ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 3, Pages 28–37 (April 9, 1997)
S 1079-6762(97)00020-6

LEFT-DISTRIBUTIVE EMBEDDING ALGEBRAS

RANDALL DOUGHERTY AND THOMAS JECH

(Communicated by Alexander Kechris)

Abstract. We consider algebras with one binary operation $\cdot$ and one generator, satisfying the left distributive law $a\cdot(b\cdot c) = (a\cdot b)\cdot(a\cdot c)$; such algebras have been shown to have surprising connections with set-theoretic large cardinals and with braid groups. One can construct a sequence of finite left-distributive algebras A_n, and then take a limit to get an infinite left-distributive algebra A_∞ on one generator. Results of Laver and Steel assuming a strong large cardinal axiom imply that A_∞ is free; it is open whether the freeness of A_∞ can be proved without the large cardinal assumption, or even in Peano arithmetic. The main result of this paper is the equivalence of this problem with the existence of a certain left-distributive algebra of increasing functions on natural numbers, called an *embedding algebra*, which emulates some properties of functions on the large cardinal. Using this and results of the first author, we conclude that the freeness of A_∞ is unprovable in primitive recursive arithmetic.

1. Introduction

We consider algebras with one binary operation $\cdot$ and one generator satisfying the left distributive law $a \cdot (b \cdot c) = (a \cdot b) \cdot (a \cdot c)$.

Such algebras became an object of study when they appeared in a set-theoretic context: Laver [10] studied the properties of an algebra of elementary embeddings arising from an extremely large cardinal. He used these properties to prove purely algebraic results about the free left-distributive algebra on one generator; for instance, he showed that the word problem for this algebra is decidable. However, this was under the assumption that a large cardinal exists.

Later Dehornoy [3] proved these algebraic results using a completely different construction based on braid groups and generalizations of them, thus eliminating the large cardinal hypothesis. (Perhaps even more surprising, results about left-distributive algebras have recently been used to prove theorems about braid groups; see Dehornoy [4].)

But further algebraic results were obtainable from the large cardinal. Laver [11] used restrictions of the original elementary embeddings to produce a sequence of

Received by the editors December 16, 1996.
1991 *Mathematics Subject Classification.* Primary 20N02; Secondary 03E55, 08B20.
Key words and phrases. Left-distributive algebras, elementary embeddings, critical points, large cardinals, primitive recursive arithmetic.
The first author was supported by NSF grant number DMS-9158092 and by a grant from the Sloan Foundation.
The second author was supported by NSF grant number DMS-9401275.

finite left-distributive algebras A_n; these algebras can also be constructed directly, without large cardinals. One can then take a limit of these algebras to get an infinite left-distributive algebra A_∞ on one generator.

In the large cardinal context, it turns out that such a limit yields the original algebra of elementary embeddings, so it is free on one generator. So "A_∞ is free" is another statement about small (finite or countable) algebras proved from a large cardinal hypothesis. This statement can be rephrased in purely algebraic form, as an assertion that certain equations do not imply certain other equations under the left distributive law.

It is now natural to ask whether the freeness of A_∞ can be proved without the large cardinal assumption, or even at the level of basic arithmetic (Dehornoy's proofs can be formalized at that level). The results we present here provide, to some extent, a negative answer to this question; we show that the freeness of A_∞ cannot be proved at a low level (Primitive Recursive Arithmetic, or PRA, which is often referred to as the formal version of Hilbert's 'finitistic reasoning').

The main result of this paper is the equivalence of "A_∞ is free" with the existence of a certain algebra of increasing functions on the set $\mathbb{N}$ of natural numbers. We introduce *embedding algebras*, which are algebras $(A, \cdot)$ of increasing functions $a\colon \mathbb{N} \to \mathbb{N}$ endowed with a binary operation $\cdot$. The axioms for embedding algebras state that the operation $\cdot$ is left-distributive and that, if $\mathrm{cr}(a)$ is the least number moved by a (assuming a is not the identity), then $\mathrm{cr}(a \cdot b) = a(\mathrm{cr}(b))$. If a nontrivial embedding algebra (one which contains a function other than the identity) exists, then A_∞ is free; conversely, we construct a nontrivial embedding algebra under the assumption that A_∞ is free.

