Journal of Pure and Applied Algebra 215 (2011) 276–282

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Left division in the free left distributive algebra on one generator

Richard Laver [a], Sheila K. Miller [b,c,*]

[a] Department of Mathematics, Campus Box 395, University of Colorado, Boulder, CO 80309, United States

[b] University of Colorado, Boulder, United States

[c] Department of Mathematical Sciences, MADN-MATH, United States Military Academy, 646 Swift Road, West Point, NY 10996, United States

ARTICLE INFO

Article history:
Received 14 January 2009
Received in revised form 31 March 2010
Available online 7 June 2010
Communicated by C.A. Weibel

MSC: 08-xx; 06-xx; 20F36; 03E55

ABSTRACT

Let $\mathcal{A}$ be the free algebra on one generator satisfying the left distributive law $a(bc) = (ab)(ac)$. Using a division algorithm for elements of an extension $\mathcal{P}$ of $\mathcal{A}$, we prove some facts about left division in $\mathcal{A}$, one consequence of which is a conjecture of J. Moody: If $a, b, c, d \in \mathcal{A}$, $ab = cd$, a and b have no common left divisors, and c and d have no common left divisors, then $a = c$ and $b = d$.

1. Introduction

A left distributive algebra (LD) is a set L together with a binary operation $\cdot$ on L satisfying the left distributive law: $a \cdot (b \cdot c) = (a \cdot b) \cdot (a \cdot c)$. That is, every left translation is a homomorphism of $(L, \cdot)$. Examples of LD's are group conjugation (where G is a group with operation $*$ and $g \cdot h = g * h * g^{-1}$) and the weighted mean (on, e.g., the complex numbers): for fixed p, let $z \cdot w = pz + (1 - p)w$. Henceforth we will write ab for $a \cdot b$, and we will adopt the convention that $a_0 a_1 \cdots a_{n-1} a_n = ((((a_0 a_1) a_2) \cdots a_{n-1}) a_n)$.

In the two examples above (with $p \neq 1$ in the second) left translation is in fact an automorphism of the algebra. Brieskorn [1] calls such LD's automorphic sets, and gives a number of other examples; see also [9]. The braid groups act on direct products of an automorphic set. Namely for $2 \leq N \leq \infty$ let B_N be the braid group on N strands: B_N is given by generators $\sigma_1, \sigma_2, \ldots, \sigma_i, \ldots (i < N)$ subject to the conditions $\sigma_i \sigma_j = \sigma_j \sigma_i$ when $| i - j | > 1$ and $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ when $| i - j | = 1$. Given an automorphic set $(L, \cdot)$, then for $2 \leq N \leq \infty$, B_N's action on L^N is given by

$$(\langle l_0, \ldots, l_{j-1}, l_j, \ldots, l_i, \ldots \rangle_{i<N})^{\sigma_j} = \langle l_0, \ldots, l_{j-1} l_j, l_{j-1}, \ldots, l_i, \ldots \rangle_{i<N}.$$

This paper is about a different type of LD—the free LD's, in particular the free left distributive algebra $\mathcal{A}$ on one generator x. Namely, for $A =$ the set of all terms in one generator x and one binary operation, $\mathcal{A} = A / \equiv_{LD}$, where, for $u, v \in A$, $u \equiv_{LD} v$ if v can be obtained from u by a series of substitutions of the form $a(bc) \leftrightarrow (ab)(ac)$. No automorphic set can be free; moreover the two examples above are idempotent (for all a, $aa = a$) and in a free LD the generators clearly aren't idempotent and indeed (see Theorem 9 below) there are no idempotent elements.

The question arose whether $\mathcal{A}$ has a natural representation. The first example, the algebra generated by a nontrivial elementary embedding of a rank into itself, is due to Laver [12]. That such embeddings exist is a very strong large cardinal axiom, so the algebra can't be proved to exist from the usual axioms of set theory (ZFC). Subsequently Dehornoy [5] found, in ZFC, a representation of $\mathcal{A}$ by a binary operation on a subset of B_∞.

Order $\mathcal{A}$ by iterated left division: $a <_L b$ if and only if there exist $b_1, b_2, \ldots, b_n \in \mathcal{A}$ such that $b = ab_1 b_2 \cdots b_n$. Dehornoy's and Laver's proofs involved showing that $<_L$ is a linear ordering of $\mathcal{A}$ [3,6,12]. The ordering satisfies $ca <_L cb$ if and only

* Corresponding author at: Department of Mathematical Sciences, MADN-MATH, United States Military Academy, 646 Swift Road, West Point, NY 10996, United States.

E-mail addresses: laver@euclid.colorado.edu (R. Laver), sheila.miller@colorado.edu (S.K. Miller).

