p_n-sequences of Algebras with One Fundamental Operation

Keith A. Kearnes and Adam W. Marczak

Abstract. We show that if $(p_0, p_1, \ldots)$ is the p_n-sequence of a nontrivial algebra with one fundamental operation, then $p_1 \geq p_0$. Moreover, if $2 < p_0 < \aleph_0$, then $p_1 > 2p_0$.

1. Introduction

The *p_n-sequence* of an algebra $\mathbf{A}$ is the sequence of cardinals $p_n(\mathbf{A}) := (p_0, p_1, \ldots)$ where p_n is the number of distinct essentially n-ary term operations of $\mathbf{A}$ if $n > 0$, and p_0 is the number of distinct constant unary term operations. In a countable language, the cardinals in the sequence must come from $\{0, 1, \ldots, \aleph_0\}$. If $\mathbf{A}$ is nontrivial, then the term operation $id(x) = x$ is essentially unary, so $p_1 > 0$. Conversely, it is known that almost any sequence of cardinals from $\{0, 1, \ldots, \aleph_0\}$ satisfying $p_1 > 0$ is the p_n-sequence of a nontrivial algebra in a countable language. For example, one argument in [1] shows that any sequence $(p_0, p_1, \ldots)$ of cardinals from this set with $p_0, p_1 > 0$ is the p_n-sequence of some algebra in a countable language. The same argument shows that if the initial segment $(p_0, p_1, \ldots, p_k)$ consists of finite cardinals, and $p_0, p_1 > 0$, then this is the initial segment of the p_n-sequence of a finite algebra in a finite language.

The situation is different if one restricts to algebras defined with only one fundamental operation. Proposition 1 of [3] shows that if $(p_0, 2)$ is the initial segment of the p_n-sequence of a groupoid, then $p_0 \leq 2$. This led the second author to conjecture that, more generally, if (p_0, p_1) is an initial segment of the p_n-sequence of a groupoid, then $p_0 \leq p_1$. We prove this conjecture here, not only for groupoids but for any nontrivial algebra defined with a single fundamental operation. We show further that $2p_0 < p_1$ when $2 < p_0 < \aleph_0$.

Although we focus exclusively on the relationship between p_0 and p_1 in this note, our work shows that there is an absolute constant $c > 0$ such that when $\mathbf{A}$ has one fundamental operation and $2 \leq p_0(\mathbf{A}) < \aleph_0$ then $p_n(\mathbf{A}) \geq 2^{2^{cn}}$ for all $n > 1$.

2. The Proofs

Let $\mathbf{A}$ be a nontrivial algebra with one fundamental operation whose p_n-sequence is $(p_0, p_1, \ldots)$. We are interested in identifying restrictions on the initial segment (p_0, p_1), so we begin by showing that there is no restriction on p_1 if $p_0 = 0$ or 1

1991 *Mathematics Subject Classification*: 20N15.
Key words and phrases: p_n-sequence, groupoid, primal algebra.

(other then the restriction $p_1 > 0$ mentioned in the introduction), and there is no restriction on p_0 if $p_1 = \aleph_0$.

If $p_0 = 0$ and $p_1 \in \{1, \ldots, \aleph_0\}$, then (p_0, p_1) is representable as the initial segment of the p_n-sequence of a unary algebra $\langle A; f\rangle$ where $|A| = p_1$ and f is a (possibly infinite) cyclic permutation of A. Similarly, if $p_0 = 1$ and $p_1 \in \{1, \ldots, \aleph_0\}$, then (p_0, p_1) is representable as the initial segment of the p_n-sequence of a unary algebra $\langle A; f\rangle$ where A is an inital segment of $\omega = \{0, 1, \ldots\}$ of appropriate length and $f(x) = \max(0, x - 1)$.