The first author proved [5] that the elementary embeddings from the large cardinal above yield numerical functions which grow faster than any primitive recursive function, and hence cannot be proved to exist in PRA. The properties of embedding algebras allow us to emulate this construction and produce the same fast-growing functions. Therefore, the existence of nontrivial embedding algebras, and hence the freeness of A_∞, cannot be proved in PRA.

In Sections 2 to 5 we outline the main results. Full proofs will appear elsewhere [7].

2. Free left-distributive algebras and elementary embeddings

We consider algebras with one binary operation $\cdot$ generated by a single element that we denote by the symbol 1. We shall often write ab instead of $a \cdot b$, and use the convention that $abc = (ab)c$.

The *left distributive law* is the identity

$$\text{(LD)} \qquad a(bc) = ab(ac).$$

Let $W = W_{\mathbf{A}}$ be the set of all words built up from 1 using the operation $\cdot$. Denote by $\equiv$ (or by $\equiv_{\mathbf{A}}$) the equivalence relation on W given by: $a \equiv b$ iff the equation $a = b$ is a consequence of (LD). Then $\mathbf{A} = W/{\equiv}$ is the free left-distributive algebra on one generator.

For the rest of this section, let $(A, \cdot)$ be a left-distributive algebra generated by 1. We will summarize the relevant known results on such algebras.

Definition 2.1. For $a, b \in A$, say that a is a *left subterm* of b, or $a <_L b$, if, for some $c_1, \ldots, c_k$ $(k > 0)$, $b = ac_1 \cdots c_k$.

Clearly the relation $<_L$ is transitive.

Theorem 2.2 (Dehornoy [1]). *On the free algebra* $\mathbf{A}$*, the relation* $<_L$ *is connected: for all* $a, b \in \mathbf{A}$*, either* $a = b$ *or* $a <_L b$ *or* $b <_L a$*.*

It follows that $<_L$ is connected in any monogenic (i.e., generated by one element) left-distributive algebra $(A, \cdot)$. Therefore, $<_L$ is a strict linear ordering of A if and only if it is irreflexive, i.e., $a \not<_L a$ for all a.

Lemma 2.3 (Dehornoy [1]). *If the relation* $<_L$ *on* A *is irreflexive, then* $(A, \cdot)$ *is free and satisfies left cancellation.*

Theorem 2.4 (Dehornoy [3]). *There is an algebra* $(A, \cdot)$ *on which* $<_L$ *is irreflexive. Consequently, the free algebra is linearly ordered by* $<_L$ *and satisfies left cancellation.*

These results were also proved by Laver [10] under a large cardinal assumption (see below).

All of the steps in Dehornoy's proofs are accomplished by explicit recursions and inductions, and the recursions are in fact primitive recursions. Therefore, these results can be proved in a very basic theory of arithmetic, such as Primitive Recursive Arithmetic (PRA). PRA is formalized in a language containing function symbols for all possible function definitions using the constant 0, the successor function $'$, composition, and primitive recursion; it has axioms stating that the function symbols satisfy their definitions, and that $0' \neq 0$, and a rule of inference allowing induction on quantifier-free formulas. (See Sieg [12] for more details.) This theory is among the weakest of the commonly studied fragments of arithmetic. It is not hard to show that the methods used to prove the above results can be formalized in this theory.

Now consider algebras with two binary operations $\cdot$ and $\circ$. We use the conventions $ab \circ c = (ab) \circ c$ and $a \circ bc = a \circ (bc)$. Let $W_{\mathbf{P}}$ be the set of all words built up from 1 using both operations, and let $\mathbf{P}$ be the free algebra on one generator under the identities:

$$\text{(LL)} \qquad \begin{aligned} a \circ (b \circ c) &= (a \circ b) \circ c, \\ (a \circ b)c &= a(bc), \\ a(b \circ c) &= ab \circ ac, \\ a \circ b &= ab \circ a. \end{aligned}$$

Then $\mathbf{P} = W_{\mathbf{P}} / \equiv_{\mathbf{P}}$, where $a \equiv_{\mathbf{P}} b$ iff the equation $a = b$ is a consequence of (LL). Note that (LD) is provable from (LL):

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

The motivation for axioms (LL) comes from large cardinal theory. Let V_λ be the collection of all sets of rank less than λ, where λ is a limit ordinal. If $\mathcal{E}$ is the set of all elementary embeddings from V_λ to V_λ, then one can 'almost' define a binary operation $\cdot$ on $\mathcal{E}$ by: $j \cdot k$ is the result of applying j to k. This does not quite work, because k is too large to be in the domain of j. Instead, one can break k into pieces which are small enough for j to digest, and recombine the results:

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

Then $j \cdot k$ will also be in $\mathcal{E}$, and it is easy to show that the operation $\cdot$ is left-distributive and, together with the operation $\circ$ of composition, satisfies (LL).

