Erhard Aichinger · Peter Mayr · Ralph McKenzie

On the number of finite algebraic structures

Received December 6, 2010 and in revised form July 12, 2012

Abstract. We prove that every clone of operations on a finite set $A$, if it contains a Malcev operation, is finitely related—i.e., identical with the clone of all operations respecting $R$ for some finitary relation $R$ over $A$. It follows that for a fixed finite set $A$, the set of all such Malcev clones is countable. This completes the solution of a problem that was first formulated in 1980, or earlier: how many Malcev clones can finite sets support? More generally, we prove that every finite algebra with few subpowers has a finitely related clone of term operations. Hence modulo term equivalence and a renaming of the elements, there are only countably many finite algebras with few subpowers, and thus only countably many finite algebras with a Malcev term.

Keywords. Malcev conditions, few subpowers, term equivalence, clones, relations

1. Introduction

An algebraic structure (or algebra, for short) is usually represented as a nonvoid set together with a set of finitary operations on it. In the present paper, we contribute to the following question: how many essentially different finite algebraic structures exist? Clearly, on a finite set of size at least two, there are countably many finitary operations, and hence there are continuum many ways to choose a set of basic operations. However, many of these algebras are equivalent in the sense that the same functions can be composed from their basic operations; these compositions are called the term functions of the algebra. Two algebras are term equivalent if they have the same set of term functions. The Boolean algebra $\langle B, \land, \lor, \neg \rangle$ and its counterpart, the Boolean ring $\langle B, +, \cdot, 1 \rangle$, are examples of term equivalent algebras. Many structural properties of an algebra, like its subalgebras, congruence relations, automorphisms, etc., depend on its term functions rather than on the particular choice of basic operations. Hence we are motivated to classify algebras modulo term equivalence. In 1941 E. Post [Pos41] proved that there are only countably many term
inequivalent algebras of size two (modulo renaming of the elements), and he described them all explicitly. In 1959 J. Janov and A. Mučnik [JM59] showed that even modulo term equivalence, the number of algebras on a finite set with at least three elements is uncountable.

Many classical algebraic structures have the property that their congruence relations commute with respect to the relation product. A. Malcev [Mal54] has characterized varieties of algebras with this property (a variety is a class of algebras of the same type that is defined by equations); a consequence of his result is that an algebra generates such a congruence-permutable variety if and only if it has a ternary (Malcev) term operation $m$ satisfying $m(x, y, y) = m(y, y, x) = x$ for all $x, y$. These algebras include all finite algebras that have a quasigroup operation among their binary term functions, and hence, e.g., all finite groups, rings, modules, loops, and planar ternary rings. It has long been open how many of the $2^{\aleph_0}$ finite term inequivalent algebras on a set of size at least three have a Malcev term (see e.g. [KP92, Problem 5.19]). We will prove that this number is at most countably infinite. In particular, Theorem 6.2 implies that for every finite algebra $A$ with a Malcev term there is an $n \in \mathbb{N}$ and a single subalgebra $R$ of $A^n$ such that $A$ is determined by $R$ up to term equivalence.

Recently a combinatorial characterization of finite algebras with a Malcev term has been found. As a consequence of [BIM+10] (see also [BD06]), a finite algebra $A$ has a Malcev term if and only if there is a positive real $c$ such that every independent subset of $A^n$ has at most $cn$ elements (here a subset $X$ is independent if no proper subset of $X$ generates the same subalgebra of $A^n$ as $X$). This condition immediately implies that $A^n$ has at most $|A|^{cn^2}$ subalgebras. In general, a finite algebra $A$ for which there exists a polynomial $p$ such that $A^n$ has at most $2^{p(n)}$ subalgebras is said to have few subpowers (note that the number of subalgebras of $A^n$ is certainly bounded by $2^{|A|^n}$; the adjective ‘few’ refers to the fact that the number of subalgebras does not grow doubly exponentially in $n$). In [BIM+10], J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote, and R. Willard characterized algebras with few subpowers by the existence of an edge operation (see Section 2) among their term functions. The class of algebras with an edge term is a vast extension of the class of algebras with a Malcev term. It also contains, e.g., all lattices and algebras with lattice operations, and is properly contained in the class of algebras that generate congruence modular varieties. Theorem 6.2 implies that every finite algebra with few subpowers is finitely related (see Section 2). This means that every such algebra—even if it has an infinite set of basic operations—has a finite description up to term equivalence. Hence on a finite set $A$, modulo term equivalence, the number of algebras with few subpowers is at most countably infinite (Corollary 6.3).

