

LARGE ORDINALS

THOMAS JECH

The Pennsylvania State University

ABSTRACT. Let j be an elementary embedding of V_λ into V_λ that is not the identity, and let κ be the critical point of j . Let \mathcal{A} be the closure of $\{j\}$ under the operation $a(b)$ of application, and let Ω be the closure of $\{\kappa\}$ under the operation $\min\{\xi : a(\xi) \geq b(\alpha)\}$.

We give a complete description of the set Ω under an assumption (Threshold Hypothesis) on cyclic left distributive algebras.

1. Introduction

Let λ be a limit ordinal such that there exists a nontrivial elementary embedding $j : (V_\lambda, \epsilon) \rightarrow (V_\lambda, \epsilon)$. The existence of such a λ is a large cardinal axiom, and by Kunen [5], $\lambda = \lim_{n \rightarrow \infty} \kappa_n$ where $\kappa_0 = \kappa$ is the critical point of j and $\kappa_{n+1} = j(\kappa_n)$ for all $n = 0, 1, 2, \dots$.

Following Laver [6], if j and k are elementary embeddings from V_λ to V_λ , let $j \cdot k$ denote the elementary embedding $j(k) = \bigcup_{\alpha < \lambda} j(k \upharpoonright V_\alpha)$. The binary operation $j \cdot k$ satisfies the left-distributive law

$$(LD) \quad a(bc) = ab(ac)$$

[Here and throughout the paper we adopt the convention that $abc = (ab)c$.]

Let $j = V_\lambda \rightarrow V_\lambda$ and let $\kappa = \text{crit}(j)$ be the critical point of j . Let $\mathcal{A} = \mathcal{A}_j$ be the closure of $\{j\}$ under \cdot and let $\mathcal{P} = \mathcal{P}_j$ be the closure of $\{j\}$ under \cdot and \circ where \circ denotes composition. Let

$$\Gamma = \{a\kappa : a \in \mathcal{A}\}.$$

[Another convention we adopt is writing $a\kappa$ instead of $a(\kappa)$.]

As $\text{crit}(ab) = a \text{crit}(b)$, Γ is the set of all critical points of all $a \in \mathcal{A}$, and it is easily seen that $\Gamma = \{a\kappa : a \in \mathcal{P}\} = \{\text{crit}(a) : a \in \mathcal{P}\}$.

In [6], Laver proved that \mathcal{A} is the free left distributive algebra on one generator, and in [7] he showed, using a result of Steel, that Γ has order type ω . In fact, if we let

$$j_1 = j, \quad j_{n+1} = j_n j$$

then $\Gamma = \{\gamma_n : n = 0, 1, 2, \dots\}$ where

$$\gamma_n = \text{crit}(j_{2^n}) \quad \text{and} \quad \gamma_0 < \gamma_1 < \dots < \gamma_n < \dots$$

In this paper we investigate certain ordinal numbers defined in terms of the embeddings in \mathcal{A} (\mathcal{P}) and the critical points in Γ . These ordinals have been studied in [7], [1] and [3].

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$ - TEX

1.1. Definition. The set Σ of *simple ordinals* is the closure of Γ under the operation

$$a''\alpha = \sup\{a\xi : \xi < \alpha\} \quad (a \in \mathcal{A})$$

The set Ω of *ordinals* is the closure of Γ under the operation

$$a^-\alpha = \min\{\xi : a\xi \geq \alpha\} \quad (a \in \mathcal{A})$$

The following facts are consequences of elementarity:

1.2. Lemma. For all $a, b \in \mathcal{P}$ and all ordinals α ,

$$\begin{aligned} a(b\alpha) &= ab(a\alpha) \\ a(b''\alpha) &= ab''a\alpha \\ a''b''\alpha &= (a \circ b)''\alpha \\ a(b^-\alpha) &= ab^-a\alpha \\ a^-b^-\alpha &= (b \circ a)^-\alpha. \end{aligned}$$

As a corollary, $\Sigma = \{a''\gamma : \gamma \in \Gamma \text{ and } a \in \mathcal{P}\}$ and $\Omega = \{a^-\gamma : \gamma \in \Gamma \text{ and } a \in \mathcal{P}\}$.

The following argument shows that every ordinal in Σ is in Ω .

1.3. Lemma. (Dougherty) Let $c \in \mathcal{A}$ be such that $\gamma = \text{crit}(c)$. Then $a''\gamma = c^-(ca\gamma)$, for every $a \in \mathcal{P}$.

Proof. We have $c(a''\gamma) = ca''c\gamma$, and because $c\gamma > \gamma$, it follows that $ca''c\gamma > ca\gamma$. Thus $c(a''\gamma) > ca\gamma$.

If $\eta < a''\gamma$, then $\eta < a\xi$ for some $\xi < \gamma$. Since $c\xi = \xi$, we have $c\eta < c(a\xi) = ca(c\xi) = ca\xi < ca\gamma$. Thus $a''\gamma$ is the least η such that $c\eta > ca\gamma$.

It has been conjectured by Laver that $\Sigma = \Omega$. We prove this equality (Theorem 3.9), under an assumption on cyclic LD algebras (the Threshold Hypothesis 3.1). Under the same hypothesis, we give a complete description of ordinals in Ω (Theorem 4.4).

To conclude this introduction, we state the following facts about the ordinals that will be used in subsequent arguments:

1.4. Lemma. (a) If $\alpha < \beta$ then $a\alpha < a''\beta$
 (b) If $\gamma \in \Gamma$ and $a\gamma > \gamma$ then $a''\gamma < a\gamma$.
 (c) If $\gamma \in \Gamma$ and $b\gamma > \gamma$ then $a''b\gamma > a(b''\gamma)$

Proof. (a) follows from the definition; (b) from the fact that $\text{cf}(a''\gamma) = \gamma$ while $\text{cf}(a\gamma) = a(\text{cf}\gamma) = a\gamma$, and (c) combines (a) and (b).