If j is a nontrivial elementary embedding from V_λ to V_λ, let $(A_j, \cdot)$ and $(P_j, \cdot, \circ)$ be the subalgebras of $(\mathcal{E}, \cdot)$ and $(\mathcal{E}, \cdot, \circ)$ generated by j. Laver [10] shows, among other things, that $(A_j, \cdot)$ and $(P_j, \cdot, \circ)$ are respectively the free monogenic left-distributive algebra and the free monogenic algebra satisfying axioms (LL).

Again, we summarize some known facts about algebras $(P, \cdot, \circ)$.

Clearly an algebra satisfying (LL) yields an algebra satisfying (LD), simply by dropping the second operation (and taking a subalgebra, if we want the result to be monogenic). But one can move in the other direction as well:

Proposition 2.5 (Laver [10], Dehornoy [2, Prop. 2])**.** *Any algebra $(A, \cdot)$ satisfying* (LD) *can be extended and expanded to an algebra $(P, \cdot, \circ)$ satisfying* (LL).

Proposition 2.6. *Let $(P, \cdot, \circ)$ be an algebra satisfying* (LL) *and generated by* 1, *and let $(A, \cdot)$ be the subalgebra of $(P, \cdot)$ generated by* 1. *Then $(P, \cdot, \circ)$ is a free* (LL)*-algebra if and only if $(A, \cdot)$ is a free left-distributive algebra.*

The proof of Propostion 2.6 can be carried out in PRA.

Now consider the algebras A_j and P_j of elementary embeddings. For each nontrivial elementary embedding a from V_λ to itself, let $\mathrm{cr}(a)$ be the *critical point* of a, i.e., the least ordinal moved by a. Let Γ be the set of all ordinals which are critical points of elements of A_j. We note that

$$\mathrm{cr}(ab) = a(\mathrm{cr}(b)), \qquad \mathrm{cr}(a \circ b) = \min(\mathrm{cr}(a), \mathrm{cr}(b)).$$

Consequently, the critical point of every $a \in P_j$ is in Γ, and every $a \in P_j$ maps Γ into Γ.

Theorem 2.7 (Laver and Steel [11])**.** *The set Γ has order type ω.*

Theorem 2.8 (Laver [11])**.** *For every $a, b \in A_j$, if $a \neq b$, then $a(\gamma) \neq b(\gamma)$ for some $\gamma \in \Gamma$.*

One can adjoin to P_j the identity embedding id. The extended algebra still satisfies axioms (LL), as well as these rules:

$$\mathrm{id} \cdot a = a, \quad a \cdot \mathrm{id} = \mathrm{id}, \quad a \circ \mathrm{id} = \mathrm{id} \circ a = a.$$

3. A limit of finite left-distributive algebras

In this section, we describe, for each natural number n, an algebra A_n on $\{0, 1, \ldots, 2^n - 1\}$ with a binary operation $*_n$ satisfying the left distributive law. We also describe a second operation $\circ_n$ on this set so that the resulting two-operation algebra P_n satisfies (LL). We then construct limit algebras $(A_\infty, \cdot)$ and $(P_\infty, \cdot, \circ)$.

The construction of these finite algebras is due to Laver; Wehrung proved some additional properties of them. The proof of the following theorem has been reconstructed independently by several people, including the authors.

Theorem 3.1 (mostly Laver)**.** *There are unique operations $*_n$ and $\circ_n$ on the set $A_n = P_n = \{0, 1, \ldots, 2^n - 1\}$ such that the axioms* (LL) *hold and, for all $a \in P_n$,*

$$a *_n 1 = a + 1 \bmod 2^n.$$

The operation $*_n$ can be defined by an explicit double recursion (which is more naturally performed over $\{1, 2, \ldots, 2^n\}$ rather than $\{0, 1, \ldots, 2^n - 1\}$); then $\circ_n$ can be defined by the formula $a \circ_n b = (a *_n (b+1)) - 1$, where the addition and subtraction are performed modulo 2^n. The theorem is then proved by multiple inductions. Along the way, one obtains additional results: reduction modulo 2^n is a homomorphism from P_m onto P_n for $m \geq n$; and, for each $a \in A_n$, the sequence $a *_n 0, a *_n 1, \ldots$ is periodic with period 2^k for some $k \leq n$ depending on a.