0022-4049/$ – see front matter
doi:10.1016/j.jpaa.2010.04.019

if $a <_L b$, thus $\mathcal{A}$ satisfies left cancellation: $ca = cb$ implies $a = b$. Dehornoy [5], weakening the condition on $(L, \cdot)$ from "automorphic set" to "left cancellative LD", then showed that B_N partially acts (as above) on L^N—for $\alpha \in B_N$ $\overrightarrow{l}^{\alpha}$ is uniquely defined when it exists for some expression for α, but, e.g., $\overrightarrow{l}^{\sigma_i^{-1}}$ need not exist. He then showed that this action plus the linearity of $<_L$ on $\mathcal{A}$ induces a linear ordering $<$ of B_∞, the Dehornoy ordering:

$$\text{for } \alpha, \beta \in B_\infty, \alpha < \beta \text{ if and only if for some } N < \infty, \text{ there is an } \overrightarrow{l} \in \mathcal{A}^N \text{ with } \overrightarrow{l}^{\alpha} \text{ lexicographically less than } \overrightarrow{l}^{\beta} \text{ with respect to } <_L .$$

Among the open questions about $\mathcal{A}$ and its relation to the B_N's is the following conjecture: for each $a \in \mathcal{A}$, the set of left divisors of a is well ordered under $<_L$. For a related conjecture about braids, see Section 3. In this paper we prove some facts about left division in $\mathcal{A}$; a consequence of them is the one generator case of a conjecture of J. Moody (Theorem 25):

If $a, b, c, d \in \mathcal{A}$, $ab = cd$, a and b have no common left divisors, and c and d have no common left divisors, then $a = c$ and $b = d$.

The proof gives that a is the $<_L$-least left divisor of w (which occurs if, e.g., the well ordering conjecture is true) if and only if, writing $w = ab$, a and b have no common left divisors.

We assume familiarity with LD algebras (see [5,6,12,13,15]). In Section 2 we give a summary of the basic results about $\mathcal{A}$ and an extension $\mathcal{P}$ of $\mathcal{A}$; $\mathcal{P}$ is the site of a division algorithm (which is the main tool of Sections 3 and 4). The algorithm yields, for $p <_L q$, a unique "normal" representation of q by a term whose leftmost member is p. In Section 3 left divisors are discussed, and a result is proved about them which is used in Section 4. In Section 4 the main results are proved by controlling the length of normal sequences. Section 5 considers the question of extending from one generator to many generators.

2. Summary of basic results about $\mathcal{A}$ and $\mathcal{P}$

In the first part of this section we summarize the results leading up to the linear ordering, $<_L$, of $\mathcal{A}$ and $\mathcal{P}$.

Definition 1. For $u, v \in A$, write $u \to^* v$ if v can be obtained from u by replacing a subterm $a(bc)$ of u with $(ab)(ac)$. Write $u \to v$ if there exist $u_0, \ldots, u_n \in A$ such that $u = u_0 \to^* u_1 \to^* \cdots \to^* u_n = v$.

Theorem 2 (*Confluence (Dehornoy [5])*)**.** *$\mathcal{A}$ is confluent. That is, given $u, v \in A$, $u \equiv_{LD} v$ if and only if $\exists w \in A$ such that $u \to w$ and $v \to w$.*

As mentioned above, the division algorithm (Theorem 12) takes place not in $\mathcal{A}$ but in an extension $\mathcal{P}$ of $\mathcal{A}$. Our basic facts will be in the setting of $\mathcal{P}$. To define $\mathcal{P}$, add a composition symbol, $\circ$, to the language and let Σ be the following set of identities in the language $\{\cdot, \circ\}$:

$$(a \circ b) \circ c = a \circ (b \circ c),\ (a \circ b)c = a(bc),\ a(b \circ c) = ab \circ ac,\ a \circ b = ab \circ a.$$

The first two identities are the normal properties of composition. The second and fourth identities give left distributivity as follows: $a(bc) = (a \circ b)c = (ab \circ a)c = (ab)(ac)$. The third identity gives that left translation is still a homomorphism of the algebra. Examples of algebras satisfying Σ are groups, where $\cdot$ is conjugation and $\circ$ is the group operation, and the algebra of nontrivial elementary embeddings $j : V_\lambda \to V_\lambda$ (see below).

Let $\mathcal{P}$ be the free algebra on one generator satisfying the laws of Σ. Namely let P be the collection of all terms, in the language $\{\cdot, \circ\}$, in one generator x; then $\mathcal{P} = P/\equiv_\Sigma$. $\mathcal{P}$ serves as a type of completion of $\mathcal{A}$, adding $<_L$-least upper bounds which are necessary for the division algorithm. Also, the addition of a composition operation facilitates the expression of connections with the braid groups.

Definition 3. For $p \in \mathcal{P}$, write $p = r_0 r_1 \cdots r_{n-1} * r_n$ to mean that either $p = r_0 r_1 \cdots r_{n-1} r_n$ or $p = r_0 r_1 \cdots r_{n-1} \circ r_n$.

Definition 4. For $p, q \in \mathcal{P}$, $p <_L q$ if and only if there exist $r_1, \ldots, r_n \in \mathcal{P}$ such that $q = p r_1 \cdots r_{n-1} * r_n$.

Lemma 5. *For $p, q, r \in \mathcal{P}$, if $q <_L r$, then $pq <_L p \circ q <_L pr$.*

Proof. We have $pq <_L pq \circ p = p \circ q$ and, for $r = q s_1 s_2 \cdots s_{n-1} * s_n$, $pr = (p \circ q) s_1 (p s_2) \cdots (p s_{n-1}) * (p s_n)$. $\square$

Fact 6. *Every $a \in A$ is uniquely expressible in the form $a_0(a_1(a_2 \cdots (a_n x)))$.*

Lemma 7. *Every $p \in P$ is Σ-equivalent to an expression of the form $a_0 \circ a_1 \circ \cdots \circ a_n$, where each $a_i \in A$ and $n = n_p$ is unique.*

Proof. The equivalence is routine. To see the uniqueness of n_p, let, for $p \in P$, $\#p$ be the number of essential compositions in p: $\#x = 0$, $\#uv = \#v$, $\#(u \circ v) = \#u + \#v + 1$. Then $\#$ is invariant under Σ. $\square$

Note that $\#u = 0$ if and only if u is Σ-equivalent to a term in A.