2. Critical points and cyclic LD algebras

We shall exploit the remarkable connection between the algebras \mathcal{A} and \mathcal{P} and the (finite) cyclic left-distributive algebras. We shall first review some facts from [3] about cyclic LD algebras.

For each n let $A_n = \{0, 1, \dots, 2^n - 1\}$. There is a unique left-distributive operation $*_n$ on A_n such that $a * 1 = a + 1 \pmod{2^n}$. For every $a \in A_n$ there exists a number $p_n(a) = 2^k$, the period of a such that

$$(2.1) \quad a < a * 1 < a * 2 < \dots < a * (2^k - 1), \quad a * 2^k = 0$$

and $a * (2^k + b) = a * b$.

In particular,

$$(2.2) \quad p_n(0) = 2^n, \quad p_n(2^n - 1) = 1, \quad p_n(2^{n-1}) = 2^{n-1}$$

and for all a , if $0 < a < 2^n - 1$ then $1 < p_n(a) < 2^n$.

Reduction modulo 2^n is a homomorphism from A_{n+1} to A_n :

$$(2.3) \quad a *_n b \pmod{2^n} = (a \pmod{2^n}) *_n (b \pmod{2^n}).$$

It follows that for every $a \in A_n$, $p_{n+1}(a)$ either remains equal to $p_n(a)$ or doubles:

$$(2.4) \quad p_{n+1}(a) = \begin{cases} p_n(a) \\ 2p_n(a) \end{cases}$$

and

$$(2.5) \quad p_{n+1}(a + 2^n) = p_n(a).$$

If the period $p_n(a) = 2^k$ doubles to 2^{k+1} , then $a *_n 2^k = 2^n$.

2.1. Definition. The *threshold* $t_n(a)$ of $a \in A_n$ is the least c such that $a *_n c \geq 2^{n-1}$:

$$(2.6) \quad a *_n (t_n(a) - 1) < 2^{n-1} \leq a *_n t_n(a).$$

If $a \geq 2^{n-1} - 1$ then $t_n(a) = 1$. If $a < 2^{n-1} - 1$ then $1 < t_n(a) \leq p_n(a)/2$.

By (2.3), the inverse limit of the A_n is a left-distributive algebra; let A_∞ denote its subalgebra generated by the element 1.

If w is an element of the free left-distributive algebra on one generator 1 (a “word”), let $[w]_n$ denote the element of A_n to which w evaluates. By (2.3) we have, for all w ,

$$(2.7) \quad [w]_{n+1} = \begin{cases} [w]_n \\ [w]_n + 2^n \end{cases}$$

and $A_\infty \models v = w$ iff for all n , $[v]_n = [w]_n$. Theorem 4.4 of [3] gives several conditions equivalent to the statement that A_∞ is the free algebra; by [6], these are true under the assumption of the existence of a nontrivial elementary embedding $j : V_\lambda \rightarrow V_\lambda$.

If a nontrivial $j : V_\lambda \rightarrow V_\lambda$ exists, then \mathcal{A} is the free one-generated left-distributive algebra and \mathcal{A} is isomorphic to A_∞ . Moreover, as Laver has shown in [6], the equivalence relation $k \stackrel{\gamma_n}{\equiv} \ell$ (defined in [6]) gives a homomorphism of \mathcal{A}

onto A_n . We recall that this equivalence relation can be defined algebraically on A_∞ ; see [3], Definition 5.1. In particular we have

$$(2.8) \quad a \stackrel{\gamma_n}{=} b \quad \text{iff} \quad [a]_n = [b]_n.$$

As \mathcal{A} and A_∞ are isomorphic, we shall identify the generator j of \mathcal{A} with 1, and consider the elements $a \in A_\infty$ to be elementary embeddings. In particular, every integer k can be identified with some $k \in \mathcal{A}$ via

$$(2.9) \quad 1 = j, \quad k + 1 = k * j.$$

Using (2.8), we note that if $A_n \models a = b$ then for every $\gamma \in \Gamma$

$$(2.10) \quad \begin{array}{ll} \text{if } a\gamma < \gamma_n & \text{then } b\gamma = a\gamma \\ \text{if } a\gamma \geq \gamma_n & \text{then } b\gamma \geq \gamma_n \\ \text{if } a''\gamma < \gamma_n & \text{then } b''\gamma = a''\gamma \end{array}$$

2.2. Definition. For every word a let $s(a)$ (the *signature* of a) be the largest n such that $[a]_n = 0$; if a is an integer then $s(a)$ is the largest $s(a)$ such that $2^{s(a)}$ divides a .

The following summarizes the connection between the algebras A_n and the critical points $\gamma \in \Gamma$:

2.3. Lemma. $\text{crit}(a) = \gamma_{s(a)}$;
 $a\gamma_k \geq \gamma_n$ iff $p_n(a) \leq 2^k$;
 $a\gamma_k = \gamma_n$ where $n = s(a * 2^k)$.