The element 0 of P_n plays the role that the identity embedding played at the end of Section 2:

$$0 * a = a, \quad a * 0 = 0, \quad a \circ 0 = 0 \circ a = a.$$

The element 1 is the generator of A_n and P_n (for $n > 0$).

Recall that $W_{\mathbf{A}}$ and $W_{\mathbf{P}}$ are the sets of words built up from 1 using $\cdot$ and using $\cdot, \circ$, respectively. For $m > 0$, let $w_m \in W_{\mathbf{A}}$ be the product $1 \cdot 1 \cdot \ldots \cdot 1$ with m 1's, associated to the left as usual. (In fact, it is often convenient to just write m for w_m when the context makes this clear. Note that w_m evaluates to m in A_n whenever $m < 2^n$.) Also, let $u_k \in W_{\mathbf{A}}$ be the product $1 \cdot (1 \cdot \ldots (1 \cdot 1) \ldots)$ of $(k+1)$ 1's associated to the right.

The algebras A_n have a natural purely algebraic definition: Wehrung [13] (see also Drápal [8]) showed that A_n is the free algebra on one generator 1 subject to the left distributive law and the equation $w_{2^n} \cdot 1 = 1$ (i.e., $w_{2^n+1} = 1$). If m is not a power of 2, then the free algebra subject to (LD) and the equation $w_m \cdot 1 = 1$ works out to be A_n, where 2^n is the largest power of 2 which divides m.

For every word $a \in W_{\mathbf{P}}$ and every $n \geq 0$, let $[a]_n$ be the value of a in P_n. Consider the equivalence relation $\equiv_\infty$ defined by:

$$a \equiv_\infty b \text{ iff } [a]_n = [b]_n \text{ for all } n \geq 0.$$

Let A_∞ and P_∞ be, respectively, the quotients by $\equiv_\infty$ of $W_{\mathbf{A}}$ and $W_{\mathbf{P}}$. Then $\cdot$ and $\circ$ are well defined on the quotients, and $(A_\infty, \cdot)$ and $(P_\infty, \cdot, \circ)$ are generated by 1; also, they satisfy (LD) and (LL), respectively, because A_n and P_n do. (In fact, an equivalent definition for A_∞ and P_∞ is that they are the subalgebras generated by 1 of the inverse limits of the algebras A_n and P_n, respectively.) Moreover, $A_\infty \subseteq P_\infty$.

Theorem 3.2. *The following are equivalent:*

(i) $(A_\infty, \cdot)$ *is a free left-distributive algebra.*
(ii) $(P_\infty, \cdot, \circ)$ *is a free* (LL)*-algebra.*
(iii) $<_L$ *on* A_∞ *is irreflexive.*
(iv) *For every* $a \in W_{\mathbf{A}}$, *there is an* n *such that* $[a]_n \neq 0$.
(v) *For every* $k \geq 1$, *there is an* n *such that* $[1 \cdot w_k]_n \neq 0$.
(vi) *For every* $k \geq 0$, *there is an* n *such that* $[u_k]_n \neq 0$.
(vii) *For every* $k \geq 0$, *there is an* $m > 0$ *such that* (LD) *together with the equation* $w_m \cdot 1 = 1$ *does* not *imply the equation* $u_k \cdot 1 = 1$.

All steps of the proof can be formalized in Primitive Recursive Arithmetic, so Theorem 3.2 is a theorem of PRA.

4. Embedding algebras

In this section, we consider algebras of increasing functions from $\mathbb{N}$ to $\mathbb{N}$ which imitate the behavior of the algebra of elementary embeddings from Laver [10] on ordinals. The existence of such algebras turns out to be equivalent to the properties in Theorem 3.2. Moreover, this equivalence can be proved (and formulated) in Primitive Recursive Arithmetic.

The algebras have the form $(A, \cdot)$, where A is a collection of strictly increasing functions from $\mathbb{N}$ to $\mathbb{N}$ and $\cdot$ is a binary operation on A (which we often denote by juxtaposition). The axioms for the algebra will include the axiom (LD).