Theorem 8 (*Laver [12, Lemmas 1–3], Dehornoy [6, Sections VI: 2, 3]*)**.**

(i) *For $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_n \in A$, $a_0 \circ a_1 \circ \cdots \circ a_n \equiv_\Sigma b_0 \circ b_1 \circ \cdots \circ b_n$ if and only if $a_0(a_1(a_2 \cdots (a_n x))) \equiv_{LD} b_0(b_1(b_2 \cdots (b_n x)))$.*

(ii) *Σ is a conservative extension of $\{LD\}$, i.e. for $a, b \in A$, $a \equiv_{LD} b \Leftrightarrow a \equiv_{\Sigma} b$. Thus $\mathcal{A}$ is a subalgebra of $(\mathcal{P}, \cdot)$. Moreover, for $a, b \in A$, $a <_L b$ via the LD law if and only if $a <_L b$ via Σ.*
(iii) *If $a_0 \circ a_1 \circ \cdots \circ a_n = b_0 \circ b_1 \circ \cdots \circ b_n$, each $a_i, b_i \in \mathcal{A}$, then for some $\alpha \in B_{n+1}$, $\langle a_0, a_1, \ldots, a_n\rangle^{\alpha} = \langle b_0, b_1, \ldots, b_n\rangle$.*

Theorem 9 (*Dehornoy [6, Proposition 6.1], Laver [12, Theorem 28]*)**.**

(i) *$\mathcal{P}$ is linearly ordered by $<_L$.*
(ii) *For $p, q \in \mathcal{P}$, $pq = pr \Leftrightarrow q = r$, $pq <_L pr \Leftrightarrow q <_L r$.*

The proofs of Theorem 9(i) in [6,12] have two parts: connectivity ($p \leq_L q$ or $q \leq_L p$) and irreflexivity ($p \not<_L p$). For irreflexivity it suffices to show that there exists an irreflexive LD; Laver [12] showed that the algebra of all nontrivial elementary embeddings $j : V_\lambda \to V_\lambda$, λ of cofinality ω, under the application operation, is irreflexive under $<_L$. (Application of embeddings is defined by: $jk = \bigcup_{\alpha<\lambda} j(k \cap V_\alpha)$. It is seen that jk is itself an elementary embedding and that the operation is left distributive. Some other facts about this algebra are in [14].) Subsequently Dehornoy [5] showed within ZFC that there is an irreflexive left distributive operation defined on B_∞. Larue [10] then found a shorter proof of the irreflexivity of Dehornoy's operation, and since then a number of other proofs of irreflexivity have been found (see [7]).

For connectivity, Dehornoy used the confluence theorem. Laver used the division algorithm. In the remainder of this section we state the division algorithm for pairs $p <_L q$ and its equivalent formulation stating that there is a "p-normal sequence" representing q.

Given $p, q \in \mathcal{P}$ with $p <_L q$, the algorithm proceeds as follows. The first assertion of the theorem is that there is a greatest r_1 such that $pr_1 \leq_L q$. If $pr_1 = q$ or if $p \circ r_1 = q$, the algorithm terminates. Otherwise, there is a greatest r_2 such that $pr_1r_2 \leq_L q$. Theorem 12 asserts that after a finite number of steps this algorithm ends with $pr_1r_2 \cdots r_{n-1} * r_n = q$.

This algorithm cannot be executed in $\mathcal{A}$ as there may be no such greatest r_1. For example, consider the term $w = xx(xxx) \in \mathcal{A}$. Then $w = xx(xx)(xxx) = x(xx)(xxx) = x(xx)(xx)[x(xx)x] = x(xxx)[x(xx)x]$. So $x(xx) <_L w$, $x(xxx) <_L w$, and more generally (from Theorems 11 and 12) there is no $<_L$-largest $a \in \mathcal{A}$ with $xa \leq_L w$. But in $\mathcal{P}$, $a = x \circ x$ works; the division algorithm for the pair $x <_L w$ yields $w = x(x \circ x)x$.

The term $pr_1r_2 \cdots r_{n-1} * r_n$ described in the algorithm satisfies a normality condition, where

Definition 10. The representation of a term $w = p_0p_1 \cdots p_{n-1} * p_n$ in $\mathcal{P}$ is said to be p_0-**normal** with respect to $<_L$ if $p_2 \leq_L p_0, p_3 \leq_L p_0p_1, \ldots, p_i \leq_L p_0p_1 \cdots p_{i-2}$ for all i such that $2 \leq i \leq n$, and if $n \geq 2$ and $* = \circ$, then $p_n <_L p_0p_1 \cdots p_{n-2}$.

