \circ x$, $J(t) = (x_1 * (x_2 * x_3), x_1 * x_4)$.

A straightforward induction gives

Lemma 2.3. *For each term t in $T^{*,\circ}$, the size of the term $I(t)$ equals the length of the sequence $J(t)$.*

Lemma 2.4. *Assume that t, t' are ALD-equivalent terms in $T^{*,\circ}$. Then we have*

$$I(t) = I(t') \quad \textit{and} \quad J(t) =_{LD} J(t'), \tag{2.3}$$

the latter meaning that the sequences $J(t)$ and $J(t')$ have equal lengths and pairwise LD-equivalent entries.

Proof. As ALD-equivalence is the congruence on $T^{*,\circ}$ generated by the pairs of terms occurring in the laws (*LD*), (*ALD*$_1$), and (*ALD*$_2$), it is sufficient to check that the relations $I(t) = I(t')$ and $J(t) =_{LD} J(t')$ are congruences on $T^{*,\circ}$, and that they include all instances of (*LD*), (*ALD*$_1$), and (*ALD*$_2$).

The fact that $I(t_1 * t_2)$ and $I(t_1 \circ t_2)$ are defined from $I(t_1)$ and $I(t_2)$ makes it clear that $I(t) = I(t')$ is a congruence, *i.e.*, that it is compatible with $*$ and $\circ$. The same argument works for $J(t) =_{LD} J(t')$, as the relation $=_{LD}$ on $\widehat{T^*}$ is itself a congruence.

Let (t, t') be an instance of (*LD*), *i.e.*, assume that t and t' are of the form $t = t_1 * (t_2 * t_3)$ and $t' = (t_1 * t_2) * (t_1 * t_3)$. The definitions yields

$$I(t) = I(t_3) = I(t'),$$
$$J(t) = J(t_1) \vec{*} (J(t_2) \vec{*} J(t_3)), \quad J(t') = (J(t_1) \vec{*} J(t_2)) \vec{*} (J(t_1) \vec{*} J(t_3)),$$

and the latter are $=_{LD}$-equivalent by lemma 2.2. Similarly, for (t, t') an instance of (*ALD*$_1$), *i.e.*, for $t = t_1 * (t_2 * t_3)$ and $t' = (t_1 \circ t_2) * t_3$, we have

$$I(t) = I(t_3) = I(t') \quad \text{and} \quad J(t) = J(t_1) \vec{*} J(t_2) \vec{*} J(t_3) = J(t').$$

Finally, for (t, t') an instance of (ALD_2), *i.e.*, for $t = t_1 * (t_2 \circ t_3)$ and $t' = (t_1 * t_2) \circ (t_1 * t_3)$, we find

$$I(t) = I(t_2) \circ I(t_3) = I(t') \quad \text{and} \quad J(t) = (J(t_1) \vec{*} J(t_2))^\frown(J(t_1) \vec{*} J(t_3)) = J(t'),$$

which completes the proof. □

Remark 2.1. The result that I is an ALD-invariant can also be deduced from applying the construction of Example 2.1 to the free algebra $(T_1^\circ, *)$—as well as the result that J mod. (LD) is an ALD-invariant follows from the construction of lemma 2.2.

2.4. *Special terms*

We shall now see that, for each term t in $T^{*,\circ}$, the pair $(I(t), J(t))$ determines the ALD-class of t.

Definition 2.5. For v is a term of size p in T_1°, and $\vec{t}$ is a length p sequence of terms in T^*, we denote by $v[\vec{t}\,]$ the term obtained from v by substituting $t_1, \dots, t_p$ to the variables of t enumerated from left to right. A term is called *special* if it is of the form $v[\vec{t}\,]$ with v, $\vec{t}$ as above.

Saying that a term t is special means that, in the tree associated with t, no $\circ$ symbol lies below an $*$ symbol (according to the convention that the root lies on the top). The following result shows non only that every term in $T^{*,\circ}$ is ALD-equivalent to a special term, but also that the pair $(I(t), J(t))$ determines the ALD-class of t.