Let id be the identity function on $\mathbb{N}$. If $f\colon \mathbb{N} \to \mathbb{N}$ is strictly increasing and different from id, let $\mathrm{cr}(f)$ be the least n such that $f(n) > n$ (the *critical point* of f). This is analogous to the standard definition for nontrivial elementary embeddings $j\colon V_\lambda \to V_\lambda$: the critical point of j is the least ordinal moved by j.

Definition 4.1. An *embedding algebra* is a structure $(A, \cdot)$, where A is a collection of strictly increasing functions from $\mathbb{N}$ to $\mathbb{N}$, $\cdot$ is a left-distributive binary operation on A, and for every $a, b \in A$ with $b \neq \mathrm{id}$, $\mathrm{cr}(a \cdot b) = a(\mathrm{cr}(b))$.

The set A need not contain the identity function, but one can extend the operation $\cdot$ to $A \cup \{\mathrm{id}\}$ in a natural way: $a \cdot \mathrm{id} = \mathrm{id}$, $\mathrm{id} \cdot a = a$. An embedding algebra is called *nontrivial* if it has an element other than id.

We will also need to work with a more abstract and elaborate form of embedding algebra, including much of the machinery Laver constructs for algebras of elementary embeddings.

Definition 4.2. A *two-sorted embedding algebra* consists of a nonempty set $\mathcal{E}$ (the 'embeddings,' for which we will use variables $a, b, \ldots$) and a nonempty set $\mathcal{O}$ (the 'ordinals,' for which we will use variables $\alpha, \beta, \ldots$), together with binary operations $\cdot$ and $\circ$ on $\mathcal{E}$, a binary relation $\leq$ on $\mathcal{O}$, a constant $\mathrm{id} \in \mathcal{E}$, an application operation $a, \beta \mapsto a(\beta)$ (which will often be written without parentheses) from $\mathcal{E} \times \mathcal{O}$ to $\mathcal{O}$, a function $\mathrm{cr}\colon \mathcal{E} - \{\mathrm{id}\} \to \mathcal{O}$, and a ternary relation $\equiv \subseteq \mathcal{E} \times \mathcal{O} \times \mathcal{E}$, satisfying the following axioms:

- The relation $\leq$ is a linear ordering of $\mathcal{O}$.
- Embeddings are strictly increasing monotone functions:
$$\beta < \gamma \quad \text{implies} \quad a\beta < a\gamma, \qquad \text{and} \qquad a\beta \geq \beta.$$
- For all $a \neq \mathrm{id}$, $a(\mathrm{cr}(a)) > \mathrm{cr}(a)$.
- The operation $\circ$ represents composition: $(a \circ b)\gamma = a(b\gamma)$.
- The constant id represents the identity:
$$\mathrm{id}(\gamma) = \gamma, \qquad a \cdot \mathrm{id} = \mathrm{id}, \qquad \text{and} \qquad \mathrm{id} \cdot a = a \circ \mathrm{id} = \mathrm{id} \circ a = a.$$
- The axioms (LL) hold.
- For each γ, $\equiv^\gamma$ is an equivalence relation on $\mathcal{E}$ which respects $\cdot$ and $\circ$; also, if $\gamma \leq \delta$ and $a \equiv^\delta b$, then $a \equiv^\gamma b$.
- If $a \equiv^\gamma b$ and $a\delta < \gamma$, then $a\delta = b\delta$.
- For any $a \neq \mathrm{id}$, $a \equiv^{\mathrm{cr}(a)} \mathrm{id}$.
- Coherence: $a \equiv^\gamma b$ implies $ca \equiv^{c\gamma} cb$.

Again, such an algebra is called nontrivial if there is an embedding other than id. Note that the important ordinals are the critical points, those ordinals of the form $\mathrm{cr}(a)$ for some embedding a; if we simply deleted all the other ordinals from $\mathcal{O}$, we would still have a two-sorted embedding algebra.

The results of Laver [10] show that one can make the set of all elementary embeddings from V_λ to itself into a two-sorted embedding algebra by letting $\mathcal{O}$ be the set of limit ordinals less than λ and defining $\equiv^\gamma$ to be Laver's $\overset{\gamma}{=}$. Conversely, many of Laver's arguments about elementary embeddings and their critical points use only the properties of a two-sorted embedding algebra.

