Algebra univers. **47** (2002) 65–68
0002-5240/02/010065 – 04 $1.50 + 0.20/0

Algebra Universalis

Well-foundedness conditions connected with left-distributivity

Richard Laver and John A. Moody

Abstract. We state a problem about free left-distributive algebras. If u and w are members of such an algebra write $u <_L w$ if $w = (((uu_0)u_1)...)u_n$ for some $u_0, \cdots, u_n$. A conjecture about left-division in such algebras is given; it entails a normal form and that for every w the set of left divisors of w is well-ordered under $<_L$.

Let $\mathcal{A}_k$ be the free left-distributive algebra on k-many generators, where k is a cardinal and the left-distributive law is the law $a(bc) = (ab)(ac)$. The purpose of this paper is the describe a conjecture connected with left division in $\mathcal{A}_k$, and some propositions related to it. This problem is one of a number of well-foundedness questions about free left-distributive algebras. Here are some basic facts (see [4] and [8], section 2 for respectively an account and a summary).

Fix a set S of cardinality k and let T be the set of S-terms in the language of one binary operation. For $\tau_0, \tau_1 \in T$, τ_1 is the result of a forward transformation on τ_0 if and only if τ_1 can be obtained from τ_0 by replacing a subterm of the form $a(bc)$ by $(ab)(ac)$. Then $\mathcal{A}_k = T/\equiv$, where $\tau \equiv \sigma$ iff σ can be obtained from τ by a sequence of forward transformations and/or their inverses. Write $[\tau]$ for the equivalence class of τ. Let $\tau_0 \to \tau_1$ mean that τ_1 is obtainable from τ_0 by a sequence of forward transformations. Then $\mathcal{A}_k$ is confluent [1], that is, if $\tau_0 \equiv \tau_1$ then there's a τ such that $\tau_0 \to \tau$ and $\tau_1 \to \tau$. For $a, b \in \mathcal{A}_k$, write $a \mid b$ iff for some c, $ac = b$. Write $a <_L b$ if a is an iterated left divisor of b; $b = ((aa_0)a_1)\ldots)a_n$ for some $n \geq 0$. Then $<_L$ is a partial ordering: transitivity is immediate, and irreflexivity ($a \not<_L a$), first shown in [6] as a corollary to a large cardinal axiom of set theory, was then shown in [3] without it—see [5] for a shorter proof of irreflexivity. And on $\mathcal{A} = \mathcal{A}_1$, $<_L$ is a linear ordering (modulo irreflexivity this was shown in different ways in [3] and [6]). On $\mathcal{A}_k$ ($k > 1$), $<_L$ is not linear, but any linear ordering of S naturally induces a linear ordering of $\mathcal{A}_k$ which extends $<_L$ [2]. Finally, $\mathcal{A}_k$ satisfies left cancellation. For $k = 1$ this follows from the linearity of $<_L$ and the fact that

Presented by R. W. Quackenbush.
Received March 25, 2001; accepted in final form April 10, 2001.
2000 *Mathematics Subject Classification*: 20F36, 20N02.
Key words and phrases: Left-distributivity, braid groups.
The work of the first author was supported by NSF Grant DMS 9972257.

$<_L$ is preserved under left translations, and for $k > 1$ it is derivable from the $k = 1$ case and confluence.

Example The linear order $<_L$ on $\mathcal{A}$ is not a well-order. Let w be any member of $\mathcal{A}$ of the form $r(st)$. Then

$$w = [((rs)r))(rs)][((rs)r)t]$$

and we have

$$((rs)r)(rs) <_L w.$$

The left hand side is of the same form, yielding an infinite descending sequence under $<_L$.

Definitions.

(1) For $w \in \mathcal{A}_k$, $D_w = \{u \in \mathcal{A}_k : u \mid w\}$.

(2) For $\langle a, b\rangle$, $\langle c, d\rangle \in \mathcal{A}_k \times \mathcal{A}_k$, $\langle c, d\rangle$ is an *LD-transformation* of $\langle a, b\rangle$ (and $\langle a, b\rangle$ is an *LD-inverse* of $\langle c, d\rangle$) if and only if for some r and s, $b = rs$, $c = ar$, and $d = as$ (so $ab = cd$).