Lemma 2.5. *For every term t in $T^{*,\circ}$ we have*

$$t =_{ALD} I(t)[J(t)]. \tag{2.4}$$

Proof. If t is a variable, (2.4) is an equality. For an induction, it is sufficient to show that the following relations hold for all terms u, v in T_1° and all sequences $\vec{s}$, $\vec{t}$ in $\widehat{T^*}$

$$u[\vec{s}\,] * v[\vec{t}\,] =_{ALD} v[\vec{s} \vec{*} \vec{t}\,], \tag{2.5}$$

$$u[\vec{s}\,] \circ v[\vec{t}\,] = (u \circ v)[\vec{s}^\frown \vec{t}\,]. \tag{2.6}$$

We establish (2.5) using induction on the sum of the sizes, say p and q, of u and v, which also are the lengths of $\vec{s}$ and $\vec{t}$, respectively. We recall that missing parentheses are to be added on the right, *i.e.*, $x * y * z$ stands for $(x * y) * (x * z)$.

For $p = q = 1$, the terms u and v are variables, so we have $u[\vec{s}\,] = s_1$ and $v[\vec{t}\,] = t_1$, and (2.5) reduces to the equality $s_1 * t_1 = v[s_1 * t_1]$. Assume now $p + q > 2$. Then we have $p \geqslant 2$ or $q \geqslant 2$. Assume first $q \geqslant 2$. Write $v = v_1 \circ v_2$, and let r be the size of v_1. We find

$$\begin{aligned}
u[\vec{s}\,] * v[\vec{t}\,] &= u[\vec{s}\,] * (v_1[t_1, \dots, t_r] \circ v_2[t_{r+1}, \dots, t_q]) && \text{(by definition)}\\
&=_{\!ALD} (u[\vec{s}\,] * v_1[t_1, \dots, t_r]) \circ (u[\vec{s}\,] * v_2[t_{r+1}, \dots, t_q])) && (ALD_2)\\
&=_{\!ALD} v_1[\vec{s} \,\vec{*}\, t_1, \dots, \vec{s} \,\vec{*}\, t_r] \circ v_2[\vec{s} \,\vec{*}\, t_{r+1}, \dots, \vec{s} \,\vec{*}\, t_q] && \text{(by ind. hyp.)}\\
&= (v_1 \circ v_2))[\vec{s} \,\vec{*}\, \vec{t}\,] && \text{(by definition).}
\end{aligned}$$

Assume now $p \geqslant 2$. Writing similarly $u = u_1 \circ u_2$, and letting r be now the size of u_1, we find

$$\begin{aligned}
u[\vec{s}\,] * v[\vec{t}\,] &= (u_1[s_1, \dots, s_r] \circ u_2[s_{r+1}, \dots, s_p]) * v[\vec{t}\,] && \text{(by definition)}\\
&=_{\!ALD} u_1[s_1, \dots, s_r] * (u_2[s_{r+1}, \dots, s_p] * v[\vec{t}\,]) && (ALD_1)\\
&=_{\!ALD} u_1[s_1, \dots, s_r] * v[s_{r+1} * \dots * s_p \,\vec{*}\, \vec{t}\,] && \text{(by ind. hyp.)}\\
&=_{\!ALD} v[s_1 * \dots * s_p * s_{r+1} * \dots * s_p \,\vec{*}\, \vec{t}\,] = v[\vec{s} \,\vec{*}\, \vec{t}\,] && \text{(by ind. hyp.).}
\end{aligned}$$

As for (2.6), it follows from the definition directly. □

2.5. *The word problem of ALD*

It is now easy to solve the word problem for *ALD*, namely to prove the following precise version of Proposition 1.1.

Proposition 2.2. *The word problem of ALD is decidable: if t, t' are terms in $T^{*,\circ}$, then $t =_{ALD} t'$ holds if and only if the terms $I(t)$ and $I(t')$ are equal, and the sequences $J(t)$ and $J(t')$ have the same length and consist of pairwise LD-equivalent terms of T^*.*

Proof. The condition is necessary by lemma 2.4. It is sufficient by lemma 2.5. Indeed, if $\vec{s}$, $\vec{t}$ are length p sequences of pairwise LD-equivalent terms in T^* and if v is any size p term in T_1°, the terms $v[\vec{s}\,]$ and $v[\vec{t}\,]$ are ALD-equivalent. So, if t, t' are terms in $T^{*,\circ}$ satisfying $I(t) = I(t')$ and $J(t) =_{LD} J(t')$, we obtain

$$t =_{ALD} I(t)[J(t)] =_{ALD} I(t')[J(t')] =_{ALD} t',$$

hence $t =_{ALD} t'$. As the relation $=_{LD}$ is known to be decidable [4], so is $=_{ALD}$. □

As for the complexity of the previous solution, the known upper bounds for the word problem of (*LD*) are a single exponential in the case of terms with one variable, and a double exponential in the general case [4]. As the size of the sequence $J(t)$ may be exponential in the length of t since each application of (ALD_2) may double the length, the solution described in Proposition 2.2 has a (certainly not optimal) upper bound which is doubly exponential in the case of one variable, and triply exponential in the general case—the results of Section 3 below will give a better, simply exponential algorithm in the case of one variable.

