99.02

Construction of Self-Distributive Operations and Charged Braids

Patrick DEHORNOY

ABSTRACT. Starting from a certain monoid that describes the geometry of the left self-distributivity identity, we construct an explicit realization of the free left self-distributive system on any number of generators. This realization lives in the charged braid group, an extension of Artin's braid group B_∞ with a simple geometrical interpretation.

AMS Classification: 20N02, 20F36, 08B20.

Constructing examples of operations that satisfy a given identity and, in particular, constructing a concrete realization of the free objects in the associated equational variety is an obviously difficult task, for which no uniform method exists. Here we consider these questions in the case of the left self-distributivity identity

$$x * (y * z) = (x * y) * (x * z). \qquad (LD)$$

Due to its connection with set theory [13] [14] [8] and knot theory [1] [9] [10], this identity has received much attention in the recent years. A binary system made of a set equipped with a left self-distributive operation will be called an *LD-system*. Thus the question we consider here is the construction of concrete realizations of free LD-systems.

The first result in this direction has been obtained by R. Laver in [13]: if j is a non-trivial elementary embedding of a rank into itself, then the family of all iterations of j equipped with the operation of applying an embedding to another one is a free LD-system. This solution however is not completely satisfactory, as the existence of the object it relies upon, namely a non-trivial elementary embedding of a rank into itself, is an unprovable set-theoretical axiom, one for which even a relative consistency result cannot be proved. Subsequently, we have shown in [6] how to deduce from the general study of the identity (LD) the existence of a left self-distributive operation on Artin's braid group B_∞. This construction provides a concrete realization for the free LD-system on one generator inside B_∞, leading in particular to an efficient solution for the word problem of the identity (LD)—and to new results about braids, such as the orderability of this group and a new efficient algorithm for its word problem. On the other hand, Larue has shown in [12] how to extend 'by hand' the braid group B_∞ so as to obtain a realization for the free LD-system on any number of generators.

In this paper, we show how to extend the analysis of [6] so as to include the case of several generators. This leads to introducing an extension of Artin's braids that we call *charged braids*. The precise result is as follows.

Proposition. *Let CB_∞ be the extension of Artin's braid group B_∞ obtained by adding an infinite sequence of mutually commuting generators ρ_1, ρ_2, ... submitted to the relations*

$$\sigma_i\rho_j = \rho_j\sigma_i \quad \text{for } j < i \text{ and } j > i+1, \qquad \sigma_i\rho_i\rho_{i+1} = \rho_i\rho_{i+1}\sigma_i \quad \text{for every } i.$$

Let sh *be the endomorphism of CB_∞ that maps σ_i to σ_{i+1} and ρ_j to ρ_{j+1} for all i, j. Then the operation $*$ defined on CB_∞ by $a * b = a\ \mathrm{sh}(b)\ \sigma_1\ \mathrm{sh}(a)^{-1}$ is left self-distributive, and the elements 1, ρ_1, ρ_1^2, ... generate in $(CB_\infty, *)$ a free LD-system.*

The realization we obtain here turns out to be a (proper) quotient of that obtained by Larue, which lives in a much bigger extension of Artin's braid group. Yet quite simple in definition, Larue's group is very large and, so to speak, abstract. The current group CB_∞ appears more canonical in its construction, and, being much closer to Artin's braid group B_∞ than Larue's group, it hopefully shares a number of properties of B_∞. In particular, the elements of CB_∞ receive natural interpretations as braids where the strands are decorated with integer charges, and we think that investigating such objects can be interesting in itself. Another advantage of using the group CB_∞ here is that the proof of freeness involved in the above proposition is more simple than the one in [12]. We also give a new proof for the freeness of the monogenic LD-systems of B_∞ which is more simple than the original argument of [6].

The organization of the text is as follows. In the first section, we explicitely describe the construction scheme which remained implicit in the published version of [6], and show how to extend it to the case of several generators. In this way, we obtain a left self-distributive operation on a quotient of a certain group that describes the geometry of Identity (LD). In Section 2, we show that the involved quotient is an extension CB_∞ of Artin's braid group B_∞, and we interpret the elements of CB_∞ as charged braids. We also mention a few elementary properties of the group CB_∞. In Section 3, we show that the group CB_∞ includes a free LD-system on countably many generators.

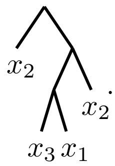
1. The characteristic operator of a term

In this section, we show how to define a certain group EG_{LD} that models the geometry of Identity (LD), and how to associate with every term t a distinguished element of EG_{LD} that reflects the inductive construction of t. This leads to the existence of a left self-distributive operation on a quotient of EG_{LD}.

Let (I) be an algebraic identity. We assume that (I) involves only one binary operation, and that the same variables occur in both members of (I). Typical examples of such identities are the associativity identity $x*(y*z) = (x*y)*z$, or the left self-distributivity identity (LD). We fix an infinite sequence of variables x_1, x_2, ..., and we write T_∞ for the set of all well-formed terms constructed using the operator $*$ and the variables x_i. Thus, (I) itself is a pair of terms in T_∞, say (t_L, t_R)—also denoted $t_L = t_R$.

For t a term and f a mapping of the variables into T_∞, we denote by $f(t)$ the term obtained from t by replacing every variable x with the corresponding term $f(x)$, *i.e.*, the image of t under the substitution f. Applying the identity (t_L, t_R) to the term t means replacing some subterm of t of the form $f(t_L)$ for some substitution f by the corresponding term $f(t_R)$. This transformation can be seen as applying to the term t an *operator* depending on the geometric position of the considered subterm in t (and on the considered identity).

In order to introduce the previous operators precisely, we use a system of addresses for the subterms of a term. To this end we consider terms as binary trees whose leaves are labelled with variables while inner nodes represent the operator. For instance, we see the term $x_2 * ((x_3 * x_1) * x_2)$ as the tree

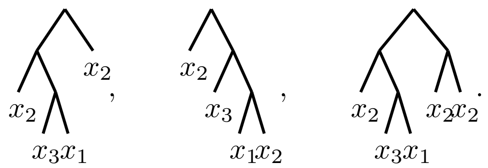


We use finite sequences of 0's and 1's as addresses in such trees, with the convention that the empty sequence λ is the address of the root of the tree, and that 0 means forking to the left, while 1 means forking to the right. For instance in the term above the subterm (*i.e.*, the subtree) with address 10, called the 10-subterm of t, is $x_3 * x_1$. The set of all addresses is denoted $\mathbf{A}$.

Definition. Let (I) be an algebraic identity, say $I = (t_L, t_R)$, and α be an address. We define I^+_α to be the partial operator on T_∞ that maps every term t that admits an α-subterm of the form $f(t_L)$, f a substitution, to the term obtained by replacing the α-subterm of t with $f(t_R)$. We define I^-_α to be the inverse mapping of I^+_α, and we define the *geometry monoid of* (I) to be the monoid $\mathcal{G}_I$ generated by all operators I^+_α and I^-_α with α in $\mathbf{A}$, using reversed composition as product.

The hypothesis that the same variables appear in both sides of the identity (I) implies that all operators $I^\pm_\alpha$ are functional and injective.

Example. Let t be the above term $x_2 * ((x_3 * x_1) * x_2)$. Then, using (A) and (LD) to denote respectively the associativity identity and the left self-distributivity identity, we find that the images of t under the operators A^+_λ, A^-_1 and LD^+_λ are respectively



Observe that the three terms above are the only existing images of t under operators of the form $A^\pm_\alpha$ or $LD^\pm_\alpha$. By construction of I-equivalence, we have the following result.