In particular, this includes Laver's result mentioned in the introduction:

$$(2.11) \quad \text{crit}(2^n) = \gamma_n, \quad 2^n\gamma_n = \gamma_{n+1};$$

the latter is equivalent to this fact about the A_n 's:

$$(2.12) \quad A_{n+2} \models 2^n * 2^n = 2^{n+1},$$

which has the following consequence (that one can also prove directly):

$$(2.13) \quad A_{n+2} \models 2^n * a = 2^n + a \quad (a \leq 2^n).$$

2.4. Lemma. $(2^n - 1)\gamma_0 = \gamma_n$, $(2^n - 1)\gamma_1 = \gamma_{n+1}$.

Proof. $(2^n - 1)\gamma_0 = (2^n - 1)\text{crit}(1) = \text{crit}((2^n - 1) * 1) = \text{crit}(2^n) = \gamma_n$;
 $(2^n - 1)\gamma_1 = (2^n - 1)(1\gamma_0) = (2^n - 1) * 1((2^n - 1)\gamma_0) = 2^n\gamma_n = \gamma_{n+1}$.

2.5. Lemma. If $a < 2^n - 1$ then $a\gamma_0 < \gamma_n$ and $a\gamma_1 < \gamma_{n+1}$.

Proof. If $a < 2^n - 1$ then $a * 1 \leq 2^n - 1$ and so $s(a * 1) < n$; hence $a\gamma_0 < \gamma_n$. the second statement is proved by induction on n : When $n = 2$, we have $a\gamma_1 = \gamma_2$ for both $a = 1$ and $a = 2$. Thus let $n > 2$. If $a < 2^{n-1} - 1$ then $a\gamma_1 < \gamma_n$, if $a = 2^{n-1} - 1$ then $a\gamma_1 = \gamma_n$ and if $a = 2^{n-1}$ then $a\gamma_1 = \gamma_1$. If $2^{n-1} < a < 2^n - 1$ then $a = 2^{n-1} + b$ where $b < 2^{n-1} - 1$, and we have (by 2.13) $a\gamma_1 = (2^{n-1} * b)(2^{n-1}\gamma_1) = 2^{n-1}(b\gamma_1) \leq 2^{n-1}\gamma_{n-1} = \gamma_n$.

Following [3], Section 3, let

$$a \circ_n b = (a * _n (b + 1)) - 1 \text{ mod } 2^n,$$

for all $a, b \in A_n$; the relation \circ_n on A_n is a homomorphic image of composition on \mathcal{P} under the homomorphism given by the equivalence relation $=^{\gamma_n}$.

2.6. Lemma. *Let $a \in \mathcal{P}$. If $a\gamma_0 = \gamma_n$ then $a''\gamma_1 = (2^n - 1)''\gamma_1$. If $k \geq 1$ and $a\gamma_k = \gamma_n$ then $a''(2^k - 1)''\gamma_1 = (2^n - 1)''\gamma_1$.*

Proof. We prove the second statement only, as the proof of the first one is similar. We have $a''(2^k - 1)''\gamma_1 = a \circ (2^k - 1)''\gamma_1$, $a \circ_{n+1} (2^k - 1) = (a *_{n+1} 2^k) - 1 = 2^n - 1$, and the statement follows by Lemma 2.4 and by (2.10).

2.7. Corollary. *γ_1 is the least ordinal in Ω above γ_0 ; for every $k \geq 1$, $(2^k - 1)''\gamma_1$ is the least ordinal in Ω above γ_k .*

Proof. Again, we only prove the second statement. Let $\alpha = a^- \gamma$ be an ordinal in Ω greater than γ_k . Let $a\gamma_k = \gamma_n$; since $\gamma_k < \alpha$, we have $\gamma_n < \gamma$. By Lemmas 2.6 and 2.4, $a''(2^k - 1)''\gamma_1 = (2^n - 1)''\gamma_1 < (2^n - 1)\gamma_1 = \gamma_{n+1} \leq \gamma$ and so $(2^k - 1)''\gamma_1 \leq \alpha$.

2.8. Lemma. *If $2^n < a < 2^{n+1}$ then there is no α such that $\gamma_n \leq a\alpha < \gamma_{n+1}$, and for no α , $\gamma_n \leq a''\alpha < \gamma_{n+1}$.*

Proof. Let $b = a - 2^n$; we have $A_{n+1} \models a = 2^n * b$. If $\alpha \geq \gamma_n$ then $a\alpha \geq \gamma_{n+1}$ because $\text{crit}(a) \leq \gamma_n$. If $\alpha < \gamma_n$ then $2^n\alpha = \alpha$, and

$$\begin{aligned} a\alpha &= 2^n b(2^n\alpha) = 2^n(b\alpha), \\ a''\alpha &= 2^n b'' 2^n\alpha = 2^n(b''\alpha). \end{aligned}$$

Hence both $a\alpha$ and $a''\alpha$ are in the range of 2^n , which is disjoint from the interval $[\gamma_n, \gamma_{n+1})$.

2.9. Corollary. *Every $\alpha \in \Sigma$ between γ_n and γ_{n+1} is equal to $a''\gamma$ for some $\gamma \in \Gamma$ and $a < 2^n$.*

Proof. Let $\alpha = b''\gamma$ where $b \in \mathcal{P}$ and let $a = [b]_{n+1}$. Hence $\alpha = a''\gamma$, and $a < 2^n$ by Lemma 2.8.

3. The Threshold Hypothesis and its consequences

We shall now formulate a conjecture about the cyclic algebras and use it to prove results about embeddings in \mathcal{P} and ordinals in Ω .

3.1. The Threshold Hypothesis (TH). Let $a < 2^n - 1$, and let $p_{n+1}(a) = 2^{k+1}$. If $c + 1$ is the threshold of a in A_{n+1} then $p_{k+2}(c) = 2p_{k+1}(c)$.

The conclusion of TH, $p_{k+2}(c) = 2p_{k+1}(c)$, is equivalent to the statement that $\gamma_{k+1} = c\gamma_m$ for some $\gamma_m \in \Gamma$. We shall call the set $\{c\delta : \delta \in \Gamma\}$ the *range* of c .