Note that $w = xx(x \circ x)x$ is normal if $p_0 = xx$ but not if $p_0 = x$, i.e. w is xx-normal but not x-normal. The strict $<_L$ condition in the last line of Definition 10 is for uniqueness; if $n \geq 2$, $w = p_0p_1p_2 \cdots p_{n-2}p_{n-1} \circ p_n$ and $p_n = p_0p_1p_2 \cdots p_{n-2}$, then $w = p_0p_1p_2 \cdots p_{n-2} \circ p_{n-1}$ and the algorithm already terminated.

p-normal terms can be compared lexicographically as follows.

Theorem 11 (*[13]*)**.** *Let $w = pw_1 \cdots w_n * w_{n+1}$, $u = pu_1 \cdots u_m * u_{m+1}$ be p-normal terms. Then $w <_L u$ if and only if*

(1) *For some i $w_i \neq u_i$; and for the least such i, $w_i <_L u_i$, or*
(2) *For all $i \leq \min\{m+1, n+1\}$, $w_i = u_i$ and $*_w = \cdot$, and either $n < m$ or ($n \geq m$ and $*_u = \circ$).*

Theorem 12 (*Division Algorithm*)**.** *If $p, w \in \mathcal{P}$, $p <_L w$, then there is a (unique) p-normal term $pp_1 \ldots p_{n-1} * p_n$ representing w.*

The original proof of this theorem is due to Laver [12,13] and utilizes results on another normal form. For a direct proof, see [19] or [16].

Definition 13.

(i) DF ("division form") is the set of x-normal terms, $xa_1a_2 \ldots a_{n-1} * a_n$. For $w \in \mathcal{P}$, let $|w|$ be the member of DF that represents w.
(ii) More generally, for $p \in \mathcal{P}$, p-division form is defined as follows. For $w \in \mathcal{P}$, let $|w|^p$ be the p-normal term representing w if $p \leq_L w$, and the x-normal term representing w if $w <_L p$. Then p-DF $= \{|w|^p : w \in \mathcal{P}\}$.

Thus, DF $= x$-DF.

Definition 14. The sequence of iterates of $\langle a, b\rangle$ is

$$a, ab, aba, aba(ab), aba(ab)(aba), \ldots,$$

i.e., $I_1 = a$, $I_2 = ab$, $I_{n+2} = I_{n+1}I_n$.

The iterates of $\langle a, b\rangle$ are a-normal, each $I_n <_L I_{n+1}$, each $I_{n+1} \circ I_n = a \circ b$, and it is a consequence of Theorems 9, 11 and 12 that $a \circ b$ is the $<_L$-least upper bound of the set of I_n's.

For completeness we mention another consequence of the way Theorem 12 was proved (which won't be used in the sequel). Part (i) of Theorem 15 says that every $p \in \mathcal{P}$ can be put into hereditary division form, and (ii) gives a related well-founded partial ordering on $\mathcal{P}$ which has been useful in inductive proofs about $\mathcal{P}$.

Theorem 15.

(i) *For every p in $\mathcal{P}$ there is a (unique) term w in P representing p such that every subterm of w is x-normal.*
(ii) *Let R be the binary relation on $\mathcal{P}$ given by the following rules; if $|w| = xa_1a_2 \cdots a_{n-1} * a_n$ then $xa_1a_2 \cdots a_{n-1}Rw$, a_nRw, and if $* = \circ$, each iterate $I_k(xa_1a_2 \cdots a_{n-1}, a_n)Rw$. Then the transitivization of R is a well-founded partial ordering of $\mathcal{P}$.*

Similar results hold for p-division form.

3. Left divisors

A stronger condition than $p <_L q$ is that p is a left divisor of q. In this section, after some basics about left division, we state a conjecture about well-orderings in the braid groups and derive from the division algorithm that if p left divides a composition it left divides all the composands.

Definition 16.

(i) For $p, q \in \mathcal{P}$, $p \mid q \Leftrightarrow \exists r(pr = q)$.
(ii) For $q \in \mathcal{P}$, $D_q = \{p \in \mathcal{P} : p \mid q\}$.

Let $E_q = \{p \in \mathcal{P} : p <_L q\}$. Then E_q is linearly ordered by $<_L$ since $\mathcal{P}$ is, but E_q need not be well-ordered by $<_L$. For example suppose q is of the form $r(st)$. We have $r(st) = (r \circ s)t$, and $r \circ s = rs \circ r = rsr \circ rs = rsr(rs) \circ rsr$. Thus $rsr(rs) <_L r \circ s <_L r(st)$, and $rsr(rs)$ is of the form $R(ST)$. Continuing in this manner, an infinite descending sequence from E_q is obtained.

The question of whether every D_q $(q \in \mathcal{P})$ is well-ordered under $<_L$ reduces to the version given in the introduction: for any $a \in \mathcal{A}$, $D_a \cap \mathcal{A}$ is well-ordered (see Theorem 26 below).

Given $a \in \mathcal{A}$, if D_a is not well-ordered, then by Theorems 12, 24 and 26, there is an infinite descending sequence constructed in a natural way, namely $a = b_0c_0 = b_1c_1 = b_2c_2 = \cdots$, where $b_{i+1}c_{i+1} = b_{i+1}(u_{i+1}v_{i+1})$, and $b_i = b_{i+1}u_{i+1}$, $c_i = b_{i+1}v_{i+1}$.