(3) A $\tau \in T$ is in *reduced normal form* just in case for every subterm $\sigma\gamma$ of τ, $D_{[\sigma]} \cap D_{[\gamma]} = \emptyset$.

In (2), $\langle u, v\rangle$ may have more than one LD transformation and LD inverse. These operations are more general than the forward transformations and their inverses at the term level: for example $\langle ab, (ac)d\rangle$ is an LD inverse of $\langle a(bc), (ab)d\rangle$, but the term $(\alpha\beta)((\alpha\gamma)\delta)$ is not obtainable from $(\alpha(\beta\gamma))((\alpha\beta)\delta)$ by the inverse of a forward transformation.

Conjecture.

(i) If $u, v, r, s \in \mathcal{A}_k$, $uv = rs$, $u \neq r$, then for one of u and r (say, u) there is a finite iteration of LD-transformations which takes $\langle u, v\rangle$ to $\langle r, s\rangle$.

(ii) If $\langle r, s\rangle \in \mathcal{A}_k \times \mathcal{A}_k$ then any sequence $\langle r_0, s_0\rangle, \ldots, \langle r_i, s_i\rangle, \ldots$ with $\langle r_0, s_0\rangle = \langle r, s\rangle$, such that each $\langle r_{n+1}, s_{n+1}\rangle$ an LD-inverse of $\langle r_n, s_n\rangle$, is finite.

(iii) If $w \in \mathcal{A}_k$ there is a unique term τ in reduced normal form with $[\tau] = w$.

Theorems on the existence of other normal forms have been proved in [6,7] and in [4].

Proposition 1. (a) *Conjecture* (i) *implies that for each $w \in \mathcal{A}_k$, D_w is linearly ordered by $<_L$.*

(b) *If Conjectures* (i) *and* (ii) *hold then for each $w \in \mathcal{A}_k$, D_w is well ordered by $<_L$.*

Proof. (a) Irreflexivity and transitivity follow from those properties of $\mathcal{A}_k$. And if $uv = rs = w$ with $u \neq r$, there is by (i) a sequence of LD-transformations taking, say, $\langle u, v\rangle$ to $\langle r, s\rangle$, which would witness $u <_L r$.

(b) Suppose there is an infinite sequence $u_0 >_L u_1 > \cdots >_L u_n >_L \cdots$ of members of D_w. Writing $u_n v_n = w$, there is by (i) a sequence of LD-inverse operations which take $\langle u_n, v_n\rangle$ to $\langle u_{n+1}, v_{n+1}\rangle$, for each n. This infinite iteration of LD-inverses contradicts (ii). □

We briefly consider some other hypotheses about $\mathcal{A}_k$ and their connections with one another. Some statements are explicitly mentioned because they have a plausibility argument, namely they have been proved to be true in $\mathcal{A}$ (see remarks at the end).

Proposition 2. *Suppose the following condition holds:*

(∗) *For all $a, b, c \in \mathcal{A}_k$, if $a \mid b$ and $a \mid bc$ then $a \mid c$.*

Then, for any $\langle u, v\rangle, \langle r, s\rangle \in \mathcal{A}_k \times \mathcal{A}_k$ there is a finite sequence of LD transformations which takes $\langle u, v\rangle$ to $\langle r, s\rangle$ if and only if $uv = rs$ and there is a sequence $u_i (0 \le i \le n)$, with $u_0 = u$, $u_i \mid u_{i+1} (i < n)$, and $u_n = r$, such that each $u_i \mid rs$.