Algebras with few subpowers recently appeared in connection with the constraint satisfaction problem (CSP) in computer science. In [IMM+07] P. Idziak, P. Marković, R. McKenzie, M. Valeriote, and R. Willard proved that CSPs that afford an edge term can be solved by a polynomial-time algorithm. It is expected that more generally, CSPs admissible over finite algebras in congruence-modular varieties are solvable in polynomial time as well. This would follow from a partial converse of our result which has been conjectured by M. Valeriote. The conjecture is that a finite algebra in a congruence-
modular variety, if it is finitely related, must have few subpowers.\footnote{The conjecture was since announced to be true by L. Barto in June 2012.} A special case of this, which had earlier been conjectured by L. Zádori, has been established recently by L. Barto [Bar13] (see also P. Marković and R. McKenzie [MM08]): A finite algebra in a congruence-distributive variety is finitely related if and only if it has a near unanimity operation.

2. Algebras and clones

We will express our results using the terminology of universal algebra [BS81, MMT87] and clone theory [PK79, Sze86]. Following [HM88], we understand an algebra $A := \langle A, F \rangle$ as a set $A$ together with a set $F$ of finitary operations on $A$. For a nonvoid set $A$, by a clone on $A$ we shall mean any set of finitary operations on $A$ (of positive arity) that is closed under compositions and contains the projection operations $e_n^i(x_1, \ldots, x_n) = x_i$ for all positive integers $n$ and for all $i \in \{1, \ldots, n\}$. The set of term operations of an algebra $A$ is a clone, and every clone on $A$ takes this form.

For $k \geq 2$ a function $t : A^{k+1} \to A$ is a $k$-edge operation if for all $x, y \in A$ we have

$$t(y, y, x, \ldots, x) = t(y, x, y, x, \ldots, x) = x,$$

and for all $i \in \{4, \ldots, k+1\}$ and for all $x, y \in A$ we have

$$t(x, \ldots, x, y, x, \ldots, x) = x,$$

with $y$ in position $i$. A ternary operation $t$ is a 2-edge operation if and only if $m(x, y, z) := t(y, x, z)$ is a Malcev operation. For $k > 2$ a $k$-ary near unanimity operation $f$ is a function such that $t(x_1, \ldots, x_{k+1}) := f(x_2, \ldots, x_{k+1})$ is a $k$-edge operation. Thus the class of clones with edge operations contains all clones with Malcev or near unanimity operations. We also note that an algebra has an edge term if and only if it has a parallelogram term as defined in [KS12].

A clone $C$ on $A$ is finitely related if there exist subalgebras $R_1, \ldots, R_k$ of finitary powers of $(A, C)$ such that every function on $A$ that preserves every $R_i$ for $i \in \{1, \ldots, k\}$ is in $C$. We call an algebra finitely related if its clone of term functions is finitely related. Clones on finite sets containing a near-unanimity operation are finitely related by the Baker–Pixley Theorem [BP75]. In [Aic10] the first author shows that, on a finite set, every clone that contains a Malcev operation and all constant functions is finitely related. Special cases of the result in [Aic10] were given, for example, by P. Idziak [Idz99], A. Bulatov [Bul01], K. Kearnes and Á. Szendrei [KS05], the second author [May08, May11], and N. Mudrinski and the first author [AM10]. In this paper we prove the common generalization that on a finite set every clone with edge operation is finitely related (Theorem 6.1).

The conjecture that on a finite set the number of clones with Malcev operation is countable dates back to the mid 1980’s or earlier. The two tools which we use to prove...
this conjecture were first combined to good effect in [Aic10]. They are, first, a combinatorial theorem due to G. Higman [Hig52], which occurs here in a generalized form as Lemma 3.2; and second, the result that for an algebra $A$ with $k$-edge term every subalgebra of a finite power of $A$ has a small generating set that takes a specific form (Lemma 4.1). The second result also lies at the core of the proof in [IMM+07] that every constraint satisfaction problem whose template relations are admissible over an algebra with few subpowers is tractable—i.e., admits a polynomial time algorithm for its solution.