The statement that $\gamma \in \text{range}(c)$ is not necessarily equivalent to $\gamma = c(\alpha)$ for some ordinal α . However, if Laver's conjecture holds then these are equivalent: if $\gamma = c(\alpha)$ then $\alpha \in \Omega$ and hence $\alpha = a''\delta$ for some $\delta \in \Gamma$, therefore $\gamma = ca''c\delta$ and by cofinality, $c\delta = \gamma$, $\alpha = \delta$.

We conjecture that (TH) holds in every n . In the applications that follow we only use the following consequence of TH:

3.2. Lemma. *Assume TH and let $a < 2^n - 1$. If $a\gamma_{k+1} = \gamma_{n+1}$ then there exists a $c < 2^k$ such that $\gamma_{k+1} \in \text{range}(c)$ and $A_{n+2} \models ac < 2^n$.*

Proof. By Lemma 2.3, $p_{n+1}(a) = 2^{k+1}$, and because $a < 2^n - 1, k \geq 1$ (by Lemma 2.5). Let $c + 1$ be the threshold of a in A_n ; by (2.6), $0 < c < 2^k$, and by TH, $\gamma_{k+1} \in \text{range}(c)$. Since $c < t_{n+1}(a)$, we have $A_{n+1} \models ac < 2^n$. By Lemma 2.3, $a\gamma_{k+1} = \gamma_{n+1}$ implies that $t_{n+2}(a) = 2^{k+1}$, and it follows that $A_{n+2} \models ac < 2^n$.

3.3. Theorem. *Assume TH. If $a < 2^n$ and $a\gamma_{k+1} = \gamma_{n+1}$ then $a''\gamma_{k+1} > \gamma_n$.*

Proof. The statement is vacuously true for $n = 0$. For every $n \geq 1$ we prove the theorem by downward induction on a .

First let $a = 2^n - 1$. By Lemma 2.4 we have $k = 0, a\gamma_0 = \gamma_n$ and $a\gamma_1 = \gamma_{n+1}$. Therefore $\gamma_n < a''\gamma_1 < \gamma_{n+1}$.

Now let $a < 2^n - 1$. by Lemma 3.2 there exists some $c < 2^k$ such that $A_{n+2} \models ac < 2^n$, and $\gamma_{k+1} \in \text{range}(c)$. Let $\delta \in \Gamma$ be such that $c\delta = \gamma_{k+1}$, and let $b = [ac]_{n+2}$. Since $c < 2^k$, we have (by Lemmas 2.3 and 2.5) $\gamma_0 < \delta < \gamma_{k+1}$ and so $a\delta = \gamma_{m+1}$ for some $m < n$. Therefore

$$ac\gamma_{m+1} = ac(a\delta) = a(c\delta) = a\gamma_{k+1} = \gamma_{n+1}$$

and so $b\gamma_{m+1} = \gamma_{n+1}$. Since $b > a$ and $b < 2^n$, we have, by the induction hypothesis, $b''\gamma_{m+1} > \gamma_n$. Now the statement for a follows (using Lemma 1.4 and (2.10)):

$$a''\gamma_{k+1} = a''c\delta > a(c''\delta) = ac''\delta = ac''\gamma_{m+1} = b''\gamma_{m+1} > \gamma_n.$$

3.4. Corollary. *(TH) If $a < 2^n$ and if $\gamma_n < a''\gamma < \gamma_{n+1}$ then $a\gamma = \gamma_{n+1}$*

Proof. Let $a\gamma = \gamma_{m+1}$. By Theorem 3.3, $a''\gamma > \gamma_m$, and so $m = n$.

3.5. Corollary. *(TH) If $a < 2^n$ and $\gamma_{n+1} \in \text{range}(a)$ then there exists an $\alpha \in \Sigma$ such that $\gamma_n < a\alpha < \gamma_{n+1}$.*

Proof. It is $\alpha = c''\delta$ in the proof of Theorem 3.3.

3.6. Definition. For $\alpha \in \Sigma$, let α^+ denote the least ordinal in Σ greater than α .

3.7. Corollary. *(TH) Let $a < 2^n$ and let $\alpha^+ = \gamma \in \Gamma$ be a critical point. If $\gamma_n \leq a\alpha < \gamma_{n+1}$ then $a\gamma = \gamma_{n+1}$.*

Proof. If $\gamma = \gamma_1$ then $\alpha = \gamma_0$ by Corollary 2.7, and so $a\gamma_0 = \gamma_n$. By Lemmas 2.4 and 2.5, $a = 2^n - 1$ and so $a\gamma_1 = \gamma_{n+1}$.

Thus let $\gamma = \gamma_{k+1}$ where $k > 0$. Then $a\gamma_{k+1} = \gamma_{m+1}$ where $m \geq n$. By Corollary 3.5 there exists a $\beta \in \Sigma$ such that $\gamma_m < a\beta < \gamma_{m+1}$, and since $\gamma = \alpha^+$, we have $\gamma_m < a\alpha$. It follows that $m = n$ and hence $a\gamma = \gamma_{n+1}$.

3.8. Corollary. *(TH) If $\gamma = \alpha^+ \in \Gamma$ and if $a \in \mathcal{P}$ is arbitrary, then there is no critical point $\delta \in \Gamma$ between $a\alpha$ and $a''\gamma$.*

Proof. This is true if $a\alpha = \alpha$, so assume that $\text{crit}(a) < \alpha$. Let n be such that $\gamma_n \leq a\alpha < \gamma_{n+1}$. We will show that $a''\gamma < \gamma_{n+1}$. By Lemma 2.8, $A_{n+1} \models a < 2^n$. Let $b = [a]_{n+1}$; then $b < 2^n, \gamma_n \leq b\alpha < \gamma_{n+1}$, and by Corollary 3.7 we have $b\gamma = \gamma_{n+1}$.