3. Parenthesized braids

The group of parenthesized braids $B_\bullet$ was introduced in [2,3,5]—in a different framework—and further investigated in [6]. It is shown in the latter paper that $B_\bullet$ can be equipped with two binary operations that make it an ALD-system. The aim of this section is to study this specific ALD-system, and in particular to show that it contains many copies of the free ALD-system on one generator.

3.1. *The group $B_\bullet$*

The simplest way to introduce $B_\bullet$ is to start from a presentation:

Definition 3.1. We denote by $B_\bullet$ the group generated by two infinite sequences $\sigma_1, \sigma_2, ..., a_1, a_2, ...$ subject to the relations

$$\begin{cases} \sigma_j\sigma_i = \sigma_i\sigma_j, \quad a_j\sigma_i = \sigma_i a_j & \text{for } j \geqslant i+2, \\ a_j\sigma_i = \sigma_{i+1}a_j, \quad a_j a_i = a_{i+1}a_j & \text{for } j \leqslant i-1, \\ \sigma_j\sigma_i\sigma_j = \sigma_i\sigma_j\sigma_i, \quad \sigma_i\sigma_j a_i = a_j\sigma_i, \quad \sigma_j\sigma_i a_j = a_i\sigma_i, & \text{for } j = i+1. \end{cases} \tag{3.1}$$

It is shown in [3] that $B_\bullet$ is actually generated by σ_1, σ_2, a_1, and a_2, and that it admits a finite—but much less readable—presentation with respect to those generators. It is shown in [6] that the elements of $B_\bullet$ admit a natural geometric interpretation in terms of parenthesized braid diagrams, which are similar to ordinary braid diagrams—*cf.* for instance [1,4,14]—but with non-uniform distances between the strands. As we shall not use this interpretation here—nor do wo either use the interpretation in terms of isotopy classes of homeomorphisms of a sphere with a Cantor set of punctures—we shall not go into details here and just refer to Figure 1 for a rough intuition.

Fig. 1. Diagram representation of the generators of $B_\bullet$: there are infinitely strands numbered by positive integer coefficients polynomials in an infinitely small variable ϵ; the effect of σ_i is to let all strands with index $i+1+o(1)$ cross over all strands with index $i+o(1)$; the effect of a_i is to shrink all strands of the form $i+o(1)$ by a factor ϵ and to left translate all strands with index $\geqslant i+1$ so as to avoid gaps.

Definition 3.2. We denote by ∂ the endomorphism of the group $B_\bullet$ that maps σ_i to σ_{i+1} and a_i to a_{i+1} for each i.

It is shown in [6] that ∂ is injective—but not surjective: neither σ_1 nor a_1 belong to Im∂.

Proposition 3.1 ([6]). *(Figure 2) Let $*$, $\circ$ be the binary operations on $B_\bullet$ defined by*

$$g * h := g \cdot \partial h \cdot \sigma_1 \cdot \partial g^{-1}, \qquad g \circ h := g \cdot \partial h \cdot a_1. \tag{3.2}$$

Then $(B_\bullet, *, \circ)$ is an ALD-system.

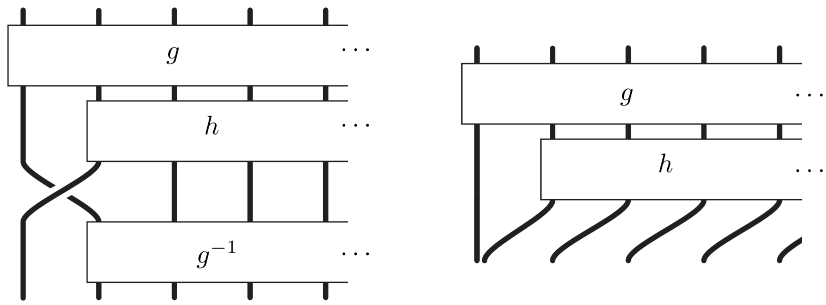

Fig. 2. Diagram representation of the ALD operations on $B_\bullet$: the diagram of $g * h$ (left) and $g \circ h$ (right) from those of g and h

3.2. *A freeness criterion*

Our aim is to show that every monogenerated subsystem of the ALD-system $(B_\bullet, *, \circ)$ is free. To prove the result, we need a criterion for recognizing free ALD-systems of rank 1.