Now assume that $(p_0, p_1) = (p_0, \aleph_0)$ with $p_0 > 1$. Let $\mathbf{B} = \langle B; f\rangle$ be an algebra with $|B| = p_0$ and f a binary operation on B such $f(x, x)$ is a cyclic permutation of B, and $f(x, y) = 0$ for some fixed $0 \in B$ whenever $x \neq y$. The unary term operation $f(x, f(x, x)) = 0$ is constant, so applying $f(x, x)$ to it repeatedly one generates exactly $|B| = p_0$ constants. $\mathbf{B}$ cannot have more than $|B|$ constants, so it has exactly $|B| = p_0$ constant unary term operations. Now $\mathbf{C} := \langle \mathbb{Z}; x - y\rangle$ has exactly one constant unary term operation and infinitely many nonconstant unary term operations, so $\mathbf{A} := \mathbf{B} \times \mathbf{C}$ has $|B| = p_0$ constant unary term operations and $\aleph_0$ nonconstant unary term operations. This shows that $(p_0, \aleph_0)$ is representable.

So, henceforth we need to consider only the cases where $p_0 \notin \{0, 1\}$ and $p_1 \neq \aleph_0$. Notice that if $\mathbf{A}^\circ$ is the subalgebra of $\mathbf{A}$ whose elements are represented by constant term operations, then $p_0(\mathbf{A}) = p_0(\mathbf{A}^\circ)$ and $p_1(\mathbf{A}) \geq p_1(\mathbf{A}^\circ)$. Therefore, to establish a lower bound on p_1 in terms of p_0 (for example $p_1 \geq p_0$) it suffices to consider only those cases where $\mathbf{A} = \mathbf{A}^\circ$. This suggests the following definition.

Definition 2.1. A nontrivial algebra $\mathbf{A}$ with p_n-sequence $(p_0, p_1, \ldots)$ is *relevant* if

(1) $\mathbf{A} = \langle A; f\rangle$ has one fundamental operation,
(2) every element of $\mathbf{A}$ is represented by a constant term operation,
(3) p_1 is finite and $p_0 \geq 2$.

The following terminology will also be used.

Definition 2.2. The *cosocle* of an algebra $\mathbf{A}$ is the quotient $\mathbf{A}/\theta$ where θ is the intersection of maximal congruences of $\mathbf{A}$.

Before proceeding to the main theorem we record some properties of relevant algebras.

Lemma 2.3. *If $\mathbf{A} = \langle A; f\rangle$ is relevant, then the following hold.*

(i) *Every nontrivial quotient $\mathbf{A}/\theta$ of $\mathbf{A}$ is relevant.*
(ii) *Every polynomial operation of $\mathbf{A}$ is a term operation.*
(iii) *$\mathbf{A}$ has no nonempty proper subuniverse and no nonidentity automorphism.*
(iv) *The polynomial $\delta(x) := f(x, x, \ldots, x)$ has no fixed points.*
(v) *Any class of a principal congruence has at most $p_1 + 1$ elements.*
(vi) *$\mathbf{A}$ is finite.*
(vii) *The cosocle of $\mathbf{A}$ is an independent product of primal algebras.*

Proof. Item (i) follows because each of Conditions (1), (2) and (3) of Definition 2.1 are preserved when passing to nontrivial quotients. Item (ii) holds because of Condition (2): every constant operation is a term operation. For item (iii), any nonempty subuniverse must contain all elements represented by constant term operations, and any automorphism must fix all elements represented by constant term operations. For item (iv), if $a \in A$ is a fixed point of $\delta(x) = f(x, x, \ldots, x)$, then $\{a\}$ is a nonempty proper subuniverse, contrary to (iii).

If $\mathbf{A}$ is a relevant algebra and $X \subseteq A \times A$, let $G(X)$ be the directed graph whose vertex set is A and whose edge set is

$$E = E(X) := \{(q(a), q(b)) \mid q \in \mathrm{Pol}_1(\mathbf{A}), (a, b) \in X\}.$$

Here and elsewhere $\mathrm{Pol}_1(\mathbf{A})$ denotes the set of unary polynomials of $\mathbf{A}$. If X consists of a single pair, write $G(a, b)$ and $E(a, b)$ instead of $G(X)$ and $E(X)$. The edge set $E = E(X)$ is the disjoint union of a subset $L \subseteq E$ of *loops* (pairs of the form (x, x)) and subset $N \subseteq E$ of *nonloops* (pairs of the form (x, y), $x \neq y$). Two elements of A are considered connected in $G(X)$ if there is an undirected path from one to the other.