If desired, one can restrict $\mathcal{E}$ to the embeddings obtained from a single embedding $j \neq \mathrm{id}$ using $\cdot$ and $\circ$ (along with id), to get a two-sorted embedding algebra generated by a single embedding. From now on, we will call a two-sorted embedding algebra *monogenic* if its embeddings are generated from a single non-identity embedding via $\cdot$ and $\circ$.

The main result of this paper is the following theorem.

Theorem 4.3. *The following are equivalent:*

(i) $(A_\infty, \cdot)$ *is a free left-distributive algebra.*
(ii) *There exists a nontrivial embedding algebra.*
(iii) *There exists a nontrivial two-sorted embedding algebra in which the ordinals have order type* ω.

In order to prove Theorem 4.3, we need to perform a number of the arguments of Laver [11] in the context of two-sorted embedding algebras. This is straightforward for arguments involving only the operations which are built into these algebras, but some arguments use additional features of elementary embeddings. In particular, a few arguments use ordinals of the form $a({<}\gamma)$, defined to be the least ordinal greater than $a(\beta)$ for all $\beta < \gamma$. For this purpose, we will define an even more elaborate algebra which includes this operation, and show that such algebras can be constructed from ordinary two-sorted embedding algebras; this will allow us to use this new operation to prove facts about the original algebra.

Definition 4.4. An *extended two-sorted embedding algebra* is a two-sorted embedding algebra (with embedding set $\mathcal{E}$ and ordinal set $\mathcal{O}$), together with two new operations, a cofinality function $\mathrm{cf}\colon \mathcal{O} \to \mathcal{O}$ and a mapping from $\mathcal{E} \times \mathcal{O}$ to $\mathcal{O}$ for which we use the notation $a, \gamma \mapsto a({<}\gamma)$, satisfying the following additional axioms:

$$\begin{gathered}
a(b({<}\gamma)) = ab({<}a\gamma);\\
a({<}b({<}\gamma)) = (a \circ b)({<}\gamma);\\
a({<}\gamma) \leq a\gamma;\\
\text{if}\quad \gamma < \delta, \quad\text{then}\quad a\gamma < a({<}\delta);\\
\text{if}\quad a \equiv^\gamma b \quad\text{and}\quad a({<}\delta) \leq \gamma, \quad\text{then}\quad a({<}\delta) = b({<}\delta);\\
\mathrm{cf}(\mathrm{cr}(a)) = \mathrm{cr}(a);\\
\mathrm{cf}(a({<}\gamma)) = \mathrm{cf}\,\gamma;\\
\mathrm{cf}(a\gamma) = a(\mathrm{cf}\,\gamma);\\
\mathrm{cf}\,\gamma \leq \gamma;\\
\text{if}\quad a(\mathrm{cf}\,\gamma) = \mathrm{cf}\,\gamma, \quad\text{then}\quad a({<}\gamma) = a\gamma.
\end{gathered}$$

Again it is not hard to verify that the axioms for an extended two-sorted embedding algebra hold in the case where $\mathcal{E}$ is the set of elementary embeddings on V_λ and $\mathcal{O}$ is the collection of limit ordinals less than λ [11].

The following is a crucial technical result:

Theorem 4.5. *Suppose that we are given a two-sorted embedding algebra, in which every ordinal is a critical point. Then the algebra can be extended to a new two-sorted embedding algebra with the same embedding set, on which the required additional operations can be defined so as to give an extended two-sorted embedding algebra.*

Theorem 4.5 can be used to transfer various arguments from the context of elementary embeddings to that of two-sorted embedding algebras. One example is the following result, which is proved by following Laver's proof of Theorem 2.8.

In a two-sorted embedding algebra, let $j \neq \mathrm{id}$ be some embedding, and let A_j be the set of embeddings generated from j by the operation $\cdot$ (so each $a \in A_j$ is given by a word in $W_{\mathbf{A}}$ evaluated at j).