The well-ordering of the D_q's is a consequence of the following conjecture:

If $a_i \in \mathcal{A}$ $(i < n)$ then $\{\alpha \in B_n : \langle a_0, a_1, \dots a_{n-1}\rangle^\alpha \text{ exists}\}$ is well-ordered under the Dehornoy ordering.

See [15,11,2,8] for results on this problem.

Lemma 17. *If $p, w \in \mathcal{P}$, $p \mid w$ then $|w|^p = pv$ for some v.*

Lemma 18. *Let $p, s, t \in \mathcal{P}$.*

(i) *If $p \mid s$ and $p \mid t$, then $p \mid st$.*
(ii) *If $p \mid s$ and $p \mid st$, then $p \mid t$.*

Proof. (i) Trivial.
(ii) Given $s = pr$, $st = pu$. Suppose $p \nmid t$.
Case 1: $t \leq_L p$. Then $st = prt$ is p-normal. This implies $p \nmid st$ by Lemma 17. Contradiction.
Case 2: $t >_L p$. Then, since $p \nmid t$, $|t|^p = pt_1 \cdots t_{k-1} * t_k$ where either $k \geq 2$ or $k = 1$ and $* = \circ$.
Case 2.1: $|t|^p = pt_1 \cdots t_{k-1}t_k$, $k \geq 2$.

$$\begin{aligned} st &= pr(pt_1 \cdots t_{k-1}t_k) \\ &= pr(pt_1t_2)(prt_3) \cdots (prt_k) \\ &= (pr \circ pt_1)t_2(prt_3) \cdots (prt_k) \\ &= p(r \circ t_1)t_2(prt_3) \cdots (prt_k). \end{aligned}$$

This term is p-normal, thus is $|st|^p$. This implies that $p \nmid st$ by Lemma 17. Contradiction.
Case 2.2: $|t|^p = pt_1 \cdots t_{k-1} \circ t_k$. For $k \geq 2$, the argument is the same as in Case 2.1. Consider then the case $k = 1$.

$$\begin{aligned} st &= pr(p \circ t_1) \\ &= pr(pt_1p \circ pt_1) \\ &= pr(pt_1p) \circ pr(pt_1) \\ &= (pr \circ pt_1)p \circ p(rt_1) \\ &= p(r \circ t_1)p \circ p(rt_1). \end{aligned}$$

The final term is p-normal, thus is $|st|^p$. By Lemma 17 we have $p \nmid st$, a contradiction. $\square$

The analogous lemma for composition has a stronger conclusion.

Lemma 19. *Given $p, r_0, \dots, r_n \in \mathcal{P}$, if $p \mid r_0 \circ r_1 \circ \cdots \circ r_n$ then $p \mid r_i$ for all i.*

Proof. Each $r \in \mathcal{P}$ is a composition of members of $\mathcal{A}$, so we may assume each $r_i \in \mathcal{A}$. Since, by Lemma 7, the number of composands from $\mathcal{A}$ making up $r \in \mathcal{P}$ is an invariant, there exist $a_0, a_1, \dots, a_n \in \mathcal{A}$ such that $r_0 \circ r_1 \circ \cdots \circ r_n = p(a_0 \circ \cdots \circ a_n) = pa_0 \circ \cdots \circ pa_n$.

Then by Theorem 8 $\langle pa_0, pa_1, \dots, pa_n\rangle^\alpha = \langle r_0, r_1, \dots, r_n\rangle$ for some $\alpha \in B_{n+1}$. By Lemma 18 we have $p \mid u$ and $p \mid v$ if and only if $p \mid uv$ and $p \mid u$. Therefore p divides each member of $\langle u_0, u_1, \dots, u_n\rangle$ if and only if p divides every member of $\langle u_0, u_1, \dots, u_n\rangle^{\pm\sigma_i}$. Thus p divides every member of $\langle pa_0, pa_1, \dots pa_n\rangle^\alpha$, giving the lemma. $\square$

4. Proofs of the main theorems

In this section the division algorithm is used to get lower bounds on the length of some normal sequences, from which we derive that if $a, b, c, d \in \mathcal{A}$, $ab = cd$, and $a <_L c$, then $\langle a, b\rangle$ can be transformed to $\langle c, d\rangle$ by a sequence of forward applications of the LD law.

Definition 20. If $w = p_0p_1 \cdots p_{n-1} * p_n$ is p_0-normal, define length$(w) = n + 1$.

For $w, z, v \in \mathcal{P}$, the length of $|w|^z$ can be greater than the length of $|w|^{zv}$. The next theorem gives, under certain conditions, a bound below which the length cannot collapse in passage from z-DF to zv-DF.

Theorem 21. *Suppose $|w|^z = zs_1s_2 \cdots s_{m-1} * s_m$, $v <_L s_1$, $|s_1|^v = vt_1 \cdots t_{n-1} * t_n$ (with $n > 1$ if $*_{s_1} = \circ$; i.e., $s_1 \neq v \circ t_1$). Then $|w|^{zv}$ begins with*

$$(zv)(zt_1) \cdots (zt_{n-1})$$

and if $*_{s_1} = \cdot$, $|w|^{zv}$ begins with

$$(zv)(zt_1) \cdots (zt_{n-1})(zt_n).$$

Proof. $w = [zv(zt_1) \cdots (zt_{n-1}) * (zt_n)]s_2 \cdots s_{m-1} * s_m$, where the expression in brackets is zv-normal. We have that $n \geq 1$, since $v <_L s_1$.