Now we consider only the case $X = \{(a, b)\}$. A nonloop $(q(a), q(b))$ in $E(a, b)$ satisfies $q(a) \neq q(b)$, hence each nonloop in $E(a, b)$ is generated from (a, b) by a nonconstant unary polynomial q. Moreover, distinct nonloops are generated from (a, b) by distinct polynomials. Thus the number of nonloops in $E(a, b)$ is not greater than the number of distinct nonconstant unary polynomials of $\mathbf{A}$, which is p_1 according to item (ii) of this lemma. It follows from Maltsev's congruence generation theorem that the connected components of $G(a, b)$ are the classes of the congruence generated by (a, b), denoted hereafter by $\mathrm{Cg}(a, b)$. By elementary graph theory, the size of a component C is at most one more than the number of nonloop edges in C, which we have shown is at most p_1. Thus, the size of any class C of $\mathrm{Cg}(a, b)$ is at most $p_1 + 1$, establishing item (v) of this lemma.

Choose $a \in A$ and let $\theta = \mathrm{Cg}(a, \delta(a))$. If $\theta \neq A \times A$, then $\mathbf{A}/\theta$ is a relevant algebra according to item (i), yet $\overline{a} := a/\theta$ is a fixed point of δ in $\mathbf{A}/\theta$ contrary to item (iv). Hence $\theta = A \times A$. Now, by item (v), the unique θ-class A has size at most $p_1 + 1$, proving item (vi): $\mathbf{A}$ is finite. (Indeed, this proves that $p_0 = |A| \leq p_1 + 1$.)

To prove item (vii), let ψ be a maximal congruence of $\mathbf{A}$. By items (i), (iii) and (vi), $\mathbf{A}/\psi$ is finite, simple, and has no proper nonempty subuniverse or nonidentity automorphism. Theorem 1 of [5] proves that an algebra with one fundamental operation that has these properties is primal. If ψ' is a different maximal congruence, then $\mathbf{A}/\psi \not\cong \mathbf{A}/\psi'$. For if $(a, b) \in \psi - \psi'$, then the constant term operations naming a and b are equal in $\mathbf{A}/\psi$ but not in $\mathbf{A}/\psi'$, and this is an identity satisfied by $\mathbf{A}/\psi$ and not $\mathbf{A}/\psi'$. Thus, if θ is the intersection of maximal congruences of $\mathbf{A}$, then $\mathbf{A}/\theta$ is a finite subdirect product of nonisomorphic primal algebras. By the main result of [4], any finite set of nonisomorphic primal algebras in the same language is independent, hence any finite subdirect product of such algebras is an independent product. □

Now we can prove the main theorem.

Theorem 2.4. *If $(p_0, p_1, \ldots)$ is the p_n-sequence of an algebra with one fundamental operation, then $p_1 \geq p_0$; moreover $p_1 > 2p_0$ if $2 < p_0 < \aleph_0$.*

Proof. It suffices to prove the theorem for relevant algebras only. If $\mathbf{A}$ is such and $2 = p_0 = |A|$, then Lemma 2.3 (vi) implies that $\mathbf{A}$ is a 2-element primal algebra. Hence $p_1 = 2^{2^1} - 2^{2^0} = 2 \geq p_0$. To finish the proof it suffices to assume that $p_0 = |A| > 2$ and show that $p_1 > 2p_0$.

