An open problem involving finite algebras, braid groups, and large cardinals

Sheila Miller

Department of Mathematical Sciences
United States Military Academy

Abstract

A left distributive algebra is a set, L, with one binary operation, $*$, satisfying the left distributive law: $a*(b*c) = (a*b)*(a*c)$. In this talk we discuss an open problem about the Laver tables, which are particular finite left distributive algebras with one generator. Left distributive algebras have connections to other areas of mathematics that range from braid groups and knot theory to set theory. We outline the problem and its importance.

Definition

A left distributive algebra (LD) is a set, L, with one binary left distributive operation, $*$ such that:

$$a * (b * c) = (a * b) * (a * c).$$

When the operation is clear, we write $a(bc)$ for $a * (b * c)$, and we adopt convention that

$$((((a_0 a_1)a_2) \cdots a_{n-1})a_n) = a_0 a_1 a_2 \cdots a_{n-1} a_n.$$

Definition

$a <_L b$ if and only if $\exists c_1, \ldots, c_n$ such that $b = ac_1 \cdots c_n$

Examples

Examples of left distributive operations from classical math are:

- Group conjugation: $a * b = a \circ b \circ a^{-1}$, where $\circ$ is the group operation.
- The weighted mean: if $p \in [0, 1]$, $r * s = pr + (1 - p)s$.

In both cases, left multiplication is a homomorphism of the algebra. Furthermore, (whenever $p \neq 1$ in the second example), $*$ is idempotent.

Namely, $a * a = a$ for each a in L.

Is there a (natural) example of an LD in which neither idempotence nor any other non-trivial relation holds?

I.e., let A be the set of all terms in one generator, x, and on binary left distributive operation $\cdot$ and define the free left distributive algebra $\mathcal{A}$ to be:

$$\mathcal{A} \cong A/\equiv_{LD}$$

Are there any natural examples of free LDs?

Example 1: Elementary Embeddings

- If j is an elementary embedding from M into N, then every sentence (without free variables) that is true in M is true in N as well, and conversely. In particular, if $\overrightarrow{a}$ is in the domain of M, then for every formula Φ, $\Phi(\overrightarrow{a})$ holds in M if and only if $\Phi(j(\overrightarrow{a}))$ holds in N.
- In general, we get stronger large cardinal axioms when we require more closure in the target model (N). Kunen's theorem says that there is no elementary embedding from the universe of set theory, V, into itself.
- Suppose there exists a nontrivial elementary embedding $j : V_\lambda \to V_\lambda$ (called a rank to rank or Laver embedding). The existence of such embeddings cannot be proven from ZFC. In fact the existence of such embeddings is a very strong large cardinal axiom.

Definition

For j and k elementary embeddings from V_λ into itself ($j, k \in \mathcal{E}_\lambda$), define the application operation:

$$j \cdot k = jk = \bigcup_{\alpha<\lambda} j(k \cap V_\alpha)$$

Theorem

1. *jk is itself a rank to rank embedding.*
2. *The application operation is left distributive.*
3. *We can form a left distributive algebra, $\mathcal{A}_j$ by closing any such nontrivial embedding j under application.*

Theorem (Laver, Steel)

If there exists $j \in \mathcal{E}_\lambda$, $j_{n+1} = j_n j$, *then* $\sup_n crit(j_n) = \lambda$.

Theorem (Laver)

For all rank to rank embeddings, j, $j \neq jk_1 \cdots k_n$ *for any* $k_1, \ldots k_n$ *not equal to the identity. (*$\mathcal{A}_j$ *is irreflexive.)*

Theorem (Laver, Steel(?))

$\{crit(a) : a \in \mathcal{A}_j\}$ *is an* ω*-sequence.*

Theorem (Laver)

$<_L$ linearly orders $\mathcal{A}_j$.

Theorem (Laver)

$\mathcal{A}_j \cong \mathcal{A}$

Example 2: Braid Groups

B_∞ is the braid group with infinitely man generators, $\{\sigma_1, \sigma_2, \ldots \sigma_i, \ldots\}$ and generating relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } \mid i-j \mid > 1$$

and

$$\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j \text{ if } \mid i-j \mid = 1.$$

sh is the operation induced by $sh(\sigma_i) = \sigma_{i+1}$.

Dehornoy's bracket operation, $[,,]$ is left distributive, where for $p, q \in B_\infty$,

$$p[q] = psh(q)\sigma_1 sh(p^{-1}).$$

Theorem (Dehornoy)

- $<_L$ *linearly orders the algebra generated by closing an element of* B_∞ *under* [ ]
- *(In ZFC!!) The algebra above is isomorphic to* $\mathcal{A}$

An Conjecture Relating Large Cardinals and Braids

Definition

For $a \in \mathcal{A}$ let $D_a = \{u \in \mathcal{A} : \exists v \in \mathcal{A}(uv = a)\}$

Theorem

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 $b = d$.

Conjecture

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

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

Definition

The Dehornoy ordering:

for $\alpha, \beta \in B_\infty, \alpha < \beta$ if and only if for some $N < \infty$, there is an $\overrightarrow{l} \in \mathcal{A}$

with $\overrightarrow{l}^\alpha$ lexicographically less than $\overrightarrow{l}^\beta$ with respect to $<_L$.

Laver Tables

Let $A_n = \langle \{0, 1, 2, \ldots, 2^n - 1\}, *_n \rangle$, where $*_n$ is the (seen to be unique) left distributive operation on $\{0, 1, 2, \ldots, 2^n - 1\}$ satisfying: $a *_n 1 = a + 1 \mod 2^n$.

Theorem (Basic Facts)

- *There exists a homomorphism from $\mathcal{A}$ to A_n such that $x \mapsto 1$ (for every A_n).*
- *For every $m < n$, $a \mapsto a \mod 2^m$ is a surjective morphism of A_n onto A_m.*

Definition

If $u \in \mathcal{A}$, let $[u]_n$ denote the image of u in A_n.

Theorem (Laver)

- *For all $u, v \in \mathcal{A}$, $u \not\equiv v \Rightarrow \exists n$ such that $[u]_n \neq [v]_n$.*
- *Equivalently: the period of 1 in A_n goes to infinity with n.*

The proof of this theorem uses the existence of a rank to rank embedding!! (Consistency strength upper bound.)

Theorem (Jech/Dougherty)

Laver's theorem above cannot be proven from Primitive Recursive Arithmetic (PRA).

The period of 1 in A_n dominates the Ackermann functions.

Indications of Jech and Dougherty's proof:

- Ackermann's Functions
  The function f_p is defined inductively by $f_0(n) = n + 1$ and

$$f_{p+1}(n) = \begin{cases} f_p(1) & \text{for } n = 0, \\ f_p(f_p(n-1)) & \text{otherwise} \end{cases}.$$

  Finally, $f_\omega(n) = f_n(n)$.
- f_0, f_1, f_2 are linear, f_3 is exponential, f_4 is a tower of exponentials, and so on.

- For every function, g on the integers definable from addition and multiplication using compositions and recurrence relations (the primitive recursive functions) is eventually dominated by some f_n. I.e. $\exists p$ and m such that for all $n > m$, $g(n) < f_p(n)$.
- The period of 1 in A_n dominates the Ackermann functions.

The Open Problem

- How much of mathematics is required to prove Laver's Theorem?