Case 1: $*_{s_1} = \cdot$. Then $w = zv(zt_1) \cdots (zt_{n-1})(zt_n)s_2 \cdots s_{m-1} * s_m$ is zv-normal and satisfies the conclusion.

Case 2: $*_{s_1} = \circ$. So $w = [zv(zt_1) \cdots (zt_{n-1}) \circ (zt_n)]s_2 \cdots s_{m-1} * s_m$.

We have:

(i) $(zv)(zt_1) \cdots (zt_{n-1})$

is zv-normal and $<_L w$.

We find a zv-normal term beginning with (i) which is an upper bound for w. Since $|w|^z = zs_1s_2 \cdots s_{m-1} * s_m$ is z-normal, by Theorem 11 we have $w \leq_L z \circ s_1$. Computing $|z \circ s_1|^{zv}$, we have $z \circ s_1 = zs_1 \circ z = ((zv)(zt_1) \cdots (zt_{n-1}) \circ (zt_n)) \circ z$, which is equal to

(ii) $(zv)(zt_1) \cdots (zt_{n-1}) \circ ((zt_n) \circ z)$,

which we claim is zv-normal. We are to show that $zt_n \circ z <_L (zv)(zt_1) \cdots (zt_{n-2})$ (recall $n > 1$). Given $t_n <_L vt_1 \cdots t_{n-2}$, then $vt_1 \cdots t_{n-2} = t_nc_1c_2 \cdots c_{k-1} * c_k$. Then $z(vt_1 \cdots t_{n-2}) = (zt_n)(zc_1) \cdots >_L zt_n \circ z$. Thus (ii) is zv-normal.

So (i) and (ii) are zv-normal terms with (i) an initial segment of (ii), such that (i) $<_L w \leq_L$ (ii). Thus by Theorem 11, $|w|^{zv}$ begins with (i).

This proves the theorem. □

Theorem 22. *Suppose $p \in \mathcal{P}$, $a, b \in \mathcal{A}$, and suppose that $pa = (pu_1u_2 \cdots u_n)b$, where $pu_1u_2 \cdots u_n$ is p-normal. Then $u_1 \mid a$.*

Proof. Suppose $u_1 \nmid a$. We claim that $|pa|^{pu_1 \cdots u_i}$ has length greater than or equal to three for all $i \leq n$. This will be a contradiction, since length$(|pa|^{pu_1 \cdots u_n}) = 2$. The cases $i = 1, 2$ are first checked separately.

We have $u_1 <_L a$ since $pu_1 \cdots u_n <_L pa$ and both are p-normal. Thus $|a|^{u_1} = u_1a_2 \cdots a_{k-1}a_k$, since $a \in \mathcal{A}$. Also $k \geq 3$, namely $a \neq u_1$ since $u_1 <_L a$, and $a \neq u_1u_2$ since $u_1 \nmid a$.

Thus $|pa|^{pu_1} = pu_1(pa_2) \cdots (pa_k)$ has length greater than or equal to 3.

To compute $|pa|^{pu_1u_2}$: by normality of $pu_1 \cdots u_n$ we know that $u_2 \leq_L p$.

Therefore $u_2 <_L pa_2$ which implies that $|pa_2|^{u_2} = u_2t_2 \cdots t_{m-1} * t_m$, so

$$\begin{aligned} pa &= pu_1(u_2t_1 \cdots t_{m-1} * t_m)(pa_3) \cdots (pa_k) \\ &= [pu_1u_2(pu_1t_1) \cdots (pu_1t_{m-1}) * (pu_1t_m)](pa_3) \cdots (pa_k) \end{aligned}$$

where the expression in brackets is pu_1u_2-normal.

We claim that the expression in brackets is not $pu_1u_2 \circ pu_1t_1$. Otherwise $pa_2 = u_2 \circ t_1$. By Lemma 19 we would have $p \mid u_2$, but $u_2 \leq_L p$, a contradiction. Thus Theorem 21 (with $w = pa$, $z = pu_1$, $v = u_2$) gives that $|pa|^{pu_1u_2}$ begins with $(pu_1u_2)(pu_1t_1)$ and, since $k \geq 3$, is $<_L$-larger than $(pu_1u_2)(pu_1t_1)$. So length$(|pa|^{pu_1u_2}) \geq 3$.

Suppose now inductively that $2 \leq i < n$ and

$$|pa|^{pu_1u_2 \cdots u_i} = (pu_1 \cdots u_i)(pu_1 \cdots u_{i-1}s)c_3 \cdots c_l$$

for some $l \geq 3$ and some s. We have $u_{i+1} \leq_L pu_1 \cdots u_{i-1}$, so $u_{i+1} <_L pu_1 \cdots u_{i-1}s$. So

$$pa = pu_1 \cdots u_i(u_{i+1}t_1 \cdots t_{m-1} * t_m)c_3 \cdots c_l.$$

We claim the expression in parentheses is not $u_{i+1} \circ t_1$. For if $pu_1 \cdots u_{i-1}s = u_{i+1} \circ t_1$, then $pu_1 \cdots u_{i-1} \mid u_{i+1}$ by Lemma 19, but $u_{i+1} \leq_L pu_1 \cdots u_{i-1}$, a contradiction.