Assume that $(S, *, \circ)$ is a double binary system generated by a single element g. Then, there exists a surjective homomorphism π of $T_1^{*,\circ}$ onto S that maps x to g: by definition, the value $\pi(t)$ is the *evaluation* of t at g, and it will be denoted by $t(g)$—exactly as the evaluation of a polynomial P at g would be denoted by $P(g)$. Then, saying that $(S, *, \circ)$ is an ALD-system means that $t =_{ALD} t'$ implies $t(g) = t'(g)$, and saying that $(S, *, \circ)$ is a free ALD-system based on $\{g\}$ means that $t =_{ALD} t'$ is equivalent to $t(g) = t'(g)$. In other words, in order to prove that some ALD-system S generated by an element g is free, the point is to prove that $t(g) \neq t'(g)$ holds for all pairs of terms (t, t') satisfying $t \neq_{ALD} t'$. The criterion we shall establish new allows one to restrict to pairs of terms (t, t') of a restricted type.

Definition 3.3. For u, v in T_1°, we say that $u < v$ holds if we have either (i) $u = x$ and $v \neq x$, or (ii) $u = u_1 \circ u_2$ and $v = v_1 \circ v_2$ with $u_1 < v_1$, or (iii) $u = u_1 \circ u_2$ and $v = v_1 \circ v_2$ with $u_1 = v_1$ and $u_2 < v_2$.

Clearly, the relation $<$ is a strict linear order on T_1°.

Definition 3.4. (i) For s, t in T^*, we say that $s \sqsubset t$ holds if there exist $p \geqslant 1$ and terms $t_1, \ldots, t_p$ in T^* satisfying

$$t = (...((s * t_1) * t_2)...) * t_p.$$

(ii) For $\vec{s}\,, \vec{t}$ in $\widehat{T^*}$, we say that $\vec{s} \mathrel{\vec{\sqsubset}} \vec{t}$ holds if the lengths of $\vec{s}$ and $\vec{t}$ are equal and there exists $k \leqslant \ell(\vec{s}\,)$ satisfying $s_i = t_i$ for $i < k$ and $s_k \sqsubset t_k$.

Proposition 3.2. *Assume that S is an ALD-system generated by an element g. Then a necessary and sufficient condition for S to be free based on $\{g\}$ is that S satisfies no equality of the form*

$$u[\vec{s}\,](g) = v[\vec{t}\,](g) \tag{3.3}$$

with u, v in T_1° and $\vec{s}\,, \vec{t}$ in $\widehat{T_1^*}$ satisfying either $u < v$, or $u = v$ and $\vec{s} \mathrel{\vec{\sqsubset}} \vec{t}$.

Proof. Assume that s, t are *ALD*-inequivalent terms in $T_1^{*,\circ}$. As was said above, the problem is to show that the evaluations $s(g)$ and $t(g)$ of s and t in S cannot be equal. By lemma 2.5, there exist u, v in T_1° and $\vec{s}, \vec{t}$ in $\widehat{T^*}$ satisfying $s =_{ALD} u[\vec{s}\,]$ and $t =_{ALD} v[\vec{t}\,]$. As S is an ALD-system, we have $s(g) = u[\vec{s}\,](g)$ and $t(g) = v[\vec{t}\,](g)$, so it is sufficient to prove $u[\vec{s}\,](g) \neq v[\vec{t}\,](g)$. Now, by lemma 2.1, the hypothesis $u[\vec{s}\,] \neq_{ALD} v[\vec{t}\,]$ implies $u \neq v$, or $u = v$ and $\vec{s} \neq_{LD} \vec{t}$. In the first case, we must have either $u < v$ or $v < u$ as $<$ is a linear ordering, hence, if no equality (3.3) holds, we deduce $s(g) \neq t(g)$. In the second case, as the sequences $\vec{s}$ and $\vec{t}$ have the same length, there exists an index $k \leqslant p$ such that we have $s_i =_{LD} t_i$ for $i < k$ and $s_k \neq_{LD} t_k$. By the results of [4], the latter relation implies the existence of terms s'_k, t'_k satisfying $s'_k =_{LD} s_k$, $t'_k =_{LD} t_k$ and either $s'_k \sqsubset t'_k$ or $t'_k \sqsubset s'_k$. Let $\vec{s}\,'$ denote the sequence obtained from $\vec{s}$ by replacing s_k by s'_k, and let $\vec{t}\,'$ denote the sequence obtained from $\vec{t}$ by replacing t_i with s_i for $i < k$, and by replacing t_k with t'_k. Then, as S is an ALD-system, we have $u[\vec{s}\,](g) = u[\vec{s}\,'](g)$ and $u[\vec{t}\,](g) = u[\vec{t}\,'](g)$, and, by construction, we have $\vec{s}\,' \mathrel{\vec{\sqsubset}} \vec{t}\,'$ or $\vec{t}\,' \mathrel{\vec{\sqsubset}} \vec{s}\,'$. If no equality (3.3) holds, we deduce $u[\vec{s}\,'](g) \neq u[\vec{t}\,'](g)$, hence $s(g) \neq t(g)$. □