Since $\text{crit}(b) = \text{crit}(a) < \gamma_n$ we have $b''\gamma < \gamma_{n+1}$, and it follows that $a''\gamma < \gamma_{n+1}$.

3.9. Theorem. *Assume TH. Then Laver's Conjecture holds; i.e. every ordinal $u^{-}\lambda \in \Omega$ is in Σ .*

Proof. Let $\xi = u^{-}\lambda$ ($\lambda \in \Gamma$) be a counterexample. Let $b''\gamma$ ($\gamma \in \Gamma$) be the least ordinal in Σ greater than ξ . Let $\alpha \in \Sigma$ be such that $\alpha^+ = \gamma$. Since $b\alpha \in \Sigma$, we have $b\alpha < \xi < b''\gamma$.

Let $a = u \circ b$. We have

$$a''\gamma = (u \circ b)''\gamma = u''b''\gamma > u\xi \geq \lambda$$

(by Lemma 1.4), and

$$a\alpha = (u \circ b)\alpha = u(b\alpha) < \lambda.$$

This contradicts Corollary 3.8.

We conclude this Section with the following observation of Laver:

3.10. Lemma (Laver). *If $\Omega = \Sigma$ then*

$$a''\alpha^+ = (a\alpha)^+$$

for all $a \in \mathcal{P}$ and all $\alpha \in \Sigma$.

Proof. Assume otherwise and let $\xi \in \Sigma$ be such that $a\alpha < \xi < a''\alpha^+$. Then $\alpha < a^{-}\xi < \alpha^+$, a contradiction.

4. Ordinals between γ_n and γ_{n+1}

In this Section we again assume TH and describe all Ω -ordinals between two consecutive critical points. We also formulate the *Uniqueness Hypothesis*, another conjecture about the cyclic algebras, and use it to prove that the representation is unique.

4.1. Definition. Let $\alpha \in \Sigma$ be such that $\gamma_n < \alpha < \gamma_{n+1}$; α is *special* (below γ_{n+1}) if $\alpha^+ = \gamma_{n+1}$.

4.2. Lemma. *If α is special then there exist no $\xi \in \Omega$, $\xi < \alpha$ and no $a \in \mathcal{P}$ such that $\alpha = a\xi$.*

Proof. If $a\xi = \alpha$ then by Lemma 3.9 the ordinal $\alpha^+ = a''\xi^+$ has cofinality cf $\xi^+ < \alpha^+$ and therefore is not a critical point.

4.3. Lemma. *If $\alpha \in \Omega$, $\gamma_n < \alpha < \gamma_{n+1}$ and α is not special, then there exist $\xi \in \Omega$, $\xi < \alpha$ and $a \in \mathcal{P}$ such that $\alpha = a\xi$.*

Proof. If α is not special then $\alpha^+ = a''\gamma$ for some $a \in \mathcal{P}$ and $\gamma \in \Gamma$, $\gamma \neq \gamma_0$. Let $\xi \in \Omega$ be such that $\xi^+ = \gamma$. By Lemma 3.10, $(a\xi)^+ = a''\xi^+ = a''\gamma = \alpha^+$, and so $\alpha = a\xi$.

4.4. Theorem. *Let $a < 2^n$, $\alpha \in \Omega$ and $\gamma_n < \alpha < \gamma_{n+1}$. The ordinal α is not special if and only if there exist $c < 2^n$, $\gamma \in \Gamma$, $a < c$, $\lambda \in \Gamma$ and b such that $\alpha = c''\gamma$, $a\lambda = \gamma$ and $A_{n+1} \models ab = c$.*

Proof. First assume that α is not special. By Lemma 4.3 there exist $\xi < \alpha$ and a such that $\alpha = a\xi$. By Lemma 2.8 we may assume that $a < 2^n$.

Let b and $\lambda \in \Gamma$ be such that $\xi = b''\lambda$. Then $\alpha = a\xi = a(b''\lambda) = ab''a\lambda$. Let $a\lambda = \gamma$ and $c = [ab]_{n+1}$. We have $a < c$, $c''\gamma = ab''a\lambda = \alpha$, and by Lemma 2.8, $c < 2^n$.

Conversely, assume that the condition holds. Then $\alpha = c''\gamma = ab''a\lambda = a(b''\lambda)$. As $a < 2^n$, its critical point is below γ_n , hence $a\alpha > \alpha$ and so $b''\lambda < \alpha$. By Lemma 4.2, α is not special.

We not describe all Ω -ordinals between consecutive critical points:

4.5. Theorem. *Let $n > 0$. There exist a finite sequence*

$$a_1 = 2^n - 1 > a_2 > \cdots > a_{k_n}$$

of embeddings and a finite sequence

$$\gamma_{i_1} = \gamma_1, \dots, \gamma_{i_{k_n}}$$

of critical points such that

$$\gamma_n < a''_1 \gamma_{i_1} < \cdots < a''_{k_n} \gamma_{i_{k_n}} < \gamma_{n+1}$$

are all the Ω -ordinals between γ_n and γ_{n+1} , and for every $k = 1, \dots, k_n - 1$,

$$a_k'' \gamma_{i_k} = a_{k+1} \alpha$$

where α is the special ordinal below $\gamma_{i_{k+1}}$.

Proof. Let $a_1 = 2^n - 1$. By Corollary 2.7, $a''_1 \gamma_1$ is the least Ω -ordinal greater than γ_n (this is proved without using TH). By induction, let $k \geq 1$, $a_k = a$ and $\gamma_{i_k} = \gamma$. If $a''\gamma$ is special below γ_{n+1} we are done. Thus assume that $a''\gamma$ is not special, and so there exist a $\xi < a''\gamma$ and some x such that $x\xi = a''\gamma$.