Lemma 1.1. *Assume that (I) is an algebraic identity involving a single binary operator and the same variables occur in both members of (I). Then two terms t, t' are I-equivalent if and only if some operator in the geometry monoid $\mathcal{G}_I$ maps t to t'.*

We refer to [4] and [7] for results about the monoids $\mathcal{G}_I$, and we consider now the specific case of Identity (LD). We begin with the case of one generator. We write x for x_1, and introduce the subset T_1 of T_∞ consisting of those terms that involve the variable x only. For p a positive integer, we denote by $x^{[p]}$ the term inductively defined by $x^{[1]} = x$, $x^{[p+1]} = x * x^{[p]}$.

Definition. Assume that f is a (partial) mapping of T_∞ into itself, and α is an address. The *α-shifting of f*, denoted $\mathrm{sh}_\alpha(f)$, is the partial mapping of T_∞ into itself that maps every term t such that the α-subterm of t is defined and belongs to the domain of f to the term obtained from t by applying f to this α-subterm of t.

Thus, for instance, we have in $\mathcal{G}_{LD}$ the equality $LD^+_\alpha = \mathrm{sh}_\alpha(LD^+_\lambda)$ for every address α, and, more generally, $LD^+_{\alpha\beta} = \mathrm{sh}_\alpha(LD^+_\beta)$ for all α, β in $\mathbf{A}$.

Let $t =_{LD} t'$ mean that t and t' are LD-equivalent. A significant property of Identity (LD) is that, for every term t in T_1, the equivalence

$$x^{[p+1]} =_{LD} t * x^{[p]} \tag{1.1}$$

holds for p large enough. So, by Lemma 1.1, some operator in $\mathcal{G}_{LD}$ has to map the term $x^{[p+1]}$ to the term $t * x^{[p]}$. Now, the inductive proof of (1.1) shows that, if we define for t in T_1 the operator $\mathrm{op}(t)$ by the rules

$$\mathrm{op}(x) = \mathrm{id}, \quad \mathrm{op}(t_0 * t_1) = \mathrm{op}(t_0) \cdot \mathrm{sh}_1(\mathrm{op}(t_1)) \cdot LD^+ \cdot \mathrm{sh}_1(\mathrm{op}(t_0))^{-1},$$

then, for p large enough, $\mathrm{op}(t)$ maps $x^{[p+1]}$ to $t * x^{[p]}$.

Assume that t and t' are LD-equivalent terms in T_1. By Lemma 1.1, some operator f in $\mathcal{G}_{LD}$ maps t to t'. Then, for every p, the operator $\mathrm{sh}_0(f)$ maps the term $t * x^{[p]}$ to the term $t' * x^{[p]}$. By construction, the quotient $\mathrm{op}(t)^{-1} \cdot \mathrm{op}(t')$ also maps the term $t * x^{[p]}$ to the term $t' * x^{[p]}$. This suggests that the operators $\mathrm{op}(t)^{-1} \cdot \mathrm{op}(t')$ and $\mathrm{sh}_0(f)$ could be equal, *i.e.*, that the operator $\mathrm{op}(t)^{-1} \cdot \mathrm{op}(t')$ could lie in the submonoid of $\mathcal{G}_{LD}$ generated by those operators of the form $LD^\pm_{0\alpha}$. If this is true, the image of $\mathrm{op}(t)$ in the "quotient" $\mathcal{G}_{LD}/\mathrm{sh}_0(\mathcal{G}_{LD})$ should depend only on the LD-equivalence class of t, *i.e.*, there should exist a left self-distributive operation on this quotient.

The previous approach does not work readily, as $\mathcal{G}_{LD}$ is not a group because it consists of partial operators only. In order to avoid the problem, our strategy is to study those relations that connect the generators of $\mathcal{G}_{LD}$, and to replace $\mathcal{G}_{LD}$ with the group G_{LD} that admits these relations as a presentation.

There exist in general a number of relations between the operators I^+_α in the monoid $\mathcal{G}_I$ associated with a given identity (I). Some of them are not really specific of the considered identity. For instance, if two addresses α and β are orthogonal, *i.e.*, if there exists some address γ such that α begins with $\gamma 0$ and β begins with $\gamma 1$, the operators I^+_α and I^+_β commute. In the particular case of (LD), we refer to [3] for a proof that the following relations hold for every addresses α, β, γ:

$$LD^+_{\alpha 0\beta} \cdot LD^+_{\alpha 1\gamma} = LD^+_{\alpha 1\gamma} \cdot LD^+_{\alpha 0\beta} \tag{1.2}$$

$$LD^+_{\alpha 1} \cdot LD^+_{\alpha} \cdot LD^+_{\alpha 1} \cdot LD^+_{\alpha 0} = LD^+_{\alpha} \cdot LD^+_{\alpha 1} \cdot LD^+_{\alpha} \tag{1.3}$$

$$LD^+_{\alpha 11\beta} \cdot LD^+_{\alpha} = LD^+_{\alpha} \cdot LD^+_{\alpha 11\beta}, \qquad LD^+_{\alpha 10\beta} \cdot LD^+_{\alpha} = LD^+_{\alpha} \cdot LD^+_{\alpha 01\beta}$$

$$LD^+_{\alpha 0\beta} \cdot LD^+_{\alpha} = LD^+_{\alpha} \cdot LD^+_{\alpha 10\beta} \cdot LD^+_{\alpha 00\beta} \tag{1.4}$$

Definition. We call G_{LD} the group generated by a sequence $(g_\alpha\ ;\ \alpha \in \mathbf{A})$ submitted to the previous relations, *i.e.*,

$$g_{\alpha 0\beta} \cdot g_{\alpha 1\gamma} = g_{\alpha 1\beta} \cdot g_{\alpha 0\gamma}, \quad g_{\alpha 1} \cdot g_\alpha \cdot g_{\alpha 1} \cdot g_{\alpha 0} = g_\alpha \cdot g_{\alpha 1} \cdot g_\alpha,$$
$$g_{\alpha 11\beta} \cdot g_\alpha = g_\alpha \cdot g_{\alpha 11\beta}, \quad g_{\alpha 10\beta} \cdot g_\alpha = g_\alpha \cdot g_{\alpha 01\beta}, \quad g_{\alpha 0\beta} \cdot g_\alpha = g_\alpha \cdot g_{\alpha 10\beta} \cdot g_{\alpha 00\beta}.$$

In order to imitate inside G_{LD} the construction of the operator $\mathrm{op}(t)$, we consider the mapping χ inductively defined on T_1 by the rules:

$$\chi(x) = 1, \quad \chi(t_0 * t_1) = \chi(t_0) \cdot \mathrm{sh}_1(\chi(t_1)) \cdot g_\lambda \cdot \mathrm{sh}_1(\chi(t_0))^{-1},$$

where sh_α is the endomorphism of G_{LD} that maps g_v to $g_{\alpha\beta}$ for every β. This amounts to saying that χ is the homomorphism of $(T_1, *)$ into $(G_{LD}, *)$ that maps x to 1, where $*$ is the binary operation defined on G_{LD} by

$$a * b = a \cdot \mathrm{sh}_1(b) \cdot g_\lambda \cdot \mathrm{sh}_1(a)^{-1}. \tag{1.5}$$

Then the result is what we expected.