Let $\theta_1, \ldots, \theta_k$ be the maximal congruences of $\mathbf{A}$. Since $\mathbf{A}/\theta_i$ is primal, the tame congruence-theoretic type of the prime quotient $\langle\theta_i, 1\rangle$ is $\mathbf{3}$ for each i (cf. [2]). Choose one $\langle\theta_i, 1\rangle$-minimal set U_i for each i. Each U_i has empty tail, since each θ_i is maximal. Since the type is $\mathbf{3}$ this means that $U_i = \{0_i, 1_i\}$ has 2 elements, and the induced algebra $\mathbf{A}|_{U_i}$ is polynomially equivalent to a Boolean algebra. Tame congruence theory guarantees the existence of idempotent polynomials $e_i \in \mathrm{Pol}_1(\mathbf{A})$ such that $e_i(A) = U_i$ for each i, as well as Boolean complementations $c_i \in \mathrm{Pol}_1(\mathbf{A})$, $c_i \circ e_i = c_i$, $c_i(0_i) = 1_i$, and $c_i(1_i) = 0_i$. Let $X = \{(0_i, 1_i)\ 1 \leq i \leq k\}$, and let $G = G(X) = \langle A; E\rangle$ be the graph defined in the proof of Lemma 2.3.

Claim 2.5. *$G(X)$ is connected.*

If θ_i is a maximal congruence, then it follows from the definition of a $\langle\theta_i, 1\rangle$-minimal set that $(0_i, 1_i) \notin \theta_i$. But $(0_i, 1_i) \in \mathrm{Cg}(X)$, so $\mathrm{Cg}(X) \not\leq \theta_i$ for all i. Hence $\mathrm{Cg}(X) = A \times A$. The claim now follows from the fact, noted in the proof of Lemma 2.3 (v), that the connected components of $G(X)$ are the $\mathrm{Cg}(X)$-classes.

Claim 2.6. *$(u, v) \in E$ if and only if $(v, u) \in E$.*

If $(u, v) = (q(0_i), q(1_i))$ for some $q \in \mathrm{Pol}_1(\mathbf{A})$ and some $(0_i, 1_i) \in X$, then $(v, u) = (q \circ c_i(0_i), q \circ c_i(1_i)) \in E$.

Claim 2.7. *If $(u, v) \in E$ is a nonloop, then there exists $q \in \mathrm{Pol}_1(\mathbf{A})$ and $1 \leq i \leq k$ such that*

1. *$(u, v) = (q(0_i), q(1_i))$,*
2. *$|q(A)| = 2$, and*
3. *$\theta_i \subseteq \ker(q)$ for some i.*

By the definition of E, if $(u, v) \in E$, there exists $1 \leq i \leq k$ and a polynomial $q' \in \mathrm{Pol}_1(\mathbf{A})$ such that $(u, v) = (q'(0_i), q'(1_i))$. Let $q := q' \circ e_i$. Then

$$(q(0_i), q(1_i)) = (q' \circ e_i(0_i), q' \circ e_i(1_i)) = (q'(0_i), q'(1_i)) = (u, v),$$

since e_i is idempotent with image $U_i = \{0_i, 1_i\}$. This shows that (1) holds for this i and q. Since $\{u, v\} \subseteq q(A) = q'(e_i(A)) \subseteq \{u, v\}$ and $u \neq v$ we get (2): $|q(A)| = 2$. Finally, since $q = q' \circ e_i$ and both q and e_i have range of size 2, it follows that $\ker(q) = \ker(e_i)$. To set up a contradiction, assume that $(a, b) \in \theta_i - \ker(e_i)$. Then $\{e_i(a), e_i(b)\}$ is a 2-element subset of $e_i(A) = \{0_i, 1_i\}$ consisting of θ_i-related elements. But this contradicts the definition of a $\langle\theta_i, 1\rangle$-minimal set. (We must have $(0_i, 1_i) \notin \theta_i$.) This contradiction yields (3): $\theta_i \subseteq \ker(e_i) = \ker(q)$.

Claim 2.8. *For each nonloop $e \in E$ choose $q_e \in \mathrm{Pol}_1(\mathbf{A})$ satisfying (1), (2) and (3) of Claim 2.7. The assignment $e \mapsto q_e$ is an injective mapping from the set of nonloops to the set of unary polynomials whose range has size 2. Consequently the number of nonloops of G is strictly less than p_1.*

By Lemma 5.15 (2) of [2], the fact that $\text{typ}(\theta_i, 1) = \mathbf{3}$ guarantees that the congruence $\rho_i := \text{Cg}(0_i, 1_i)$ is the smallest $\rho \in \text{Con}(\mathbf{A})$ for which $\rho \vee \theta_i = 1$. If θ_j is a maximal congruence different from θ_i, then $\theta_j \vee \theta_i = 1$, implying that $(0_i, 1_i) \in \rho_i \leq \theta_j$.