Let α be the least ξ such that $x\xi = a''\gamma$ for some x . We claim that α is special: if not then $\alpha = y''\eta$ for some y and $\eta < \alpha$; then $(x \circ y)\eta = x(y\eta) = x\alpha = a''\gamma$, contradicting the minimality of α . Therefore there exists a special $\alpha < a''\gamma$ such that $c\alpha = a''\gamma$. By Corollary 2.9, there is such a c with the property that $c < 2^n$.

Let a_{k+1} be the largest $c < 2^n$ such that for some special α , $a''\gamma \leq c\alpha < \gamma_{n+1}$. First we note that by the induction hypothesis, it is impossible that $c \geq a$: this is clear for $k = 1$, and if $k > 1$, then this would contradict the fact that a_k is the largest $a < 2^n$ such that for some special ξ , $a''_{k-1} \gamma_{i_{k-1}} \leq a\xi < \gamma_{n+1}$. Hence $c < a_k$.

We conclude the proof by showing that $c\alpha = a''\gamma$. Thus assume that $c\alpha > a''\gamma$. There exist a b and some $\lambda \in \Gamma$ such that $a = b''\gamma$, and we have

$$c\alpha = c(b''\lambda) = cb''c\lambda = d''c\lambda$$

where $d = [cb]_{n+1}$. By Lemma 2.8 we have $c < d < 2^n$.

Let η be special below $c\lambda$. By Lemma 3.10, $d''c\lambda$ is the successor of $d\eta$, and so $d\eta \geq a''\gamma$. This contradicts the maximality of c .

We shall now address the question of *uniqueness* of the representation given by Theorem 4.5. If $a''\gamma = b''\delta$ and $\gamma, \delta \in \Gamma$ then, by the reason of cofinality, $\gamma = \delta$. The question is whether we can have $a''\gamma = b''\gamma$ when $a, b < 2^{n-1}$ and $a''\gamma < \gamma_{n+1}$. We prove the uniqueness of $a''\gamma$ under the assumption of the following *Uniqueness Hypothesis*:

4.6. The Uniqueness Hypothesis (UH). Let $a, b < 2^{n-1}$ and let $p_n(a) = p_n(b) = 2^k$. Let c be the least c such that γ_k is in the range of c and let $c\gamma_i = \gamma_k$. If $a\gamma_i = b\gamma_i$ and $A_n \vDash ac = bc$, then $a = b$.

We conjecture that (UH) holds in every A_n . The proof of Theorem 4.8 uses the following consequence of UH:

4.7. Lemma. Assume UH and let $a, b < 2^{n-1}$, $a \neq b$. If $a\gamma_k = b\gamma_k = \gamma_n$ and if c is the least c such that $\gamma_k \in \text{range}(c)$, then $A_n \vDash ac \neq bc$.

Proof. Let $a, b < 2^{n-1}$ and let c be least with $\gamma_k \in \text{range}(c)$; let $c\gamma_i = \gamma_k$. Assume that $A_n \vDash ac = bc$.

By TH, c is smaller than the threshold of either a or b in A_n and so $[ac]_n = [bc]_n < 2^{n-1}$. Since γ_n is in the range of both a and b , $[ac]_{n+1} = [bc]_{n+1} < 2^{n-1}$. Thus $\gamma_n = a(c\gamma_i) = ac(a\gamma_i) = [ac]_{n+1}(a\gamma_i) = [bc]_{n+1}(b\gamma_i)$, and it follows that $a\gamma_i = b\gamma_i$. By UH, $a = b$.

4.8. Theorem. Assume UH. If $a, b < 2^n$ and $\gamma_n < a''\gamma = b''\gamma < \gamma_{n+1}$ then $a = b$.

Proof. We proceed by induction on n and, for a given n , by downward induction on $a < 2^n$. If $a = 2^n - 1$ then $\gamma = \gamma_1$, and because $\gamma_1 = \gamma_0^+$, Lemma 3.10 implies that if $b''\gamma_1 = a''\gamma_1$ then $b\gamma_0 = a\gamma_0 = \gamma_n$, and by Lemma 2.5 we have $b = 2^n - 1$.

Now let $b < a < 2^n - 1$ be such that $\gamma_n < a''\gamma = b''\gamma < \gamma_{n+1}$. By Corollary 3.4, $a\gamma = b\gamma = \gamma_{n+1}$. Let $c''\delta$ be the special ordinal below γ . By Theorem 4.5 and the induction hypothesis on n , c is the least c such that $\gamma \in \text{range}(c)$, and so by Lemma 4.7, $A_{n+1} \vDash ac \neq bc$. By TH and by Lemma 2.3 we have $[ac]_{n+1} < 2^n$ and $[bc]_{n+1} < 2^n$. By Lemma 3.10, $a''\gamma = (a(c''\delta))^+$, and it follows that $[ac]_{n+1}''a\delta = [bc]_{n+1}''b\delta$. This contradicts the induction hypothesis on a , since $a < [ac]_{n+1} < 2^n$.

5. The conjectures TH and UH

The main result of our paper depends on the conjecture TH for finite LD algebras. In this Section we discuss the numerical evidence for the conjecture as well as related conjectures.

The statement TH is formulated in terms of the algebras A_n . In principle, one can verify the validity of the statement TH for any particular value of n . In practice, the number of calculations for A_n grows exponentially, so we can't really expect to verify TH for too large values of n .