Proposition 1.2. [6] *Let H_0 be the subgroup of G_{LD} generated by all elements $g_{0\alpha}$. Then the binary operation $*$ of (1.5) induces a left self-distributive operation on the right coset set G_{LD}/H_0.*

The point in the previous argument was to associate with every one variable term t a characteristic operator $\mathrm{op}(t)$ that describes it in some convenient sense, here in the sense that $\mathrm{op}(t)$ maps $x^{[p+1]}$ to $t * x^{[p]}$ for p large enough. Let us mention that a similar approach is possible in the case of associativity [7], where it leads to the simple group G of [15].

In order to extend the construction to the case of several generators, we have to define the characteristic operators $\mathrm{op}(t)$ so as to be able to generate all terms in T_∞, and not only those with one variable. To this end, besides the operators $LD_\alpha^\pm$, we introduce new operators whose action is to shift the names of the variables.

Definition. Assume that α is an address. We define Θ_α^+ to be the partial function of T_∞ into itself that maps every term t such that the α-subterm of t exists to the term obtained from t by shifting by one unit the indices of those variables that occur below the address α in t. We define Θ_α^- to be the inverse of Θ_α^+. Finally, the *extended geometry monoid* of Identity (LD) is the monoid $\mathcal{EG}_{LD}$ generated by all operators $LD_\alpha^\pm$ and $\Theta_\alpha^\pm$ for α in $\mathbf{A}$.

Proposition 1.3. *For t in T_∞, define the operator $\mathrm{op}(t)$ inductively by the rules:*

$$\mathrm{op}(x_i) = (\Theta_0^+)^{i-1}, \qquad \mathrm{op}(t_0 * t_1) = \mathrm{op}(t_0) \cdot \mathrm{sh}_1(\mathrm{op}(t_1)) \cdot LD_\lambda^+ \cdot \mathrm{sh}_1(\mathrm{op}(t_0))^{-1}.$$

Then, for p large enough, the operator $\mathrm{op}(t)$ maps the term $x_1^{[p+1]}$ to the term $t * x_1^{[p]}$.

Proof. Induction on t. If t is a variable, say x_i, then, by definition, the operator $(\Theta_0^+)^{i-1}$ maps $x_1^{[p+1]}$ to $x_i * x_1^{[p]}$ for every $p \geq 1$. Assume now $t = t_0 * t_1$. For p large enough, we obtain, using the induction hypothesis,

$$\begin{aligned} x^{[p+1]} \overset{\mathrm{op}(t_0)}{\longmapsto} t_0 * x^{[p]} &\overset{\mathrm{sh}_1(\mathrm{op}(t_1))}{\longmapsto} t_0 * (t_1 * x^{[p-1]}) \\ &\overset{LD_\lambda^+}{\longmapsto} (t_0 * t_1) * (t_0 * x^{[p-1]}) \overset{\mathrm{sh}_1(\mathrm{op}(t_0))^{-1}}{\longmapsto} (t_0 * t_1) * x^{[p]}, \end{aligned}$$

i.e., $\mathrm{op}(t)$ maps $x^{[p+1]}$ to $t * x^{[p]}$. ∎

Like $\mathcal{G}_{LD}$, the extended monoid $\mathcal{EG}_{LD}$ is not a group, so we consider instead a group that resembles $\mathcal{EG}_{LD}$. To this end, we first list the additional relations caused by the introduction of the operators Θ^+_α in $\mathcal{G}_{LD}$. In the following statement, the relation $f \approx f'$ means that the operators f and f' coincide on the intersection of their domains, which are not supposed to be equal.

Lemma 1.4. *The following relations hold in $\mathcal{EG}_{LD}$ for all addresses α, β, γ:*

$$\Theta^+_\alpha \approx \Theta^+_{\alpha 1} \cdot \Theta^+_{\alpha 0}, \quad \Theta^+_{\alpha 0\beta} \cdot \Theta^+_{\alpha 1\gamma} = \Theta^+_{\alpha 1\gamma} \cdot \Theta^+_{\alpha 0\beta} \tag{1.6}$$

$$\Theta^+_{\alpha 0\beta} \cdot LD^+_{\alpha 1\gamma} = LD^+_{\alpha 1\gamma} \cdot \Theta^+_{\alpha 0\beta}, \qquad \Theta^+_\alpha \cdot LD^+_{\alpha\beta} = LD^+_{\alpha\beta} \cdot \Theta^+_\alpha, \tag{1.7}$$

$$\Theta^+_{\alpha 0\beta} \cdot LD^+_\alpha = LD^+_\alpha \cdot \Theta^+_{\alpha 10\beta} \cdot \Theta^+_{\alpha 00\beta}, \quad \Theta^+_{\alpha 10\beta} \cdot LD^+_\alpha = LD^+_\alpha \cdot \Theta^+_{\alpha 01\beta},$$
$$\Theta^+_{\alpha 11\beta} \cdot LD^+_\alpha = LD^+_\alpha \cdot \Theta^+_{\alpha 11\beta} \tag{1.8}$$

Proof. Straightforward in the case of (1.5) and (1.6). In the case of the three relations (1.7), which are similar to the three relations (1.4), we use the fact that, assuming that the operator LD^+_α maps the term t to the term t', then every $\alpha 0\beta$-subterm in t has two copies in t', namely the $\alpha 10\beta$- and $\alpha 00\beta$-subterms. Similarly, every $\alpha 01\beta$-subterm of t' comes from the associated $\alpha 10\beta$-subterm of t. ■

As in the case of $\mathcal{G}_{LD}$ and G_{LD}, we introduce the group for which the above mentioned relations make a presentation.

Definition. The group EG_{LD} is the extension of G_{LD} obtained by adding a sequence of new generators $(h_\alpha\ ;\ \alpha \in \mathbf{A})$ submitted to the relations

$$h_\alpha = h_{\alpha 1} \cdot h_{\alpha 0}, \qquad h_{\alpha 0\beta} \cdot h_{\alpha 1\gamma} = h_{\alpha 1\gamma} \cdot h_{\alpha 0\beta} \tag{1.9}$$

$$h_{\alpha 0\beta} \cdot g_{\alpha 1\gamma} = g_{\alpha 1\gamma} \cdot h_{\alpha 0\beta}, \qquad h_\alpha \cdot g_{\alpha\beta} = g_{\alpha\beta} \cdot h_\alpha, \tag{1.10}$$

$$h_{\alpha 0\beta} \cdot g_\alpha = g_\alpha \cdot h_{\alpha 10\beta} \cdot h_{\alpha 00\beta},\ h_{\alpha 10\beta} \cdot g_\alpha = g_\alpha \cdot h_{\alpha 01\beta},\ h_{\alpha 11\beta} \cdot g_\alpha = g_\alpha \cdot h_{\alpha 11\beta} \tag{1.11}$$

For α an address, we define sh_α to be the endomorphism of EG_{LD} that maps g_β to $g_{\alpha\beta}$ and h_β to $h_{\alpha\beta}$ for every β; we use $*$ for be the binary operation defined on EG_{LD} by (1.5).

By construction, the group G_{LD} embeds in the group EG_{LD}, and the operation $*$ on EG_{LD} extends that of G_{LD}. According to our general strategy, we mimic the definition of the characteristic operator $\mathrm{op}(t)$ in the group EG_{LD}.