3.3. *Term evaluation*

In order to apply the criterion of Proposition 3.2 in the ALD-system $(B_\bullet, *, \circ)$, we need to be able to evaluate in $B_\bullet$ expressions of the form $v[\vec{t}\,](g)$ with v a term in T_1° and $\vec{t}$ a sequence of terms in T_1^*. To this end, we shall use the following explicit formulas.

Lemma 3.1. *Assume that v is a term of size p in T_1°. Then, for each g in $B_\bullet$, we have*

$$v(1) \cdot \partial g = \partial^p g \cdot v(1), \tag{3.4}$$

where we recall $v(1)$ denotes the result of substituting x with 1 in v and evaluating the result in $B_\bullet$.

Proof. We use induction on v. For $v = x$, we have $p = 1$ and $v(1) = 1$, so (3.4) is true. Otherwise, assume $v = v_1 \circ v_2$. By definition, $v(1)$ is $v_1(1) \cdot \partial v_2(1) \cdot a_1$. Let p_i be the size of v_i. Using the induction hypothesis, we find

$$\begin{aligned} v(1) \cdot \partial g &= v_1(1) \cdot \partial v_2(1) \cdot a_1 \cdot \partial g && \text{(by definition)} \\ &= v_1(1) \cdot \partial v_2(1) \cdot \partial^2 g \cdot a_1 && \text{(by the relations of } B_\bullet) \\ &= v_1(1) \cdot \partial(v_2(1) \cdot \partial g) \cdot a_1 \\ &= v_1(1) \cdot \partial(\partial^{p_2} g \cdot v_2(1)) \cdot a_1 && \text{(by induction hypothesis)} \\ &= v_1(1) \cdot \partial(\partial^{p_2} g) \cdot \partial v_2(1) \cdot a_1 \\ &= \partial^{p_1}(\partial^{p_2} g) \cdot v_1(1) \cdot \partial v_2(1) \cdot a_1 && \text{(by induction hypothesis)} \end{aligned}$$

and the latter is $\partial^p g \cdot v(1)$. □

Lemma 3.2. *Assume $t = v[\vec{t}]$, with v a size p term in T_1° and $\vec{t}$ a length p sequence of terms in T_1^*. Then, for each g in $B_\bullet$, we have*

$$t(g) = t_1(g) \cdot \partial t_2(g) \cdot \ldots \cdot \partial^{p-1} t_p(g) \cdot v(1). \tag{3.5}$$

Proof. We use induction on v. For $v = x$, we have $p = 1$ and $t = t_1$, so the result is clear. Otherwise, assume $v = v_1 \circ v_2$. Let q be the size of v_1. Then we have

$$t = v_1[t_1, \ldots, t_q] \circ v_2[t_{q+1}, \ldots, t_p],$$

and, using the induction hypothesis twice, we deduce

$$\begin{aligned} t(g) &= v_1[t_1, \ldots, t_q](g) \cdot \partial v_2[t_{q+1}, \ldots, t_p](g) \cdot a_1 \\ &= t_1(g) \cdot \ldots \cdot \partial^{q-1} t_q(g) \cdot v_1(1) \cdot \partial v_2[t_{q+1}, \ldots, t_p](g) \cdot a_1 && \text{(ind. hyp.)} \\ &= t_1(g) \cdot \ldots \cdot \partial^{q-1} t_q(g) \cdot \partial^q v_2[t_{q+1}, \ldots, t_p](g) \cdot v_1(1) \cdot a_1 && (3.4) \\ &= t_1(g) \cdot \ldots \cdot \partial^{q-1} t_q(g) \cdot \partial^q t_{q+1}(g) \cdot \ldots \cdot \partial^{p-1} t_p(g) \cdot \partial^q v_2(1) \cdot v_1(1) \cdot a_1 && \text{(ind. hyp.)} \\ &= t_1(g) \cdot \ldots \cdot \partial^{q-1} t_q(g) \cdot \partial^q t_{q+1}(g) \cdot \ldots \cdot \partial^{p-1} t_p(g) \cdot v_1(1) \cdot \partial v_2(1) \cdot a_1, && (3.4) \end{aligned}$$

which gives (3.5) since we have $v(1) = v_1(1) \cdot \partial v_2(1) \cdot a_1$. □

3.4. *Monogenerated subsystems of $B_\bullet$*

With the previous criterion at hand, we can now establish that the ALD-system $(B_\bullet, *, \circ)$ is torsion-free, *i.e.*, that every element of $B_\bullet$ generates a free ALD-subsystem.