Now suppose that $d, e \in E$ are nonloops, and q_d and q_e satisfy Conditions (1), (2) and (3) of Claim 2.7. If $q_d = q_e =: q$, then for some i and j we must have $(q(0_i), q(1_i)) = d$ and $(q(0_j), q(1_j)) = e$ (Condition (1)). If $i \neq j$, then $(0_i, 1_i) \in \theta_j \leq \ker(q)$, according to Condition (3), and this contradicts the fact that $(q(0_i), q(1_i)) = d$ is a nonloop. Hence $i = j$. But then $d = (q(0_i), q(1_i)) = (q(0_j), q(1_j)) = e$; i.e., $q_d = q_e$ implies that $d = e$.

This proves that the size of the set of nonloops $e \in E$ is not greater than the size of the set of $q_e \in \text{Pol}_1(\mathbf{A})$. Each q_e is nonconstant, by Condition (2) of Claim 2.7, so the set of q_e's is not larger than p_1. Indeed, the number of the q_e's must be strictly less than p_1, since $id \in \text{Pol}_1(\mathbf{A})$ is nonconstant and cannot equal any q_e. (The range of id has size $|A|$, not 2.)

Let $\overline{G} = \langle A; \overline{E} \rangle$ be the undirected graph associated to $G = \langle A; E \rangle$. $\overline{G}$ differs from G in that we have discarded all loops and replaced each nonloop (u, v) by the corresponding doubleton $\{u, v\}$. The purpose for this is to eliminate the obvious 1-vertex cycles guaranteed by the loops and 2-vertex cycles guaranteed by Claim 2.6. Yet, as we now prove, at least one cycle still remains.

Claim 2.9. *$\overline{G}$ has a cycle.*

We assume to the contrary that $\overline{G}$ has no cycle. It is connected, by Claim 2.5, so it is a tree.

Because of the way the edge relation of G is defined, any $q \in \text{Pol}_1(\mathbf{A})$ is an endomorphism $q \colon G \to G$ of directed graphs. We will apply this observation to powers of $\delta(x) = f(x, \dots, x) \in \text{Pol}_1(\mathbf{A})$. Some iterate δ^k of δ is idempotent, and δ is a permutation of the set $\delta^k(A)$. Since G is connected and δ^k is a graph endomorphism, the graph induced on the image $B := \delta^k(A)$ is connected. The undirected graph $\overline{B}$ with vertex set B is a subgraph of $\overline{G}$, which is an acyclic graph, so $\overline{B}$ is also acyclic and therefore is a tree.

The exponent of δ^k was chosen so that δ is a permutation of B. Since δ is a polynomial, it is an automorphism of the tree $\overline{B}$.

An automorphism of a (finite, nonempty, undirected) tree has fixed vertex or a fixed edge. To see this, suppose not and let $\alpha \colon T \to T$ be a counterexample with $|T|$ minimal. T cannot have a single vertex only (else it would be a fixed vertex of α), and T cannot have only two vertices (else the edge connecting them would be fixed by α). This implies that T has both leaves and nonleaves. If O is an α-orbit consisting of leaves, then $T - O$ is a smaller nonempty tree, and α restricts to an automorphism of $T - O$. By the minimality of $|T|$, the tree $T - O$ has a vertex or edge fixed by α, which is also a fixed vertex or edge of T.