Thus, as in the case $i = 2$, Theorem 21 applies. Unlike the case computing $|pa|^{pu_1u_2}$ from $|pa|^{pu_1}$, here $pu_1 \cdots u_{i-1}s$ might equal $u_{i+1}t_1$; but also unlike that case there is at least one c_j at the end of $|pa|^{pu_1\cdots u_i}$, so the application of Theorem 21 yields $|pa|^{pu_1\cdots u_{i+1}} = (pu_1 \cdots u_iu_{i+1})(pu_1 \cdots u_it_1)d_3 \cdots d_l$ for some $l \geq 3$. □

Definition 23. For $p, r \in \mathscr{P}$, a forward application of the LD law on $\langle p, r\rangle$ is a transformation $\langle p, r\rangle \rightarrowtail^* \langle pr_1, pr_2\rangle$, where $r = r_1r_2$. Define $\langle p, r\rangle \rightarrowtail \langle u, v\rangle$ if and only if there exists a chain $\langle p, r\rangle \rightarrowtail^* \langle p_0, r_0\rangle \rightarrowtail^* \ldots \rightarrowtail^* \langle p_n, r_n\rangle \rightarrowtail^* \langle u, v\rangle$. So if $\langle p, r\rangle \rightarrowtail \langle u, v\rangle$ then $pr = uv$.

Theorem 24. *If $a, b, c, d \in \mathscr{A}$, $ab = cd$ and $a <_L c$, then $\langle a, b\rangle \rightarrowtail \langle c, d\rangle$.*

Proof. As $a <_L c$ and $c \in \mathscr{A}$, $|c|^a$ is of the form $ac_1c_2 \cdots c_{n-1}c_n$.

By Theorem 22, we have $c_1 \mid b$, so $b = c_1b_1$. This gives

$$ab = a(c_1b_1) = ac_1(ab_1) = cd = ac_1 \cdots c_nd.$$

As $ac_1 \cdots c_n$ is a-normal it is also $ac_1 \cdots c_i$-normal for all i, $1 \leq i \leq n$. Letting $i = 1$ Theorem 22 yields that $c_2 \mid ab_1$, so $ab_1 = c_2b_2$. By repeating this process we get:

$$\begin{aligned} ab &= ac_1(ab_1) \\ &= ac_1(c_2b_2) \\ &= ac_1c_2(ac_1b_2) \\ &= ac_1c_2(c_3b_3) \\ &= \vdots \\ &= ac_1c_2 \cdots c_{n-1}c_n(ac_1c_2 \cdots c_{n-1}b_n), \end{aligned}$$

where $ac_1c_2 \cdots c_{n-1}c_n = c$ and (by left cancellation) $ac_1c_2 \cdots c_{n-1}b_n = d$. □

The conjecture of Moody for $\mathscr{A}$ follows.

Theorem 25. *Given $a, b, c, d \in \mathscr{A}$, $ab = cd$, $D_a \cap D_b \cap \mathscr{A} = \emptyset = D_c \cap D_d \cap \mathscr{A}$, then $a = c$ and $b = d$.*

Proof. If $a = c$, then by left cancellation $b = d$. Thus assume for a contradiction that $a \neq c$. Without loss of generality, $a <_L c$.

By Theorem 24, $\langle a, b\rangle \rightarrowtail \langle c, d\rangle$. Thus there exist some u, v in the penultimate step such that $\langle u, v\rangle \rightarrowtail^* \langle c, d\rangle$. So $u \mid c$ and $u \mid d$. Either $u \in \mathscr{A}$ or $u = e \circ q$ with $e \in \mathscr{A}$, and thus $e \mid c$ and $e \mid d$. In either case $D_c \cap D_d \cap \mathscr{A} \neq \emptyset$, a contradiction. □

5. Concluding remarks

Let $\mathscr{A}_\kappa$ (respectively $\mathscr{P}_\kappa$) be the free left distributive algebra (respectively the free algebra satisfying Σ) on κ generators. We have that $\mathscr{P}_\kappa$ ($\kappa > 1$) is not linearly ordered by $<_L$ since the generators are not ordered. More generally, say that u and v have a *variable clash*($u \nsim v$) if and only if there exists some (possibly empty) $w \in \mathscr{P}_\kappa$ such that for distinct generators, x and y, $wx \leq_L u$ and $wy \leq_L v$. Then members of $\mathscr{P}_\kappa$ with a variable clash are not ordered; in place of the linear ordering we have (see [4,5,15]) quadrichotomy: for $u, v \in \mathscr{P}_\kappa$, exactly one of $u <_L v$, $v <_L u$, $u = v$ and $u \nsim v$ holds.

The well ordering question for $\mathscr{P}_\kappa$ reduces to the one for $\mathscr{A}$.