In our experiments we use a sophisticated software developed by Randall Dougherty. Using various unpublished results about the algebras A_n , Dougherty devised an algorithm that can compute the binary operation in the algebras A_n for all $n \leq 48$. We used the code [2] with the author's permission. I am grateful to the Computer Science Department of Penn State for letting me use their equipment.

5.1. Experimental result. TH is true for all $n \leq 30$.

The proof of Lemma 3.2 that uses TH uses only the instance of TH when γ_{n+1} is in the range of the embedding a . Thus we can formulate a weaker hypothesis that is still sufficient for the results of our paper. (We also use $n - 1$ instead of n .)

5.2. The weak threshold hypothesis (WTH). Let $a < 2^{n-1} - 1$ be such that $a\gamma_k = \gamma_n$. If $c + 1$ is threshold of a in A_n then γ_k is in the range of c .

WTH can be reformulated in several equivalent ways. To see that, we first observe the following:

5.3. Lemma. *Let $a < 2^{n-1} - 1$ be such that $\gamma_n \in \text{range}(a)$ and let $c + 1 = t_n(a)$. Then*

$$\begin{aligned} [ac]_{n+1} &= [ac]_n = [ac]_{n-1}, \\ [a \circ c]_{n+1} &= [a \circ c]_n. \end{aligned}$$

Proof. As $c + 1 = t_n(a)$, we have $[ac]_n < 2^{n-1} \leq [a(c+1)]_n$. Thus $[ac]_n = [ac]_{n-1}$. Since $\gamma_n \in \text{range}(a)$, we have $t_{n+1}(a) = p_n(a) > c + 1$, and so $[ac]_{n+1} = [ac]_n$, and $[a \circ c]_{n+1} = [a(c+1) - 1]_{n+1} = [a(c+1) - 1]_n = [a \circ c]_n$.

5.4. Lemma. *Let $a < 2^{n-1} - 1$, $a\gamma_k = \gamma_n$ and $c + 1 = t_n(a)$. Consider the following statements:*

- (i) $\gamma_k \in \text{range}(c)$
- (ii) $\gamma_n \in \text{range}([ac]_n)$
- (iii) $\gamma_n \in \text{range}([ac]_{n-1})$
- (iv) $\gamma_n \in \text{range}([a \circ c]_n)$
- (v) $\gamma_{n-1} \in \text{range}([a \circ c]_{n-1})$

The statements (i), (iv) and (v) are equivalent and imply (ii) and (iii) that are also equivalent; under Laver's conjecture all five statements are equivalent.

Proof. (ii) and (iii) are equivalent by Lemma 5.3. To show that (i) implies (ii), let $c\delta = \gamma_k$; we have

$$\gamma_n = a\gamma_k = a(c\delta) = ac(a\delta) = [ac]_{n+1}(a\delta) = [ac]_n(a\delta).$$

Conversely, if $\gamma_n \in \text{range}([ac]_n) = \text{range}([ac]_{n+1})$ then $a\gamma_k = \gamma_n \in \text{range}(ac)$. By elementarity, $\gamma_k = c\alpha$ for some ordinal α , and by Laver's conjecture $\gamma_k \in \text{range}(c)$. (See the remarks following Definition 3.1.)

To show the equivalence of (i) and (iv), let first $c\delta = \gamma_k$; we have

$$\gamma_n = a\gamma_k = a(c\delta) = (a \circ c)\delta = [a \circ c]_{n+1}\delta = [a \circ c]_n\delta.$$

Conversely, if $a\gamma_k = \gamma_n = [a \circ c]_n\delta = [a \circ c]_{n+1}\delta = (a \circ c)\delta = a(c\delta)$, then $\gamma_k = c\delta$.

Finally, to show the equivalence of (iv) and (v), we first observe that if $[a(c+1)]_n = 2^{n-1}$, we have $[a \circ c]_{n-1} = [a \circ c]_n = 2^{n-1} - 1$ and both γ_{n-1} and γ_n are in the range of $2^{n-1} - 1$.

If $[a(c+1)]_n > 2^{n-1}$, then

$$[a \circ c]_n = [a \circ c]_{n-1} + 2^{n-1} = 2^{n-1} *_{n-1} [a \circ c]_{n-1}$$

and because $2^{n-1}\gamma_{n-1} = \gamma_n$, we have $\gamma_{n-1} \in \text{range}([a \circ c]_{n-1})$ if and only if $\gamma_n \in \text{range}([a \circ c]_n)$: Let $u = [a \circ c]_{n-1}$ and $v = [a \circ c]_n$. If $u\delta = \gamma_{n-1}$ then $v\delta = 2^{n-1}u(2^{n-1}\delta) = 2^{n-1}(u\delta) = \gamma_n$. Conversely, if $v\delta = \gamma_n$ then $\delta < \gamma_{n-1}$, and $\gamma_n = 2^{n-1}(u\delta)$, hence $u\delta = \gamma_{n-1}$.

An inspection of the arguments in the proof of Theorem 3.3 will confirm that (WTH1) below suffices in place of (WTH) to prove the theorem, and consequently Laver's conjecture. Thus it follows from Lemma 5.4 that (WTH) is equivalent to any of the following three statements:

5.5 .

(WTH1) If $a < 2^{n-1} - 1$, $\gamma_n \in \text{range}(a)$ and $c + 1 = t_n(a)$ then $\gamma_n \in \text{range}([ac]_n)$.

(WTH2) If $a < 2^{n-1} - 1$, $\gamma_n \in \text{range}(a)$ and $c + 1 = t_n(a)$ then $\gamma_n \in \text{range}([a \circ c]_n)$.