3. Preliminaries from order theory

We will first give a short survey of those results from order theory that we will need. The partially ordered set $(X, \leq)$ is well partially ordered if it satisfies the descending chain condition (DCC) and has no infinite antichains. The following facts about well partial orders can be found in [Lav76] (cf. [NW63]). A sequence of elements $\langle (a, b) \mid k \in \mathbb{N} \rangle$ is good if there are $i, j \in \mathbb{N}$ with $i < j$ and $a_i \leq_a x_j$; a sequence is bad if it is not good. Using Ramsey’s Theorem, one can prove that $(X, \leq)$ is well partially ordered if and only if every sequence in $X$ is good. If $(X, \leq)$ satisfies the (DCC), but is not well partially ordered, then there exists a bad sequence $\langle x_k \mid k \in \mathbb{N} \rangle$ with the property that for all $i \in \mathbb{N}$ and for all $y_i \in X$ with $y_i < x_i$, every sequence starting with $(x_1, \ldots, x_{i-1}, y_i)$ is good. Such a sequence is called a minimal bad sequence. For an ordered set $(X, \leq)$, a subset $Y$ of $X$ is upward closed if for all $y \in Y$ and $x \in X$ with $y \leq x$, we have $x \in Y$.

For $A = \{1, \ldots, t\}$, we will use the lexicographic ordering on $A^n$. For $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$, we say $a \leq_{\text{lex}} b$ if

$$(\exists i \in \{1, \ldots, n\} : a_1 = b_1 \land \cdots \land a_{i-1} = b_{i-1} \land a_i < b_i) \lor (a_1, \ldots, a_n) = (b_1, \ldots, b_n).$$

For every finite set $A$, we let $A^+$ be the set $\bigcup [A^n \mid n \in \mathbb{N}]$. We will now introduce an order relation on $A^+$. For $a = (a_1, \ldots, a_n) \in A^+$ and $b \in A$, we define the index of the first occurrence of $b$ in $a$, $\text{firstOcc}(a, b)$, by $\text{firstOcc}(a, b) := 0$ if $\emptyset \not\subseteq \{a_1, \ldots, a_n\}$, and $\text{firstOcc}(a, b) := \min\{i \in \{1, \ldots, n\} \mid a_i = b\}$ otherwise.

**Definition 3.1.** Let $A$ be a finite set, and let $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_n)$ be elements of $A^+$. We say $a \leq_E b$ (read: $a$ embeds into $b$) if there is an injective and increasing function $h : \{1, \ldots, m\} \to \{1, \ldots, n\}$ such that

1. $a_i = b_{h(i)}$ for all $i \in \{1, \ldots, m\}$,
2. $\{a_1, \ldots, a_m\} = \{b_1, \ldots, b_n\}$,
3. $h(\text{firstOcc}(a, c)) = \text{firstOcc}(b, c)$ for all $c \in \{a_1, \ldots, a_m\}$.

We will call such an $h$ a function witnessing $a \leq_E b$.

Less formally, we have $a \leq_E b$ for words $a, b$ over the alphabet $A$ if and only if $b$ can be obtained from $a$ by inserting additional letters anywhere after their first occurrence in $a$. We will use the following fact about this ordering, which generalizes Higman’s Theorem 4.4 in [Hig52].
Lemma 3.2. Let A be a finite set. Then \(A^+, \leq_E\) is well partially ordered.

Proof. It is easy to see that \(\leq_E\) is a partial order relation and that \(A^+, \leq_E\) satisfies the (DCC). It remains to show that for every sequence \(\langle x^{(k)} \mid k \in \mathbb{N} \rangle\) in \(A^+\), there exist \(i, j \in \mathbb{N}\) such that \(i < j\) and \(x^{(i)} \leq_E x^{(j)}\). We will prove this by induction on \(|A|\). For \(|A| = 1\), the claim is obvious. Assume that \(|A| > 1\) and \((B^+, \leq_E)\) is well partially ordered for every proper subset \(B\) of \(A\).

Seeking a contradiction we suppose we have a minimal bad sequence \(\langle x^{(k)} \mid k \in \mathbb{N} \rangle\) in \(A^+\). For each \(x = (x_1, \ldots, x_n) \in A^+\), let Symbols(x) := \{x_1, \ldots, x_n\} be the set of all elements of \(A\) that occur in the word \(x\), let Last(x) := \(x_n\) denote the last letter of \(x\), and, if \(n > 1\), let Start(x) := \((x_1, \ldots, x_{n-1})\). Since \(A\) is finite, we have \(a \in A\) and an infinite \(T \subseteq \mathbb{N}\) such that for all \(i \in T\), Last(x\(^{(i)}\)) = \(a\) and the length of \(x^{(i)}\) is at least two.