In Lemma 2.3 we showed that δ has no fixed points in A. Since it is an automorphism of $\overline{B}$ it follows from the previous paragraph that some edge $\{u, v\}$ of $\overline{B}$ is fixed by δ, i.e. $\delta(u) = v$ and $\delta(v) = u$. Since $|\{u, v\}| = 2 < |A|$, the set

$\{u, v\}$ is not a subuniverse. Reordering the variables of the basic operation if necessary, we may assume that $f(u, u, \ldots, u, v, \ldots, v, v) = w \notin \{u, v\}$. According to Claim 2.7, there exist $q \in \mathrm{Pol}_1(\mathbf{A})$ and $1 \leq i \leq k$ such that $(u, v) = (q(0_i), q(1_i))$. Let $r(x) = f(u, u, \ldots, u, x, \ldots, x, x)$ and $s(x) = f(x, x, \ldots, x, v, \ldots, v, v)$. Then u, v and w are distinct, $(u, v) \in E$,

$$(v, w) = (r(u), r(v)) = (r \circ q(0_i), r \circ q(1_i)) \in E,$$

and

$$(w, u) = (s(u), s(v)) = (s \circ q(0_i), s \circ q(1_i)) \in E,$$

so there is a cycle in G involving u, v and w, hence also one in $\overline{G}$.

Now we prove the theorem. Since the undirected graph $\overline{G}$ has $|A| = p_0$ vertices, is connected, and has a cycle, it follows that $\overline{G}$ has at least p_0 edges. But each undirected edge in $\overline{G}$ corresponds to two nonloops of G, according to Claim 2.6. Thus, the number of nonloops in G is at least $2p_0$ and, by the last statement in Claim 2.8, the number of nonloops is strictly less than p_1. This proves that $2p_0 < p_1$. □

In the introduction we claimed that there is an absolute constant $c > 0$ such that when $\mathbf{A}$ has one fundamental operation and $2 \leq p_0(\mathbf{A}) < \aleph_0$ then $p_n(\mathbf{A}) \geq 2^{2^{cn}}$ for all $n > 1$. To establish this it suffices to consider only the case where $\mathbf{A}$ is relevant. Now, if θ is a maximal congruence of $\mathbf{A}$, then there is a $c > 0$ such that $p_n(\mathbf{A}) \geq p_n(\mathbf{A}/\theta) \geq 2^{2^{cn}}$ for all $n > 1$ because $\mathbf{A}/\theta$ is primal. The value of c that works when $|A| = 2$ also works for all larger $\mathbf{A}$, so this c is absolute.

If $\mathbf{A}$ is an independent product of primal algebras, then $\mathbf{A}$ is term equivalent to an algebra with one fundamental operation. If all direct factors of $\mathbf{A}$ have size 2, then $p_1 = p_0(p_0 - 1)$. As we have not found an example of an algebra with one fundamental operation which fails to satisfy $p_1 \geq p_0(p_0 - 1)$, we speculate that this inequality may be closer to the truth than the inequalities established in Theorem 2.4. In the case where $\mathbf{A} = \mathbf{A}^\circ$ and the cosocle of $\mathbf{A}$ is simple, it may be that the graph $G(X)$ defined in the proof of Lemma 2.3 is a complete directed graph. If this is the case, then $p_1 \geq p_0(p_0 - 1)$ holds simply because p_1 exceeds the number $p_0(p_0 - 1)$ of nonloops in $G(X)$. But $G(X)$ is not complete when the cosocle is not simple, so a proof that $p_1 \geq p_0(p_0 - 1)$ holds for any algebra with one fundamental operation (if this inequality is indeed true) will no doubt require estimates on the number of unary polynomials with range of size greater than 2.

References

[1] Grätzer, G.; Płonka, J.; Sekanina, A. *On the number of polynomials of a universal algebra. I.* Colloq. Math. **22** (1970), 9–11.

[2] Hobby, D.; McKenzie, R. *The structure of finite algebras.* Contemporary Mathematics, **76** American Mathematical Society, Providence, RI, 1988.

[3] Marczak, A. W. *A combinatorial characterization of Boolean algebras.* Algebra Universalis **41** (1999), no. 2, 143–150.

[4] O'Keefe, Edward S. *On the independence of primal algebras.* Math. Z. **73** (1960), 79–94.

[5] Rousseau, G. *Completeness in finite algebras with a single operation.* Proc. Amer. Math. Soc. **18** 1967 1009–1013.

(Keith A. Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA
E-mail address: kearnes@euclid.colorado.edu

(Adam W. Marczak) Institute of Mathematics and Computer Sciences, Wrocław University of Technology, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
E-mail address: amarczak@pwr.wroc.pl