Definition. The mapping χ is defined to be the homomorphism of $(T_\infty, *)$ into $(EG_{LD}, *)$ that maps x_i to h_0^{i-1}.

Lemma 1.5. *For all a, b, c in EG_{LD} and all α, β in $\mathbf{A}$, we have*

$$(a * b) * (a * c) = (a * (b * c)) \cdot g_0 \tag{1.12}$$

$$(a \cdot g_{0\alpha}) * (b \cdot g_{0\beta}) = (a * b) \cdot g_{00\alpha} \cdot g_{01\beta} \tag{1.13}$$

Proof. For (1.12), using the defining relations, in particular the fact that g_λ commutes with $g_{11\alpha}$ and $h_{11\alpha}$, we find

$$(a * b) * (a * c) = a \cdot \mathrm{sh}_1(b) \cdot tr_{11}(c) \cdot g_\lambda \cdot g_1 \cdot g_\lambda \cdot g_1^{-1} \cdot \mathrm{sh}_{11}(b)^{-1} \cdot \mathrm{sh}_1(a)^{-1},$$
$$a * (b * c) = a \cdot \mathrm{sh}_1(b) \cdot tr_{11}(c) \cdot g_1 \cdot g_\lambda \cdot \mathrm{sh}_{11}(b)^{-1} \cdot \mathrm{sh}_1(a)^{-1}.$$

Now $g_\lambda g_1 g_\lambda g_1^{-1}$ is $g_1 g_\lambda g_0$, and g_0 commutes with all generators $g_{1\alpha}$ and $h_{1\alpha}$.

For (1.13), using the defining relations, in particular the fact that $g_{0\alpha}$ commutes with $g_{1\beta}$ and $h_{1\beta}$, we find

$$\begin{aligned}(a \cdot g_{0\alpha}) * (b \cdot g_{0\beta}) &= a \cdot g_{0\alpha} \cdot \mathrm{sh}_1(b) \cdot g_{10\beta} \cdot g_\lambda \cdot g_{10\alpha}^{-1} \cdot \mathrm{sh}_1(a)^{-1}\\ &= a \cdot \mathrm{sh}_1(b) \cdot g_{0\alpha} \cdot g_{10\beta} \cdot g_\lambda \cdot g_{10\alpha}^{-1} \cdot \mathrm{sh}_1(a)^{-1}\\ &= a \cdot \mathrm{sh}_1(b) \cdot g_{0\alpha} \cdot g_\lambda \cdot g_{01\beta} \cdot g_{10\alpha}^{-1} \cdot \mathrm{sh}_1(a)^{-1}\\ &= a \cdot \mathrm{sh}_1(b) \cdot g_\lambda \cdot g_{10\alpha} \cdot g_{00\alpha} \cdot g_{01\beta} \cdot g_{10\alpha}^{-1} \cdot \mathrm{sh}_1(a)^{-1}\\ &= a \cdot \mathrm{sh}_1(b) \cdot g_\lambda \cdot g_{00\alpha} \cdot g_{01\beta} \cdot \mathrm{sh}_1(a)^{-1}\\ &= a \cdot \mathrm{sh}_1(b) \cdot g_\lambda \cdot \mathrm{sh}_1(a)^{-1} \cdot g_{00\alpha} \cdot g_{01\beta} = (a * b) \cdot g_{00\alpha} \cdot g_{01\beta}. \qquad \blacksquare\end{aligned}$$

Lemma 1.6. *Assume that the operator LD_α^+ maps the term t to the term t'. Then the equality*

$$\chi(t') = \chi(t) \cdot g_{0\alpha} \tag{1.14}$$

holds in the group EG_{LD}.

Proof. We use induction on the length of the address α. Assume that α is the empty address λ. This means that there exist terms t_0, t_1, t_2 such that t is $t_0 * (t_1 * t_2)$ and t' is $(t_0 * t_1) * (t_0 * t_2)$. Applying (1.12) with $a = \chi(t_0)$, $b = \chi(t_1)$ and $c = \chi(t_2)$ gives (1.14).

Assume now that α is $1\alpha_1$. Then t has the form $t = t_0 * t_1$, and, by hypothesis, t' is then $t_0 * t_1'$ where t_1' is the image of t_1 under the operator $LD_{\alpha_1}^+$. By induction hypothesis, we have $\chi(t_1') = \chi(t_1) \cdot g_{0\alpha_1}$, so we find using (1.13)

$$\chi(t') = \chi(t_0) * \chi(t_1') = \chi(t_0) * (\chi(t_1) \cdot g_{0\alpha_1}) = (\chi(t_0) * \chi(t_1)) \cdot g_{01\alpha_1} = \chi(t) \cdot g_{0\alpha}.$$

Similarly assume that α is $0\alpha_0$. Then t' is $t_0' * t_1$, where t is $t_0 * t_1$ and t_0' is the image of t_0 under $LD_{\alpha_0}^+$. Using again (1.13), we find

$$\chi(t') = \chi(t_0') * \chi(t_1) = (\chi(t_0) \cdot g_{0\alpha_0}) * \chi(t_1) = (\chi(t_0) * \chi(t_1)) \cdot g_{00\alpha_0} = \chi(t) \cdot g_{0\alpha}. \qquad \blacksquare$$

Proposition 1.7. *Let EH_0 be the subgroup of EG_{LD} generated by all elements $g_{0\alpha}$. Then the binary operation $*$ of EG_{LD} induces a left self-distributive operation on the right coset set EG_{LD}/EH_0.*

Proof. By construction, the result is true for those elements that belong to the image of the mapping χ. It is not true that every element of EG_{LD} belongs to the image of χ, and a general proof is needed. Now, Formula (1.13) shows that $*$ induces a well-defined operation on EG_{LD}/EH_0, while Formula (1.12) shows that the induced operation satisfies Identity (LD). $\blacksquare$

The group EG_{LD} is very large. An easy verification shows that the image of the homomorphism χ is included in the subgroup EG'_{LD} of EG_{LD} generated by all g_α's and by those h_α's for which α has the form 1^i0 for some i. The same proof as above gives:

Proposition 1.8. *Let EH'_0 be the subgroup of EG'_{LD} generated by all elements $g_{0\alpha}$. Then the binary operation $*$ of EG'_{LD} induces a left self-distributive operation on the right coset set EG'_{LD}/EH'_0.*

2. The charged braid group

There exists a close connection between the group G_{LD} of Section 1 and Artin's braid group B_∞. We recall that, for $n \le \infty$, B_n can be defined as the group generated by a sequence $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ submitted to the braid relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \ge 2, \qquad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for every } i. \tag{2.1}$$

Proposition 2.1. *Let N_0 be the normal subgroup of G_{LD} generated by those elements of the form $g_{0\alpha}$ with α in $\mathbf{A}$. Then the quotient group G_{LD}/N_0 is isomorphic to the braid group B_∞.*

Proof. Consider $\pi : G_{LD} \to B_\infty$ such that $\pi(g_\alpha) = 1$ holds if the address α contains at least one 0, and $\pi(g_{1^i})$ is σ_{i+1} (here 1^i denotes the address consisting of i times 1). By comparing the defining relations of G_{LD} and B_∞, we see that π is a well-defined surjective homomorphism. It remains to show that the kernel of π is the subgroup N_0. First, by definition, π vanishes on every generator of the form $g_{0\alpha}$, so N_0 is included in $\mathrm{Ker}(\pi)$. Conversely, repeatedly using the equalities

$$g_{\alpha 10\beta} = g_\alpha \cdot g_{\alpha 01\beta} \cdot {g_\alpha}^{-1},$$

we see that every generator of the form g_u with α an address containing at least one 0 is conjugated in G_{LD} to a generator of the form $g_{0\beta}$, hence one in N_0. ∎