First, it is shown in [6] that the evaluation mapping $v \mapsto v(1)$ of T_1° into $B_\bullet$ is injective. We shall need the following strengthening of this result:

Lemma 3.3. *If u, v are distinct terms in T_1°, then, in $B_\bullet$, the quotient $u(1)^{-1} v(1)$ does not belong to* $\mathrm{Im}\partial$.

Proof. Let $x^{[N]}$ denote the term of T_1° inductively defined by $x^{[1]} = x$ and $x^{[N]} = x \circ x^{[N-1]}$ for $N \geqslant 2$. The subgroup of $B_\bullet$ generated by the elements a_i is isomorphic to Thompson's group F, and it gives rise to a partial action on T_1° corresponding to applying the associativity law [6]: the action of a_i on a term v is defined provided v can be expressed as $v_1 \circ ... \circ v_{i+2}$, *i.e.*, we have $\mathrm{ht}_R(v) \geqslant i+2$, and, in this case, one defines $v \cdot a_i = v_1 \circ ... \circ v_{i-1} \circ (v_i \circ v_{i+1}) \circ v_{i+2}$. Then, an easy induction shows that, for each term v of size p in T_1°, the element $v(1)$ of $B_\bullet$ maps any sufficiently large term $x^{[N]}$ to the term $v \circ x^{[N-p]}$. Hence $u(1)^{-1}v(1)$ maps $u \circ x^{[N-p]}$ to $v \circ x^{[N-q]}$, where p is the size of u. Now any element of $\mathrm{Im}\partial$ maps a term of the form $u \circ ...$ to another term of the form $u \circ ...$, since only a_1 may change the left subterm of the initial term. Hence $u(1)^{-1}v(1) \in \mathrm{Im}\partial$ is impossible for $v \neq u$. $\square$

We can now establish Proposition 1.2 as

Proposition 3.3. *For every parenthesized braid g, the closure of $\{g\}$ under $*$ and $\circ$ in $B_\bullet$ is free ALD-system.*

Proof. We apply the criterion of Proposition 3.2. Assume that u, v are terms in T_1° and $\vec{s}\,, \vec{t}$ are sequences of terms in T_1^*. Let $s = u[\vec{s}\,]$ and $t = v[\vec{t}\,]$. Our aim is to prove $s(g)^{-1}t(g) \neq 1$ both for $u < v$, and for $u = v$ with $\vec{s} \mathrel{\vec{\sqsubset}} \vec{t}$. Applying lemma 3.2, we find

$$s(g)^{-1}t(g) = u(1)^{-1} \cdot \partial^{p-1}s_p(g)^{-1} \cdot ... \cdot s_1(g)^{-1} \cdot t_1(g) \cdot ... \cdot \partial^{q-1}t_q(g) \cdot v(1). \quad (3.6)$$

We shall consider three cases, which cover the cases $u < v$, and $u = v$ with $\vec{s} \mathrel{\vec{\sqsubset}} \vec{t}$, and prove in each of them that the right hand side of (3.6) is not 1.

Assume first that there exists $k \leqslant \inf(p, q)$ such that $s_i =_{LD} t_i$ holds for $i < k$, and $s_k \neq_{LD} t_k$ holds. Then we have $s_i(g) = t_i(g)$ for $i < k$, and (3.6) becomes

$$s(g)^{-1}t(g) = u(1)^{-1} \cdot \partial^{p-1}s_p(g)^{-1} \cdot ... \cdot \partial^{k-1}(s_k(g)^{-1}t_k(g)) \cdot ... \cdot \partial^{q-1}t_q(g) \cdot v(1).$$

By the results of [4], the hypothesis $s_k \neq_{LD} t_k$ implies either $s_k \sqsubset_{LD} t_k$ or $t_k \sqsubset_{LD} s_k$, and the explicit definition of operation $*$ on $B_\bullet$ then implies that the braid $s_k(g)^{-1}t_k(g)$ admits an expression where the generator σ_1 appears but σ_1^{-1} does not, or σ_1^{-1} appears but σ_1 does not. It follows that $s(g)^{-1}t(g)$ admits an expression in which σ_k appears but neither σ_k^{-1} nor any $\sigma_i^{\pm 1}$ with $i < k$ does, or vice versa exchanging σ_k and σ_k^{-1}. By [6], Proposition 4.6, this guarantees $s(g) < t(g)$ in the canonical ordering of $B_\bullet$, hence $s(g) \neq t(g)$.