Theorem 26. *If for all $a \in \mathscr{A}$, $D_a \cap \mathscr{A}$ is well ordered under $<_L$, then for all $p \in \mathscr{P}_\kappa$, D_p is well ordered under $<_L$.*

Proof. We claim that, for $a \in \mathscr{A}$, if $D_a \cap \mathscr{A}$ is well ordered then D_a is well ordered. It suffices for the claim to show that if $p, q \in \mathscr{P}$ are members of D_a with $p <_L q$ then there's a b in $D_a \cap \mathscr{A}$ with $p \leq_L b \leq_L q$. If $q \notin \mathscr{A}$, write $q = r \circ s$ where $r \in \mathscr{P}$ and $s \in \mathscr{A}$. Then the even iterates $I_{2n}\langle r, s\rangle$ are in $\mathscr{A}$ and their least upper bound is $r \circ s = q$. Pick an n such that $b = I_{2n}\langle r, s\rangle$ is greater than p. Then $a = qc = (r \circ s)c = I_{2n}(I_{2n-1}c) = b(I_{2n-1}c)$. So $b \in D_a \cap \mathscr{A}$ and $p <_L b <_L q$.

Next we claim that if, for all $a \in \mathscr{A}$, $D_a \cap \mathscr{A}$ is well ordered then for all $p \in \mathscr{P}$, D_p is well ordered. Given $p \in \mathscr{P} \setminus \mathscr{A}$, write $p = c \circ s$ with $c \in \mathscr{A}$. By Lemma 19, $D_p \subseteq D_c$. D_c is well ordered by the assumption of the theorem and the first claim. Thus D_p is well ordered.

To prove the theorem, let $p \in \mathscr{P}_\kappa$. Thus D_p is linearly ordered by $<_L$ (if not, by quadrichotomy we would have $p = qr = q'r'$ where $q \nsim q'$. But then $p \nsim p$, contradicting quadrichotomy.). Thus if D_p weren't well ordered there would be a $<_L$-descending sequence $w_0, w_1, \ldots, w_n, \ldots$ of members of D_p. Let H be the homomorphism from $\mathscr{P}_\kappa$ to $\mathscr{P}$ obtained by sending each generator to x. Then $H(w_0), H(w_1), \ldots, H(w_n), \ldots$ is a $<_L$-descending sequence of members of $D_{H(p)}$. This contradicts the assumption of the theorem and the second claim. □

What about an analogue for $\mathscr{P}_\kappa$ of the division algorithm? Let $u \lhd v$ denote that either $u <_L v$ or $u \nsim v$. We can generalize the idea of normal terms to $\mathscr{P}_\kappa$ by permitting in the definition of normal sequence the condition $a_i \unlhd a_0a_1 \cdots a_{i-2}$ in place of $a_i \leq_L a_0a_1 \cdots a_{i-2}$. We have that a term in P_κ can have at most one normal representation with respect to its leftmost generator [19]. It is not known whether there always is such a representation. In the one generator case, two normal terms can be compared lexicographically to determine their relation under $<_L$. In P_κ, however, for a generator, y, there are two y-normal terms between which lexicographic comparison fails.

The conjectured division algorithm above is examined in [19] and shown, in a more complicated way, to prove the conjecture of J. Moody for many generators. See [17–19] for results on these and related topics for many generators.

References

[1] E. Brieskorn, Automorphic sets and braids and singularities, in: Braids, in: Contemporary Math., vol. 78, American Math. Soc., 1988.
[2] S. Burckel, The well-ordering on positive braids, Journal of Pure and Applied Algebra 120 (1997) 1–17.
[3] P. Dehornoy, Sur la structure des gerbes libres, Comptes-rendu Acad Sci Paris (1989) 143–148.
[4] P. Dehornoy, The adjoint representation of left-distributive structures, Communications in Algebra 20-4 (1992) 1201–1215.
[5] P. Dehornoy, Braid groups and left-distributive structures, Transactions of the American Mathematical Society 345 (1994) 115–150.
[6] P. Dehornoy, Braids and Self-Distributivity, in: Progress in Mathematics, vol. 192, Birkhäuser, 2000.
[7] P. Dehornoy, I. Dynnikov, D. Rolfsen, B. Wiest, Why are Braids Orderable? in: Panoramas et Syntheses, vol. 14, Soc. Math Francais, 2002.
[8] J. Fromentin, A well-ordering of dual braid monoids, Comptes Rendus Mathematics 346 (2008) 729–734.
[9] D. Joyce, A classifying invariant of knots: the knot quandle, Journal of Pure and Applied Algebra 23 (1982) 37–65.
[10] D. Larue, Braid words and irreflexivity, Algebra Universalis 31 (1994) 104–112.
[11] D. Larue, Left distributive algebras and left distributive idempotent algebras, Ph.D. thesis, University of Colorado, 1994.
[12] R. Laver, The left-distributive law and the freeness of an elgebra of elementary embeddings, Advances in Mathematics 91 (1992) 209–231.
[13] R. Laver, A division algorithm for the free left distributive algebra, in: Lecture Notes in Logic 2, Logic Colloquim'90, Springer-Verlag, 1993.
[14] R. Laver, On the algebra of elementary embeddings of a rank into itself, Advances in Mathematics 110 (1995) 334–346.
[15] R. Laver, Braid group actions on left distributive structures and well-orderings in the braid groups, Journal of Pure and Applied Algebra 108 (1996) 81–98.
[16] R. Laver, S. Miller, Left distributive algebras and the division algorithm (submitted for publication).
[17] R. Laver, J. Moody, Well-foundedness conditions connected with left-distributivity, Algebra Univsersalis 27 (2002) 65–68.
[18] S. Miller, Free left distributive algebras on κ generators (in preparation).
[19] S. Miller, Free left distributive algebras, Ph.D. Thesis, University of Colorado, Boulder, 2007.