Proposition 2.2. *Let EN_0' be the normal subgroup of EG_{LD}' generated by those elements of the form $g_{0\alpha}$ with α in $\mathbf{A}$. Then the quotient EG_{LD}'/EN_0' is isomorphic to the group obtained from B_∞ by adding a sequence of mutually commuting generators $\rho_1, \rho_2, \ldots$ submitted to the additional relations*

$$\sigma_i\rho_j = \rho_j\sigma_i \quad \text{for } j < i \text{ and } j > i+1, \qquad \sigma_i\rho_i\rho_{i+1} = \rho_i\rho_{i+1}\sigma_i \quad \text{for every } i. \tag{2.2}$$

Proof. We extend the projection π defined in the proof of Proposition 2.1 to the group EG_{LD}' so that h_{1^i0} is mapped to ρ_{i+1}. Again, it is clear from the defining relations that π is a surjective homomorphism of EG_{LD} onto CB_∞. The same proof as above shows that the kernel of π is EN_0'. ∎

Definition. For $n \le \infty$, we define the *n strand charged braid group* to be the extension CB_n of the braid group B_n obtained by adding mutually commuting generators $\rho_1, \ldots, \rho_{n-1}$ submitted to Relations (2.2).

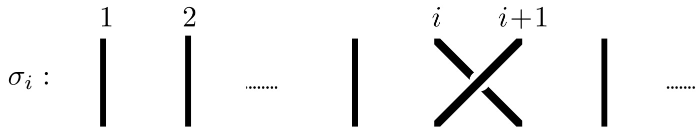
We still write sh for the shift endomorphism of CB_∞ that maps σ_i to σ_{i+1} and ρ_j to ρ_{j+1} for every i, j. Then sh is the image in CB_∞ of the shift mapping sh_1 of EG_{LD}. As in the case of braids, it is not obvious that the left self-distributive operation of EG_{LD}'/EH_0' induces a well-defined operation on EG_{LD}'/EN_0', *i.e.*, on CB_∞. However, an immediate direct verification gives the result.

Proposition 2.3. *The binary operation defined on the group CB_∞ by*

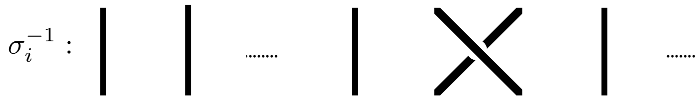
$$a * b = a \cdot \mathrm{sh}(b) \cdot \sigma_1 \cdot \mathrm{sh}(a)^{-1} \tag{2.3}$$

satisfies Identity (LD).

There exists a standard interpretation of the group B_∞ as the group of equivalence classes of two-dimensional braid diagrams consisting of a sequence of mutually crossing strands. One usually associates with the generator σ_i and its inverses the diagrams

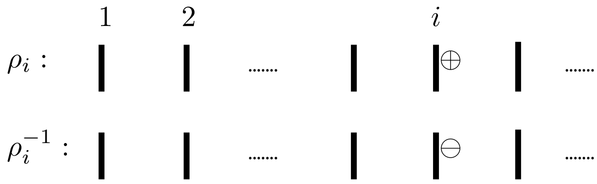


and

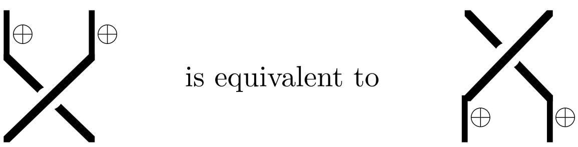


Then the braid diagram associated with the word $\sigma_{i_1}^{e_1} \ldots \sigma_{i_\ell}^{e_\ell}$ is obtained by composing the elementary diagrams associated with the successive letters, this meaning that one connects the bottom ends of the strands in the first diagram to the top ends of the strands in the second diagram. The braid relations (2.1) express that two braid diagrams represent the same element in B_∞ if and only if they can be seen as plane projections of isotopic three-dimensional figures (see for instance [2])

A similar geometrical interpretation can be given for the elements of CB_∞. We consider *charged* braid diagrams consisting of standard braid diagrams completed with additional signed charges appended to the strands of the braids. We interpret the generator ρ_i as a $\oplus$-charge on the i-th strand, and its inverse ρ_i^{-1} as an opposite $\ominus$-charge on the i-th strand:



Then the relations of the group CB_∞ express that a $\oplus$-charge is the inverse of a $\ominus$-charge and that the charges may freely move on the strands, with the exception that a $\oplus$-charge is allowed to go through a crossing only if another $\oplus$-charge simultaneously goes on the other strand of the crossing:



With the above interpretation, calling the elements of CB_n charged braids should appear as natural. We shall not develop a systematic study of the charged braid groups CB_n here, but only mention a few easy properties.

Proposition 2.4. *Let ϕ_n denote the forgetful mapping that keeps σ_i unchanged, and collapses ρ_j to 1 for every j. Then ϕ_n induces a surjective homomorphism of CB_n onto B_n. The group B_n embeds in CB_n, and CB_n is a semidirect product of B_n by* $\mathrm{Ker}(\phi_n)$.

Proof. Everything is clear, as ϕ_n projects the additional relations (2.2) to trivial relations in B_∞. ■

The subgroup $\mathrm{Ker}(\phi_n)$ includes the subgroup generated by all ρ_j's, a group isomorphic to the direct power $\mathbf{Z}^n$. But the inclusion is strict: for instance, $\sigma_1\rho_1\sigma_1^{-1}$ belongs to $\mathrm{Ker}(\phi_n)$, but not to the above subgroup. To prove the latter statement formally, we can resort to a linear representation of charged braids. We recall that the (unreduced) Burau representation of B_n is the linear representation that maps σ_i to the matrix obtained from the $n\times n$ identity matrix by replacing the $(i, i+1)$-submatrix with $\begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix}$.

Proposition 2.5. *Extending the Burau representation r of B_n by defining $r(\rho_j)$ to be the diagonal matrix with diagonal values $(1, \dots, 1, u, 1, \dots, 1)$, u at position j, yields a linear representation of CB_n into $\mathrm{GL}_n(\mathbf{Z}[t, t^{-1}, u, u^{-1}])$.*

The verification is straightforward. So, for instance, we find

$$r(\sigma_1\rho_1\sigma_1^{-1}) = \begin{pmatrix} 1 & (u-1)(1-t) \\ 0 & u \end{pmatrix}, \quad r(\sigma_1\rho_2\sigma_1^{-1}) = \begin{pmatrix} u & (1-u)(1-t) \\ 0 & 1 \end{pmatrix}.$$

These values prove that $\sigma_1\rho_1\sigma_1^{-1}$ cannot belong to the subgroup of CB_∞ generated by the ρ_j's, as the Burau representation of every element of this subgroup is a diagonal matrix.