Assume now $p < q$ with $s_i =_{LD} t_i$ for $i \leqslant p$. In this case, (3.6) reduces to

$$s(g)^{-1}t(g) = u(1)^{-1} \cdot \partial^p(t_{p+1}(g) \cdot ... \cdot \partial^{q-p-1}t_q(g)) \cdot v(1).$$

By lemma 3.1, we have $u(1)^{-1} \cdot \partial^p z = \partial z \cdot u(1)^{-1}$ for each z in $B_\bullet$, so we get

$$s(g)^{-1} \cdot t(g) = \partial(t_{p+1}(g) \cdot ... \cdot \partial^{q-p-1}t_q(g)) \cdot u(1)^{-1}v(1).$$

This cannot be 1, as the first factor belongs to $\mathrm{Im}\partial$, while, according to lemma 3.3, $u(1)^{-1}v(1)$ does not unless $u = v$ holds.

Assume finally $p = q$ with $s_i =_{LD} t_i$ for $i \leqslant p$, and $u < v$. Then (3.6) reduces to

$$s(g)^{-1}t(g) = u(1)^{-1} \cdot v(1),$$

and, by lemma 3.1, the above expression cannot be 1. □

Remark 3.1. It is shown in [6] that the parenthesized braid group $B_\bullet$ can be equipped with a distinguished linear ordering that extends both the linear ordering of braids and the natural ordering on Thompson's group induced by the lexicographical ordering of finite trees. Let us define a relation $<_{ALD}$ on special terms in $T_1^{*,\circ}$ as follows: first say that $u[\vec{s}\,] < v[\vec{t}\,]$ holds if we have either $\vec{s} \sqsubset \vec{t}$, or $\vec{s}$ is a proper prefix of $\vec{t}$, or we have $\vec{s} = \vec{t}$ and $u < v$ holds; then say that $s <_{ALD} t$ holds if there exist special terms $u[\vec{s}\,]$, $v[\vec{t}\,]$ satisfying $u[\vec{s}\,] < v[\vec{t}\,]$, $s =_{ALD} u[\vec{s}\,]$, and $t =_{ALD} v[\vec{t}\,]$. Then the relation $<_{ALD}$ induces a linear ordering on the free ALD-system $T_1^{*,\circ}/{=_{ALD}}$, and what the proof of Proposition 3.3 actually shows is that, for each parenthesized braid g in $B_\bullet$, the evaluation mapping $t \mapsto t(g)$ is increasing.

The result that monogenerated sub-ALD-systems of $B_\bullet$ are free does not extend to sub-ALD-systems with more than one generator. For instance, the sub-ALD-system of $B_\bullet$ generated by σ_1 and σ_2 is not free, as we have $\sigma_1 * \sigma_1 = \sigma_2 * \sigma_2$ $(= \sigma_2\sigma_1)$, while, by Proposition 2.2, the terms $x{*}x$ and $y{*}y$ are not ALD-equivalent when x and y are distinct variables.

Question 3.1. *Does $(B_\bullet, *, \circ)$ include a free ALD-system of rank 2?*

It is not even known whether $(B_\bullet, *)$ or $(B_\infty, *)$ includes a free LD-system of rank 2; it might be tempting to conjecture that 1, a_1, a_1^2, ... generate a free sub-LD-system of $(B_\bullet, *)$, but we have no evidence to support this conjecture so far.

Question 3.2. *Does the ALD-system $(B_\bullet, *, \circ)$ admit a natural generating family?*

The similar question of finding a natural generating family for the LD-system $(B_\infty, *)$ is equally open.