Let us first consider the case that there exists an infinite \(S \subseteq T\) such that Symbols(Start(x\(^{(i)}\))) \(\subseteq A \setminus \{a\}\) for all \(i \in S\). By the induction hypothesis, \(\leq_E\) is a well partial order on \((A \setminus \{a\})^+\). Hence there are \(i, j \in S\) with \(i < j\) such that Start(x\(^{(i)}\)) \(\leq_E\) Start(x\(^{(j)}\)). Since \(a\) does not occur in Start(x\(^{(j)}\)) nor in Start(x\(^{(i)}\)), and since Last(x\(^{(i)}\)) = Last(x\(^{(j)}\)) = \(a\), we have x\(^{(i)}\) \(\leq_E\) x\(^{(j)}\), contradicting the fact that \((x^{(k)} \mid k \in \mathbb{N})\) is a bad sequence.

Thus we may assume that there exists an infinite subset \(S := \{s_1, s_2, \ldots\}\) of \(T\) (with \(s_i < s_j\) whenever \(i < j\)) such that Symbols(Start(x\(^{(s)}\))) = \(A\) for all \(s \in S\). Now consider the sequence

\[
\langle y^{(k)} \mid k \in \mathbb{N}\rangle := \langle x^{(1)}, \ldots, x^{(s_1 - 1)}, \text{Start}(x^{(s_1)}), \text{Start}(x^{(s_2)}), \ldots \rangle.
\]

We show that \(\langle y^{(k)} \mid k \in \mathbb{N}\rangle\) is bad by distinguishing three cases: If \(i < j < s_1\), then clearly \(x^{(i)} \leq_E x^{(j)}\). If \(i < s_1\) and \(j \geq 1\), then \(x^{(i)} \leq_E \text{Start}(x^{(s_1)})\) yields \(x^{(i)} \leq_E x^{(s_1)}\), contradicting the fact that \((x^{(k)} \mid k \in \mathbb{N})\) is bad. If \(i < j\), then Start(x\(^{(s_1)}\)) \(\leq_E\) Start(x\(^{(s_2)}\)) implies \(x^{(s_1)} \leq_E x^{(s_2)}\) because Last(x\(^{(s_1)}\)) = Last(x\(^{(s_2)}\)) = \(a\) and \(a\) already occurs both in \(\text{Start}(x^{(s_1)})\) and in \(\text{Start}(x^{(s_2)})\). This again contradicts the badness of \((x^{(k)} \mid k \in \mathbb{N})\). Hence \((x^{(k)} \mid k \in \mathbb{N})\) is bad. However, since \(y^{(s_1)} = \text{Start}(x^{(s_1)}) \leq_E x^{(s_1)}\), this contradicts the choice of \((x^{(k)} \mid k \in \mathbb{N})\) as a minimal bad sequence. Hence \((A^+, \leq_E)\) is well partially ordered. \(\square\)

For \(a, b \in A^+\) with \(a \leq_E b\) we observe a correspondence between the elements that are lexicographically smaller than \(a\) and certain elements that are lexicographically smaller than \(b\). But before that we need to introduce some notation.

Definition 3.3. Let \(A\) be a finite set, let \(a = (a_1, \ldots, a_m) \in A^m, b = (b_1, \ldots, b_n) \in A^n\) be such that \(a \leq_E b\), and let \(h\) be a function from \([1, \ldots, m]\) \(\rightarrow [1, \ldots, n]\) witnessing \(a \leq_E b\). We define a function \(T_{a,b,h} : A^m \rightarrow A^n\). Let \(x = (x_1, \ldots, x_m) \in A^m\). If \(j \in \text{range}(h)\), then the \(j\)-th entry of \(T_{a,b,h}(x)\), abbreviated by \(T_{a,b,h}(x)(j)\), is defined by

\[
T_{a,b,h}(x)(j) := x_i,
\]

where \(i \in [1, \ldots, m]\) is such that \(h(i) = j\). If \(j \notin \text{range}(h)\), then

\[
T_{a,b,h}(x)(j) := x_i,
\]

where \(i := \text{firstOcc}(a, b_j)\).
Lemma 3.4. Let \( t \in \mathbb{N} \), let \( A = \{1, \ldots, t \} \), and let \( a \in A^m \), \( b \in A^n \) with \( h : \{1, \ldots, m\} \to \{1, \ldots, n\} \) witnessing \( a \leq_E b \). Let \( c \in A^m \) be such that \( c <_{\text{lex}} a \). Then

1. \( T_{a,b,h}(a) = b \).
2. \( T_{a,b,h}(c) <_{\text{lex}} b \).