Proposition 2.6. *The group B_∞ is not a normal subgroup of CB_∞.*

Proof. Still letting r denote the extended Burau representation, we find

$$r(\rho_1\sigma_1\rho_1^{-1}) = \begin{pmatrix} 1-t & tu \\ u^{-1} & 0 \end{pmatrix}, \quad r(\rho_2\sigma_1\rho_2^{-1}) = \begin{pmatrix} 1-t & tu^{-1} \\ u & 0 \end{pmatrix}.$$

Now, the Burau representation of every element of B_∞ is a t-Markovian matrix: the sum of the elements in the i-th row is equal to t^{i-1}. So $\rho_1\sigma_1\rho_1^{-1}$ cannot belong to B_∞. ■

In particular, the semi-direct product of Proposition 2.4 is not a direct product. The next observation is that the usual representation of braids into automorphisms of a free group can be extended to charged braids.

Proposition 2.7. *For $n \le \infty$, let $FG_{n,\infty}$ denote a free group based on a double sequence of generators $(x_{p,q})_{1\le p\le n, q\in\mathbf{Z}}$. Then the mapping ψ defined by*

$$\psi(\sigma_i)(x_{p,q}) = \begin{cases} x_{p,q} & \text{for } p \neq i, i+1, \\ x_{p,q}x_{p+1,q}x_{p,q}^{-1} & \text{for } p = i, \\ x_{p,q} & \text{for } p = i+1, \end{cases} \qquad \psi(\rho_j)(x_{p,q}) = \begin{cases} x_{p,q} & \text{for } p \neq j, \\ x_{p,q+1} & \text{for } p = j, \end{cases}$$

provides a homomorphism of the group CB_n into $\mathrm{Aut}(FG_{n,\infty})$.

The result follows from the defining relations of CB_∞. We conjecture that the previous homomorphism is an embedding.

As a final result, we observe that the charged braid group CB_∞ is a quotient of Larue's group of [12].

Proposition 2.8. *Let LB_∞ be the extension of Artin's braid group obtained by adding a double sequence of generators $(\theta_{j,k}\ ;\ j, k \ge 1)$ submitted to $\sigma_i\theta_{j,k} = \theta_{j,k}\sigma_i$ for $j > i+1$. Then the mapping defined by $\theta_{j,k} \mapsto \rho_j^{k-1}$ induces a surjective homomorphism of LB_∞ onto CB_∞.*

The result follows again from the defining relations of the groups.

3. Proofs of freeness

We have seen above that the existence of a left self-distributive operation on the groups B_∞ and CB_∞ is implied and somehow explained by their connection with the monoids $\mathcal{G}_{LD}$ and $\mathcal{EG}_{LD}$. The main interest of the construction lies in the fact that the LD-systems obtained in this way include *free* LD-systems.

Proposition 3.1. *The element* 1 *generates a free LD-system in* $(B_\infty, *)$.

Proposition 3.2. *The elements* 1, ρ_1, ρ_1^2, ... *generate a free LD-system in* $(CB_\infty, *)$.

Proposition 3.1 already appears in [6]. Here, we present a new proof, which is much more direct than the original proof, provided the fact that free LD-systems admit left cancellation is known.

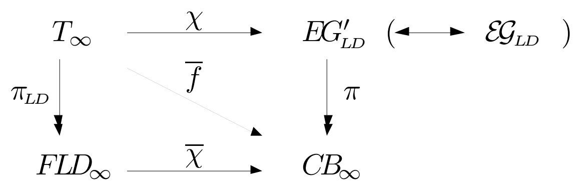
Let us first fix some notations. We use BW_∞ for the free monoid of all braid words, *i.e.*, of all words formed on the letters $\sigma_i^{\pm 1}$. Similarly, we use CBW_∞ for the free monoid of all charged braid words. We say that the (charged) braid word w represents the (charged) braid b if b is the class of w in CB_∞. We still use $*$ for the binary operation defined on CBW_∞ by

$$u * v = u \cdot \mathrm{sh}(v) \cdot g_1 \cdot \mathrm{sh}(u)^{-1}, \tag{3.1}$$

where sh is the shift endomorphism of CBW_∞ that maps $\sigma_i^{\pm 1}$ to $\sigma_{i+1}^{\pm 1}$ and $\rho_j^{\pm 1}$ to $\rho_{j+1}^{\pm 1}$ for all i, j. So, the word $u * v$ represents the (charged) braid $a * b$ when u, v represent a and b.

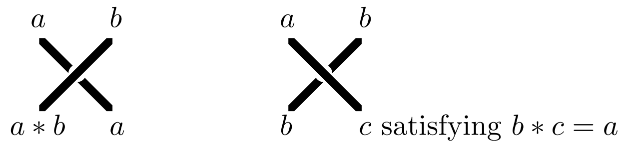
We let f denote the homomorphism of $(T_\infty, *)$ into $(CBW_\infty, *)$ that maps x_i to ρ_1^{i-1}, and $\overline{f}$ for the homomorphism of $(T_\infty, *)$ into $(CB_\infty, *)$ induced by f. By construction, the charged braid $\overline{f}(t)$ is the projection in CB_∞ of the element $\chi(t)$ in EG'_{LD}. If t lies in T_1, then $f(t)$ belongs to BW_∞, and $\overline{f}(t)$ is an ordinary braid. For instance, the reader can verify that, if t is the term $x_2 * ((x_3 * x_1) * x_2)$, then $f(t)$ is the charged braid word $\rho_1\rho_2^2\sigma_2\rho_3^{-1}\sigma_2\rho_4^2\sigma_3^{-1}\rho_3^{-2}\sigma_1\rho_2^{-1}$ displayed in Figure 3.1 below.

Let FLD_1 and FLD_∞ denote respectively the free LD-system on one generator and the free LD-system on countably many generators. By construction, FLD_1 is $T_1/=_{LD}$, and FLD_∞ is $T_\infty/=_{LD}$. We write π_{LD} for the corresponding projections. The fact that the operation $*$ on CB_∞ is left self-distributive implies that the homomorphism $\overline{f}$ factors through a homomorphism $\overline{\chi}$ of FLD_∞ into CB_∞, and we have the following commutative diagram:



Proving Proposition 3.1 and 3.2 amounts to proving that the mapping $\overline{\chi}$ is injective, *i.e.*, that, if t and t' are LD-unequivalent terms in T_1 (*resp.* in T_∞), then the (charged) braid words $f(t)$ and $f(t')$ represent distinct elements in B_∞ (*resp.* in CB_∞).

To this end, we use an action of (charged) braids on LD-systems equipped with a distinguished endomorphism, which we describe now using the intuition of *braid colourings.* We begin with uncharged braids. Let $(S, *)$ be a given binary system. We attribute colours from S to the strands of the braid diagrams according to the following scheme: initial colours are attributed to the top strands, and the colours are propagated downwards so that, when two strands cross, the colours obey the rules



Assuming that $\vec{a}$ is a sequence of colours in S and w is a braid word, we denote by $(\vec{a})w$ the colours of the bottom ends of the strands obtained when $\vec{a}$ is attributed to the top strands in w. This amounts to letting B_∞ act on the right on $S^{\mathbf{N}}$. In order that $(\vec{a})w$ be well defined, we have to assume that the system $(S, *)$ is left divisible and left cancellative, *i.e.*, that left division is always defined in $(S, *)$. If we assume only that $(S, *)$ is left cancellative, then the value of $(\vec{a})w$ is unique when it exists, but it need not exist in every case. It is easily checked that the hypothesis that $(S, *)$ is an LD-system is exactly what is needed for the value of $(\vec{a})w$ to depend only on the braid represented by w, *i.e.*, for the colouring to be compatible with the braid relations (2.1) [1], [6]. We obtain in this way the following result.