Theorem 4.6. *Assume that the set of all critical points of elements of A_j has order type ω. If a and b are distinct elements of A_j, then there is a critical point γ such that $a(\gamma) \neq b(\gamma)$.*

We now outline the proof of Theorem 4.3. First, suppose that A_∞ is free, and hence all of the statements in Theorem 3.2 hold. We build a two-sorted embedding algebra with embedding set $\mathbf{P} \cup \{\mathrm{id}\}$ and ordinal set $\mathbb{N}$, as follows. For $a \in \mathbf{P}$, define $\mathrm{cr}(a)$ to be the least n such that $[a]_{n+1} \neq 0$, or, equivalently, the largest n such that $[a]_n = 0$. Let $a(n) = \mathrm{cr}(a \cdot w_{2^n})$, and define $a \equiv^n b$ to mean that $[a]_n = [b]_n$ (where we put $[\mathrm{id}]_n = 0$). Then one can prove from the properties of the finite algebras A_n that these definitions meet the requirements of a two-sorted embedding algebra.

Next, suppose we have a nontrivial two-sorted embedding algebra in which the ordinals have order type ω. We may take the subalgebra A_j generated by some $j \neq \mathrm{id}$, and then throw away all ordinals that are not critical points of members of A_j. The remaining ordinals still have order type ω, so we can relabel them as the natural numbers. By Theorem 4.6, distinct embeddings yield distinct functions from $\mathbb{N}$ to $\mathbb{N}$; the resulting set of functions, with the binary operation $\cdot$ transferred from the set of embeddings, forms an embedding algebra.

On the other hand, if we have a nontrivial embedding algebra, then we can turn it into a two-sorted embedding algebra. The set of ordinals will be the set of critical points of the embeddings (which has order type ω, since it is an infinite subset of $\mathbb{N}$). Proposition 2.5 lets us extend the set of embeddings to admit a composition operation; the result of applying composite embeddings $a \circ b$ to ordinals is defined by the obvious formula $(a \circ b)(n) = a(b(n))$. With more work, one can define suitable equivalence relations $\equiv^n$ and show that all the axioms of a two-sorted embedding algebra hold.

Finally, again assuming we have a nontrivial two-sorted embedding algebra in which the ordinals have order type ω, we can imitate the arguments of Laver [11] for constructing the finite algebras in the first place, to show that statement (iv) of Theorem 3.2 is true, and hence A_∞ is free. The only part of this argument that cannot be carried out in two-sorted embedding algebras is the proof of the Laver-Steel result (Theorem 2.7 here), so we have made this a hypothesis instead. This completes the proof outline.

In the process of proving Theorem 4.3, we also obtain the following uniqueness result for monogenic embedding algebras.

Theorem 4.7. *If $(A, \cdot)$ is a monogenic embedding algebra for which every natural number is a critical point, then $(A, \cdot)$ is the embedding algebra constructed from the algebras A_n as above.*

Similarly, any monogenic two-sorted embedding algebra in which the ordinals have order type ω and are all critical points must be isomorphic to the one constructed from the algebras A_n.

5. The strength of "A_∞ is free"

Laver's proof of the irreflexivity of the free left distributive algebra on one generator assumed the existence of a nontrivial elementary embedding from V_λ to itself; this is an extremely strong large cardinal hypothesis. (Actually, Laver had noted that the assumption can be reduced to the existence of an n-huge cardinal for each natural number n.) The possibility that the irreflexivity property was strong enough to require large cardinal assumptions for its proof remained until Dehornoy proved the property without such assumptions (in fact, using only Primitive Recursive Arithmetic).

We now consider the statement "A_∞ is free" (and its equivalent versions). Laver [11] showed that this statement also follows from the existence of a nontrivial elementary embedding $j: V_\lambda \to V_\lambda$. (In fact, one might consider "A_∞ is free" to be the algebraic content of the set-theoretic Theorem 2.7.) Laver (personal communication) has noted, and the authors have confirmed, that one can use the method of proof of Theorem 2.7 while working with only an n-huge embedding, to get a correspondingly weaker result; hence, the freeness of A_∞ follows from the existence of an n-huge cardinal for each natural number n.

However, unlike the irreflexivity of the free algebra, the freeness of A_∞ cannot be proved without some 'strong' hypothesis:

Theorem 5.1. *The statement "A_∞ is free" is not provable in Primitive Recursive Arithmetic.*

Of course, we assume throughout that PRA is itself consistent.

It is a well-known result from proof theory (see Sieg [12]) that the only recursive functions that can be proved to be total using only PRA are the primitive recursive functions. Therefore, to prove Theorem 5.1, it will suffice to show that PRA+3.2(vi) proves the totality of a recursive function F which is not primitive recursive.