(WTH3) If $a < 2^{n-1} - 1$, $\gamma_n \in \text{range}(a)$ and $c + 1 = t_n(a)$ then $\gamma_{n-1} \in \text{range}([a \circ c]_{n-1})$.

We remark that the assumption that $\gamma_n \in \text{range}(a)$ is necessary in each (WTH1), (WTH2) and (WTH3):

5.6. Example. (i) Let $n = 5$, $a = 5$; then $c = 1$, $ac = 6$ and γ_5 is not in the range of 6.

(ii) Let $n = 10$, $a = 34$; then $c = 4$, $[a \circ c]_9 = 242$ and γ_9 is not in the range of 242.

When investigating the weak threshold hypothesis, we notice that in most cases it is true for trivial reasons, namely because if γ_n is in the range of a then γ_{n-1} is in the range of a as well. This leads to the following conjecture.

5.7. The Twin Hypothesis. If n is odd, $a < 2^{n-1}$ and $\gamma_n \in \text{range}(a)$, then $\gamma_{n-1} \in \text{range}(a)$.

If a satisfies the Twin Hypothesis then it satisfies WTH: this is because $t_n(a) = 2^{k-1}$ where $a\gamma_k = \gamma_n$, and $\gamma_k \in \text{range}(2^{k-1} - 1)$.

5.8. Experimental result. The Twin Hypothesis is true for all odd $n \leq 31$.

Now we turn our attention to the Uniqueness Hypothesis. When we apply (UH) (in Lemma 4.7) we only use a weaker version:

5.9. If $a, b < 2^{n-1}$ are such that $a\gamma_k = b\gamma_k = \gamma_n$ and if c is the least c such that $\gamma_k \in \text{range}(c)$, then $[ac]_n = [bc]_n$ implies $a = b$.

We have verified both UH and 5.9 for a large number of embeddings:

5.10. Experimental result. UH is true for all $n \leq 17$; 5.9 is true for all $n \leq 25$.

As a final remark, we observe that the 5.9 does not necessarily hold when c is not the least c :

5.11. Example. Let $n = 9$, $a = 48$, $b = 192$ and $c = 51$. Then $a\gamma_7 = b\gamma_7 = \gamma_9$, $c\gamma_3 = \gamma_7$ and $[ac]_9 = [bc]_9 = 243$.

6. Appendix. Ordinals below γ_{12} γ_0 γ_1 $1''\gamma_1$ γ_2 $3''\gamma_1$ γ_3 $7''\gamma_1$ $4''\gamma_3$ $3''\gamma_2$ $2''\gamma_2$ $1''\gamma_2$ γ_4 $15''\gamma_1$ $12''\gamma_3$ $3''\gamma_3$ γ_5 $31''\gamma_1$ $28''\gamma_3$ $19''\gamma_3$ $16''\gamma_5$ $15''\gamma_2$ $2''\gamma_3$ γ_6 $63''\gamma_1$ $60''\gamma_3$ $51''\gamma_3$ $48''\gamma_5$ $15''\gamma_3$ γ_7 $127''\gamma_1$ $124''\gamma_3$ $115''\gamma_3$ $112''\gamma_5$ $79''\gamma_3$ $64''\gamma_7$ $63''\gamma_2$ $50''\gamma_3$ $48''\gamma_6$ $47''\gamma_2$

34" γ_3
32" γ_6
31" γ_2
18" γ_3
16" γ_6
15" γ_4
14" γ_2
1" γ_3
 γ_8
255" γ_1
252" γ_3
243" γ_3
240" γ_5
207" γ_3
192" γ_7
63" γ_3
48" γ_7
15" γ_5
 γ_9
511" γ_1
508" γ_3
499" γ_3
496" γ_5
463" γ_3
448" γ_7
319" γ_3
304" γ_7
271" γ_5
256" γ_9
255" γ_2
242" γ_3
240" γ_6
47" γ_3
32" γ_7
15" γ_6
 γ_{10}
1023" γ_1
1020" γ_3
1011" γ_3
1008" γ_5

975" γ_3
960" γ_7
831" γ_3
816" γ_7
783" γ_5
768" γ_9
255" γ_3
240" γ_7
15" γ_7
 γ_{11}
2047" γ_1
2044" γ_3
2035" γ_3
2032" γ_5
1999" γ_3
1984" γ_7
1855" γ_3
1840" γ_7
1807" γ_5
1792" γ_9
1279" γ_3
1264" γ_7
1039" γ_7
1024" γ_{11}
1023" γ_2
1010" γ_3
1008" γ_6
815" γ_3
800" γ_7
783" γ_6
768" γ_{10}
767" γ_2
754" γ_3
752" γ_6
559" γ_3
544" γ_7
527" γ_6
512" γ_{10}
511" γ_2
498" γ_3
496" γ_6
303" γ_3
288" γ_7
271" γ_6
256" γ_{10}
255" γ_4
14" γ_3

REFERENCES

1. R. Dougherty, *Critical points in an algebra of elementary embeddings*, *Annals of Pure and Applied Logic* **65** (1993), 211-241.
2. _____, *unpublished*.
3. R. Dougherty and T. Jech, *Finite left-distributive algebras and embedding algebras*, *Advances in Mathematics*, to appear.
4. A. Drápal, *Homomorphisms of primitive left distributive groupoids*, *Comm. Algebra*.
5. K. Kunen, *Elementary embeddings and infinitary combinatorics*, *J. Symb. Logic* **36** (1971), 407-413.
6. R. Laver, *The left-distributive law and the freeness of an algebra of elementary embeddings*, *Advances in Mathematics* **91** (1992), 209-231.
7. _____, *On the algebra of elementary embeddings of a rank into itself*, *Advances in Mathematics*, to appear.

DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802

E-mail: jech@math.psu.edu