Lemma 3.3. [6] *Assume that $(S, *)$ is a left cancellative LD-system, and that w, w' are equivalent braid words. If $\vec{a}$ is a sequence in S such that both $(\vec{a})w$ and $(\vec{a})w'$ exist, then these sequences are equal.*

It is known that the free LD-system FLD_1 is left cancellative [6]. Hence FLD_1 is eligible for colouring braids.

Lemma 3.4. *For every term t, the braid word $f(t)$ is $(FLD_1, *)$-colourable, and we have*

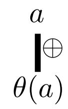
$$(x, x, x, \dots)f(t) = (\pi_{LD}(t), x, x, \dots), \tag{3.2}$$

Proof. The result is obvious if t is x. If t is $t_0 * t_1$, we find inductively

$$\begin{aligned}(x, x, x, \dots)\, f(t) &= (x, x, x, \dots)\, f(t_0) \cdot \mathrm{sh}(f(t_1)) \cdot \sigma_1 \cdot \mathrm{sh}(f(t_0))^{-1} \\ &= (\pi_{LD}(t_0), x, x, \dots)\, \mathrm{sh}(f(t_1)) \cdot \sigma_1 \cdot \mathrm{sh}(f(t_0))^{-1} \\ &= (\pi_{LD}(t_0), \pi_{LD}(t_1), x, \dots)\, \sigma_1 \cdot \mathrm{sh}(f(t_0))^{-1} \\ &= (\pi_{LD}(t), \pi_{LD}(t_0), x, \dots)\, \mathrm{sh}(f(t_0))^{-1} = (\pi_{LD}(t), x, x, \dots)\end{aligned}$$ ∎

We achieve a proof of Proposition 3.1 as follows. Assume that t and t' are terms in T_1 such that $f(t)$ and $f(t')$ represent the same element of B_∞: by Lemma 3.4, the classes $\pi_{LD}(t)$ and $\pi_{LD}(t')$ are equal. Hence the class of $f(t)$ in B_∞ determines the class of t in FLD_1, *i.e.*, the mapping $\overline{\chi}$ is injective. ∎

The natural idea for proving Proposition 3.2 is to use similar colourings for charged braids. To this end, we consider a mapping θ of the colours into themselves, and we add the rule



Compatibility with the relation $\sigma_i \rho_i \rho_{i+1} = \rho_i \rho_{i+1} \sigma_i$ requires that we assume $\theta(a*b) = \theta(a)*\theta(b)$ for the involved colours, and, therefore, it holds true provided that θ is a homomorphism of $(S,*)$. Finally compatibility with $\rho_i \rho_i^{-1} = \rho_i^{-1} \rho_i = 1$ requires that θ be bijective if we want the colouring to be defined everywhere, but only that θ be injective if we accept partial colourings.

Let θ denote the shift endomorphism of FLD_∞ that maps x_i to x_{i+1} for every i. As FLD_∞ is a left cancellative LD-system and θ is an injective endomorphism of FLD_∞, the system $(FLD_\infty, *, \theta)$ is eligible for defining charged braid colourings, and we have the following counterpart of Lemma 3.4.

Lemma 3.5. *The charged braid word $f(t)$ is $(FLD_\infty, *, \theta)$-colourable, and we have*

$$(x_1, x_1, x_1, \ldots) f(t) = (\pi_{LD}(t), x_1, x_1, \ldots), \tag{3.3}$$

The inductive proof is the same as for Lemma 3.4. The colouring of the word $f(t)$ in the case when t is the term $x_2 * ((x_3 * x_1) * x_2)$ is displayed in Figure 3.1.

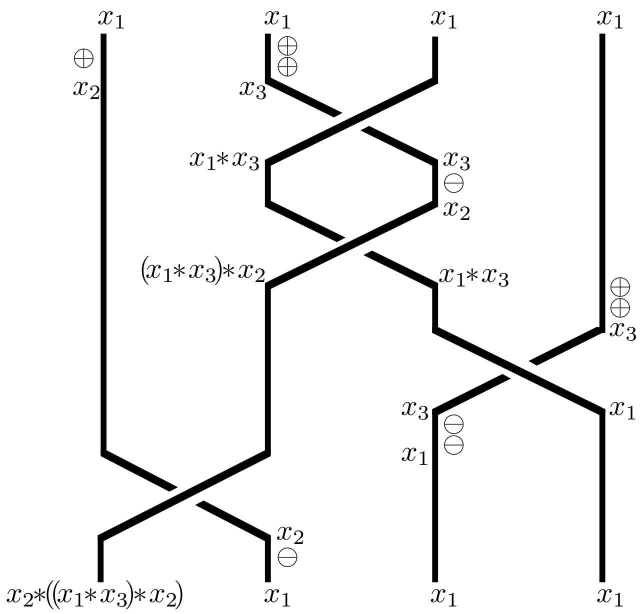


Figure 3.1: Colouring of a charged braid

To go further, we need a counterpart of Lemma 3.3.

Conjecture 3.6. *Assume that $(S,*)$ is a left cancellative LD-system, and that θ is an injective endomorphism of $(S,*)$. Assume that w, w' are equivalent charged braid words, and $\vec{a}$ is a sequence from S such that $(\vec{a})w$ and $(\vec{a})w'$ exist. Then $(\vec{a})w$ and $(\vec{a})w'$ are equal.*

A proof of the previous statement would enable us to conclude the proof of Proposition 3.2 as we did for Proposition 3.1. Now, the problem is that, if w and w' are charged braid words that represent the same element of CB_∞, there exists a finite sequence $(w_0, \ldots, w_N)$ such that w_0 is w, w_N is w' and each word w_i is obtained from w_{i-1} by applying exactly one of the charged braid relations. If there exist initial colours $\vec{a}$ in FLD_∞ such that $(\vec{a})w_i$ exists for every i, then we can show that the sequences $(\vec{a})w$ and $(\vec{a})w'$ are equal. Now it is not clear that such a sequence exists, as the word reversing technique of [6] used in the case of B_∞ does not extend to CB_∞.

The only situation where we can state a compatibility result is the case when the colourings are always defined.

Lemma 3.7. *Assume that $(S, *)$ is a left cancellative left divisible LD-system, and that θ is an automorphism of $(S, *)$. Assume that w, w' are equivalent charged braid words. Then, for every sequence $\vec{a}$ from S, the sequences $(\vec{a})w$ and $(\vec{a})w'$ are equal.*

The verification is easy using the defining relations of the group CB_∞, for, in this case, division is always possible and colouring the negative crossings is not a problem. A typical example of an LD-system that is eligible for Lemma 3.7 to apply is a group equipped with conjugacy and a distinguished injective endomorphism.

Let $FG_{\infty,\infty}$ be a free group based on a double infinite sequence $(x_{p,q})_{p\geq 1, q\in \mathbf{Z}}$, and $*$ be the conjugacy operation of $FG_{\infty,\infty}$ defined by $a * b = a\, b\, a^{-1}$; finally, let θ denote the automorphism of $FG_{\infty,\infty}$ that maps $x_{p,q}$ to $x_{p,q+1}$ for every p, q. The argument we develop now for proving Proposition 3.2 essentially amounts to using the above action of CB_∞ on $(FG_{\infty,\infty}, *, \theta)$. Actually, it will be more convenient to use here the language of automorphisms of $FG_{\infty,\infty}$ so as to be able to apply Larue's method of [11] directly. In order to prove that a given LD-system is free, we have to the following criterion.