For each natural number n, let $F(n)$ be the largest m such that $[u_n]_m = 0$, where u_n is the word $1 \cdot (1 \cdot (\ldots (1 \cdot 1) \ldots))$ with $n+1$ 1's. It follows from 3.2(vi) that F is a total recursive function.

This function can be characterized in another way in terms of the monogenic embedding algebra or two-sorted embedding algebra constructed from the finite algebras. Let j be the generating embedding, and let Γ be the set of all critical points of embeddings in the algebra. Among these critical points are a special sequence $\kappa_0 < \kappa_1 < \kappa_2 < \cdots$ called the *critical sequence* of j: $\kappa_0 = \mathrm{cr}(j)$ and $\kappa_{n+1} = j(\kappa_n)$. Then $F(n)$ is the number of members of Γ lying below κ_n.

The main result of Dougherty [5] shows that, in the context of elementary embeddings from V_λ to V_λ, the function F defined as in the preceding paragraph grows faster than the Ackermann function, and hence cannot be primitive recursive. However, the methods used in that proof use only the properties of embeddings that follow immediately from the axioms of an embedding algebra or two-sorted embedding algebra. (In fact, all of the proofs in Dougherty [5] can be carried out in any extended two-sorted embedding algebra.) Therefore, the same growth estimates apply to the embedding algebra constructed from the finite algebras, and this requires only the assumption that A_∞ is free. Therefore, this assumption is too strong to be proved in PRA.

In a sense, the function F gives a measure of the proof-theoretic strength of the statement "A_∞ is free." This can be stated precisely as follows.

Proposition 5.2. *Any recursive function which is provably total in* PRA + *"A_∞ is free" must grow more slowly than F_m for some m, where $F_0 = F$ and F_{m+1} is the iteration of F_m (starting at 1, say; that is, $F_{m+1}(n) = F_m^n(1)$).*

There remain a number of open problems related to these algebras. The main one, of course, is the exact strength of the statement "A_∞ is free"; the gap between "more than PRA" and "there is an n-huge cardinal for each n" is rather large. More recent results about the finite algebras A_n [6], [8], [9] may be steps toward a proof without large cardinals that A_∞ is free, but the full situation is not at all clear.

References

1. P. Dehornoy, *Sur la structure des gerbes libres*, C. R. Acad. Sci. Paris Sér. I Math. **309** (1989), 143–148. MR **90j**:20146
2. ———, *The adjoint representation of left distributive structures*, Comm. Algebra **20** (1992), 1201–1215. MR **93a**:20108
3. ———, *Braid groups and left distributive operations*, Trans. Amer. Math. Soc. **345** (1994), 115–150. MR **95a**:08003
4. ———, *From large cardinals to braids via distributive algebra*, J. Knot Theory Ramifications **4** (1995), 33–79. MR **96g**:20056
5. R. Dougherty, *Critical points in an algebra of elementary embeddings*, Ann. Pure Appl. Logic **65** (1993), 211–241. MR **95i**:03117
6. ———, *Critical points in an algebra of elementary embeddings, II*, Logic: from Foundations to Applications (W. Hodges *et al.*, eds.), Clarendon, Oxford, 1996, pp. 103–136. CMP 97:06
7. R. Dougherty and T. Jech, *Finite left-distributive algebras and embedding algebras*, Adv. Math. (to appear).
8. A. Drápal, *Homomorphisms of primitive left distributive groupoids*, Comm. Algebra **22** (1994), 2579–2592. MR **95c**:20107
9. ———, *Persistence of cyclic left distributive algebras*, J. Pure Appl. Algebra **105** (1995), 137–165. MR **96m**:20113
10. R. Laver, *The left distributive law and the freeness of an algebra of elementary embeddings*, Adv. Math. **91** (1992), 209–231. MR **93b**:08008
11. ———, *On the algebra of elementary embeddings of a rank into itself*, Adv. Math. **110** (1995), 334–346. MR **96c**:03098
12. W. Sieg, *Fragments of arithmetic*, Ann. Pure Appl. Logic **28** (1985), 33–71. MR **86g**:03099
13. F. Wehrung, *Gerbes primitives*, C. R. Acad. Sci. Paris Sér. I Math. **313** (1991), 357–362. MR **92i**:08004

Department of Mathematics, Ohio State University, Columbus, OH 43210
E-mail address: `rld@math.ohio-state.edu`

Pennsylvania State University, 215 McAllister Building, University Park, PA 16802
E-mail address: `jech@math.psu.edu`