3.5. *The converse direction*

According to Proposition 3.1, the operations of (3.2) define operations on $B_\bullet$ that make it an ALD-system. We conclude with the easy observation that, conversely, the operations defined on a group G by formulas of the type (3.2) give rise to an ALD-system only if G is closely connected to $B_\bullet$:

Proposition 3.4. *Assume that G is a group, ∂ is an endomorphism of G, and a, σ are fixed elements of G. Write σ_i for $\partial^{i-1}(\sigma)$ and a_i for $\partial^{i-1}(a)$. Then defining*

$$x * y = x \cdot \partial y \cdot \sigma \cdot \partial x^{-1}, \qquad x \circ y = x \cdot \partial y \cdot a \tag{3.7}$$

yields an ALD-system on the subgroup H generated by the σ_i's and the a_i's—i.e., on the smallest subgroup of G containing σ and a and closed under ∂—if and only if the elements σ_i and a_i obey the relations (3.1), i.e., if and only if H is a homomorphic image of $B_\bullet$.

Proof. Assume that $(G, *, \circ)$ is an ALD-system. The instance $1*(1*z) = (1*1)*(1*z)$ of (LD) expands into

$$\partial^2 z \cdot \sigma_2\sigma_1 = \sigma_1 \cdot \partial^2 z \cdot \sigma_2\sigma_1\sigma_2^{-1}. \tag{3.8}$$

For $z = 1$, we obtain the braid relation

$$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2, \tag{3.9}$$

and, then, (3.8) gives

$$\partial^2 z \cdot \sigma_1 = \sigma_1 \cdot \partial^2 z \tag{3.10}$$

for each z. Similarly, the instance $1*(1*z) = (1 \circ 1)*z$ of (ALD_1) expands into

$$\partial^2 z \cdot \sigma_2\sigma_1 = a_1 \cdot \partial z \cdot \sigma_1 a_2^{-1}. \tag{3.11}$$

For $z = 1$, we deduce

$$a_1\sigma_1 = \sigma_2\sigma_1 a_2, \tag{3.12}$$

and, then, (3.11) gives

$$\partial^2 z \cdot a_1 = a_1 \cdot \partial z \tag{3.13}$$

for each z. Finally, the instance $1*(1 \circ 1) = (1*1) \circ (1*1)$ of (ALD_2) expands into

$$a_2\sigma_1 = \sigma_1\sigma_2 a_1. \tag{3.14}$$

Conversely, it is easy to verify that the conjunction of (3.8), (3.11) (for each z), and (3.9), (3.12), and (3.14) guarantees that $(G, *, \circ)$ be an ALD-system. When we restrict to the subgroup H, this amounts to saying that the elements σ_i and a_i satisfy the defining relations (3.1) of $B_\bullet$. □

The previous result shows that there is no flexibility or randomness in the construction of an ALD-system using the formulas of (3.7). However, what was not explained here—nor was it in [6] either—is where do these formulas come from. Actually, the group $B_\bullet$ and the formulas (3.7) arise naturally when investigating the so-called geometry monoid of the ALD laws. This will be explained in a forthcoming paper.

References

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

[2] M. Brin, *The algebra of strand splitting. I. A braided version of Thompson's group V*, Int. J. for Algebra and Comput., to appear, math.GR/040642.

[3] M. Brin, *The algebra of strand splitting. II. A presentation for the braid group on one strand*, J. Group Th., to appear, math.GR/040643.

[4] P. Dehornoy, *Braids and Self-Distributivity*, Progress in Math. vol. 192, Birkhäuser, (2000).

[5] P. Dehornoy, *Geometric presentations of Thompson's groups*, J. Pure Appl. Algebra, to appear, math.GR/0407096.

[6] P. Dehornoy, *The group of parenthesized braids*, Advances in Math., to appear, math.GR/0407097.
[7] A. Drápal, *Persistence of left distributive algebras*, J. Pure Appl. Algebra **105** (1995) 137–165.
[8] A. Drápal, *Finite left distributive algebras with one generator*, J. Pure Appl. Algebra **121** (1997) 233–251.
[9] R. Fenn & C.P. Rourke, *Racks and links in codimension 2*, J. of Knot Theory and its Ramifications (1992) 343–406;
[10] D. Joyce, *A classifying invariant of knots: the knot quandle*, J. of Pure and Appl. Algebra **23** (1982) 37–65;
[11] R. Laver, *Elementary embeddings of a rank into itself*, Abstracts Amer. Math. Soc. **7** (1986) 6.
[12] R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Advances in Math. **91-2** (1992) 209–231.
[13] S.V. Matveev, *Distributive groupoids in knot theory*, Math. Sbornik **119, 1-2** (1982) 73–83.
[14] V.V. Prasolov & A.B. Sossinsky, *Knots, links, braids, and 3-manifolds*, Translation of mathematical monographs **154** Amer. Math. Soc.; 1997.