Definition. (i) We say that an LD-system $(S, *)$ is *acyclic* if left division in $(S, *)$ has no cycle, *i.e.*, no equality of the form

$$a = (\ldots(a * a_1) * \ldots) * a_p \tag{3.4}$$

with $p \geq 1$ holds in S.
(ii) We say that a subset A of S is *quasifree* in $(S, *)$ if no equality of the form

$$(\ldots((c_1 * \ldots * c_r * x) * a_1) * \ldots) * a_p = (\ldots((c_1 * \ldots * c_r * y) * b_1) * \ldots) * b_q \tag{3.5}$$

with $p, q, r \geq 0$ and x, y distinct elements of A holds in S.

Lemma 3.8. [5] *Assume that $(S, *)$ is an LD-system, and A generates S. Then the following are equivalent:*
(i) The LD-system $(S, *)$ is free based on A;
(ii) The LD-system $(S, *)$ is acyclic and A is quasifree in $(S, *)$.

Lemma 3.9. *The LD-system $(CB_\infty, *)$ is acyclic.*

Proof. By [6], we know that the LD-system $(B_\infty, *)$ is acyclic. Now B_∞ is a homomorphic image of CB_∞. Every possible cycle for left division in CB_∞ would project onto a cycle for left division in B_∞. Hence, such a cycle cannot exist. ∎

Lemma 3.10. *The family* $\{1, \rho_1, \rho_1^2, \ldots\}$ *is quasifree in* $(CB_\infty, *)$.

Proof. By Proposition 2.7, there exists a homomorphism ψ of CB_∞ into $\mathrm{Aut}(FG_{\infty,\infty})$. We denote by ψ^r the composition of ψ with the reversing antiautomorphism of CB_∞ that is the identity on the σ_i's and the ρ_j's. Using ψ^r instead of ψ amounts to using reversed composition rather than composition, *i.e.*, thinking of CB_∞ as acting on the right.

We wish to prove that $a \neq b$ holds in CB_∞ whenever a and b admit decompositions of the form

$$\begin{cases} a = (\ldots((c_1 * \ldots * c_r * \rho_1^i) * a_1) * \ldots) * a_p, \\ b = (\ldots((c_1 * \ldots * c_r * \rho_1^j) * b_1) * \ldots) * b_q \end{cases} \tag{3.6}$$

with $i \neq j$. So assume that a and b satisfy (3.6), and $j = i + k$ holds for some $k > 0$ Expanding (3.6) gives equalities of the form

$$\begin{cases} a = c\,\sigma_r\sigma_{r-1}\ldots\sigma_1\,a_0, \\ b = c\,\rho_r^k\,\sigma_r\sigma_{r-1}\ldots\sigma_1\,b_0, \end{cases}$$

where a_0 and b_0 admit expressions where neither σ_1^{-1} nor $\rho_1^{\pm 1}$ occurs. Now, let x be the element $\psi^r(c\sigma_r..\sigma_1)^{-1}(x_{1,0})$. By construction, we have $\psi^r(c\sigma_r...\sigma_1)(x) = x_{1,0}$, and we find

$$\begin{cases} \psi^r(a)(x) = \psi^r(a_0)(x_{1,0}), \\ \psi^r(b)(x) = \psi^r(b_0)(\psi^r(\sigma_1^{-1}...\sigma_r^{-1}\rho_r^k\sigma_r...\sigma_1(x_{1,0})) = \psi^r(b_0)(x_{1,k}) \end{cases}$$

(we recall that ψ^r is an antihomomorphism). We resort now to Larue's argument used in [11] for establishing the acyclicity of $(B_\infty, *)$. With our current notations, he proves that, if a is a braid that admits an expression where σ_1^{-1} does not occur, then $\psi^r(a)(x_1)$ either is x_1, or it is a reduced word that finishes with x_1^{-1}: by definition, the result is true when $\psi^r(\sigma_1)$ is applied once, and, then, Larue shows that the final letter x_1^{-1} in the image of x_1 can never be cancelled when subsequent automorphisms $\psi^r(\sigma_1)$ or $\psi^r(\sigma_i^{\pm 1})$ with $i \geq 2$ are applied. In the extended framework of charged braids, the only new fact is that some $\rho_j^{\pm 1}$ can change the second index q of some variables $x_{p,q}$ or $x_{p,q}^{-1}$. Now the variables $x_{1,q}^{\pm 1}$ can be changed by the action of $\rho_1^{\pm 1}$ only. So, the hypothesis that a_0 admits an expression without σ_1^{-1} and $\rho_1^{\pm 1}$ implies that Larue's result remains valid, *i.e.*$\psi^r(a_0)(x_{1,0})$ is either $x_{1,0}$, or it finishes with $x_{1,0}^{-1}$. Similarly, the hypothesis that b_0 admits an expression without σ_1^{-1} and $\rho_1^{\pm 1}$ implies that $\psi^r(b_0)(x_{1,k})$ is either $x_{1,k}$, or it finishes with $x_{1,k}^{-1}$. We deduce $\psi^r(a)(x) \neq \psi^r(b)(x)$, hence $\psi^r(a) \neq \psi^r(b)$, and, finally, $a \neq b$. Therefore, any equality of the form (3.6) is impossible in CB_∞. ∎

We can now complete the proof of Proposition 3.2. Let S be sub-LD-system of $(CB_\infty, *)$ generated by 1, ρ_1, ρ_1^2, ... Then, by Lemma 3.9, $(S, *)$ is acyclic, and, by Lemma 3.10, $(1, \rho_1, \rho_1^2, \ldots)$ is quasifree in $(S, *)$. By Lemma 3.8, this implies that S is free based on $\{1, \rho_1, \rho_1^2, \ldots\}$.

We finish with an open question.

Question 3.11. *Does the LD-system* $(B_\infty, *)$ *include a free subsystem with two generators?*

A negative answer seems probable, for space may be missing in B_∞ for constructing independent elements. For instance, we have $\sigma_1 * \sigma_1 = \sigma_2 * \sigma_2$, which shows trivially that the subsystem of $(B_\infty, *)$ generated by σ_1 and σ_2 is not free. More general counterexamples involving arbitrary positive braids can be given, but no complete argument is known to date.

References

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

[2] G. Burde & H. Zieschang, *Knots*, de Gruyter, Berlin (1985).

[3] P. Dehornoy, *Free distributive groupoids*, J. P. Appl. Algebra **61** (1989) 123–146.

[4] —, *Structural monoids associated to equational varieties*, Proc. Amer. Math. Soc. **117-2** (1993) 293–304.

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

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

[7] —, *The structure group for the associativity identity*, J. Pure Appl. Algebra **111** (1996) 59–82.

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

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

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

[11] D. Larue, *On Braid Words and Irreflexivity*, Algebra Univ. **31** (1994) 104–112.

[12] —, *Left-Distributive and Left-Distributive Idempotent Algebras*, Ph D Thesis, University of Boulder (1994).

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

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

[15] R. McKenzie & R.J. Thomson, *An elementary construction of unsolvable word problems in group theory*, *in* Word Problems, Boone & *al.* eds., North Holland, Studies in Logic vol. 71 (1973).

SDAD, Mathématiques, Université Campus 2, BP 5186, 14 032 Caen, France
email address: dehornoy@math.unicaen.fr
URL: http://www.math.unicaen.fr/∼dehornoy