Proof. For the right to left direction, write $rs = u_i t_i$, $u_{i+1} = u_i q_i$. Since $u_i \mid u_{i+1}$ and $u_i \mid u_{i+1} t_{i+1}$, $u_i s_i = t_{i+1}$ for some s_i, by (∗). Then $\langle u_{i+1}, t_{i+1}\rangle = \langle u_i s_i, u_i q_i\rangle$ has an LD-inverse $\langle u_i, q_i s_i\rangle$, and $q_i s_i = t_i$ by left cancellation. Also by left cancellataion $t_0 = v$ and $t_n = s$. This gives a sequence of LD inverses taking $\langle r, s\rangle$ to $\langle u, v\rangle$. □

Proposition 3. *Conjecture* (i) *implies that the reduced normal form of a $w \in \mathcal{A}_k$ is unique if it exists.*

Lemma 1. *Assume* (i). *Then if $u, v, r, s \in \mathcal{A}_k$, $uv = rs$, and $D_u \cap D_v = D_r \cap D_s = \emptyset$, then $u = r$ and $v = s$.*

Proof. Let $w = uv = rs$. It suffices by left cancellation to show $u = r$. Suppose $u \ne r$. Then by (i), for one of u and r, say r, we have that $\langle r, s\rangle$ is in the range of an LD-transformation. Thus $D_r \cap D_s \ne \emptyset$, a contradiction. □

To show uniqueness of reduced normal forms, we show by induction on length τ ($\tau \in T$), that if $\tau \equiv \sigma$ and τ, σ are in reduced normal form, then $\tau = \sigma$. We are done if either $[\tau]$ or $[\sigma]$ is a generator, so assume $\tau = \tau_0\tau_1$, $\sigma = \sigma_0\sigma_1$. By the normal form, $D_{[\tau_0]} \cap D_{[\tau_1]} = D_{[\sigma_0]} \cap D_{[\sigma_1]} = \emptyset$. By the lemma then, $[\tau_0] = [\sigma_0]$ and $[\tau_1] = [\sigma_1]$. Since τ_0, τ_1 have smaller length than τ and the τ_i's and σ_i's are in reduced normal form, $\tau_i = \sigma_i$ holds by induction. Thus $\tau = \sigma$, proving Proposition 3.

Assuming the conjecture, part (iii) is expressible as follows. For every $w \in \mathcal{A}_k$, let T_w be the $\mathcal{A}_k$-labelled tree, with root node labelled by w, such that nodes which are labelled by generators are terminal, and every node labelled by a nongenerator v has two immediate successors which are labelled by the elements r and s such that $rs = v$ and r is the $<_L$-least member of D_v. Then for each w, T_w is finite.

A number of the above statements are known in the one-generator case (results of the first author). Namely, if $w \in \mathcal{A}$, then Conjecture (i) is true for w. It follows that the conclusion of Lemma 1 is true for $\mathcal{A}$, and that the reduced normal form of a member of $\mathcal{A}$ is unique if it exists. Also, $(*)$ is true for $\mathcal{A}$. Conjectures (ii) and (iii) are open for $\mathcal{A}$.

A number of theorems about free left distributive algebras have related versions about the braid groups, and vice-versa (see [3] and [4], also see [8], Section 3 for facts about braids which are related to the question of well ordering of D_w under $<_L$).

References

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

[2] P. Dehornoy, *A canonical ordering for free LD systems*, Proc. Amer. Math Soc. **122** (1994), 31–37.

[3] P. Dehornoy, *Braid groups and left distributive operations*, Trans. Amer. Math Soc. **345** (1994), 115–151.

[4] P. Dehornoy, *Braids and self-distributivity*, Progress in Mathematics 192, Birkhauser, 2000.

[5] D. Larue, *On braid words and irreflexivity*, Algebra Universalis **31** (1994), 104–112.

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

[7] R. Laver, *A division algorithm for the free left-distributive algebra*, Oikkonen et al., eds., Logic Colloquium '90, Springer-Verlag Lecture Notes in Logic 2, 1993, pp. 155–162.

[8] R. Laver, *Braid group actions on left-distributive structures and well-orderings in the braid groups*, Jour. Pure and Applied Algebra **108** (1996), 81–98.

Richard Laver
University of Colorado, Boulder, Colorado

John A. Moody
University of Warwick, Warwick, UK