Proof. (1) follows immediately from the definition of \( T_{a,b,h} \). To prove (2), let \( k \) be the index of the first place where \( c \) differs from \( a \). Hence \( c = (a_1, \ldots, a_{k-1}, c_k, c_{k+1}, \ldots) \), \( a = (a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots) \), and \( c_k < a_k \).

We first show that for all \( j < h(k) \), we have \( T_{a,b,h}(c)(j) = T_{a,b,h}(a)(j) \). If \( j \) is in the range of \( h \), there is an \( i \) with \( h(i) = j \), and we have \( T_{a,b,h}(c)(j) = c_i \) and \( T_{a,b,h}(a)(j) = a_i \). Since \( h(i) < h(k) \), we have \( i < k \). Thus \( c_i = a_i \), since \( k \) is the first index at which \( c \) and \( a \) differ. We now assume that \( j \) is not in the range of \( h \). Since \( \{b_1, \ldots, b_n\} = \{a_1, \ldots, a_m\} \), we see that \( i := \text{firstOcc}(a, b_j) \) satisfies \( i > 0 \). By the definition of \( \leq_E \) we see \( h(i) = \text{firstOcc}(b, b_j) \) and therefore \( h(i) \leq h(i) \). Hence \( h(i) < h(k) \) and \( i < k \). Thus \( c_i = a_i \). Since \( T_{a,b,h}(x_1, \ldots, x_m)(j) := x_i \) for all \( x \in A^m \), we finally obtain \( T_{a,b,h}(c)(j) = T_{a,b,h}(a)(j) \).

Since \( T_{a,b,h}(a)(h(k)) = a_k \) and \( T_{a,b,h}(c)(h(k)) = c_k \), we have \( T_{a,b,h}(c) <_{\text{lex}} T_{a,b,h}(a) \).

\( \Box \)

4. Algebras with edge term

Let \( A \) be a set, and let \( m \in \mathbb{N} \). For \( a = (a_1, \ldots, a_m) \in A^m \) and \( T \subseteq \{1, \ldots, m\} \), we denote the projection to the tuple of entries that are indexed by \( T \) as

\[ \pi_T(a) := (a_i \mid i \in T) \].

For \( F \subseteq A^m \) and \( i \in \{1, \ldots, m\} \), define

\[ \varphi_i(F) := \{(a_i, b_i) \in A^2 \mid a, b \in F \text{ and } \pi_{\{1, \ldots, i-1\}}(a) = \pi_{\{1, \ldots, i-1\}}(b)\} \].

By [Aic10, Lemma 3.1] a subuniverse \( G \) of a Malcev algebra \( A^m \) is generated by every subset \( F \) of \( G \) with \( \varphi_i(F) = \varphi_i(G) \) for all \( i \in \{1, \ldots, m\} \).

In [BIM+10] these relations \( \varphi_i \) and projections \( \pi_T \) occur in the description of small generating sets for the subuniverses of \( A^m \) for a finite algebra \( A \) with edge term operation. These generating sets were then used to obtain a bound on the number of subuniverses of \( A^m \). We reformulate the representation result [BIM+10, Corollary 3.9] for our purposes.

Lemma 4.1. Let \( k, m \) be positive integers with \( k > 1 \), let \( A \) be a finite algebra with \( k \)-edge term operation \( t \), and let \( F, G \) be subuniverses of \( A^m \) with \( F \subseteq G \). Assume \( \pi_T(F) = \pi_T(G) \) for all \( T \subseteq \{1, \ldots, m\} \) with \( |T| < k \), and \( \varphi_i(G) \subseteq \varphi_i(F) \) for all \( i \in \{1, \ldots, m\} \). Then \( F = G \).
Proof. We only have to check that $F$ is what is called a representation of $G$ in [BIM+10, Def. 3.2]. For that we need to introduce some more notation. By Lemma 2.13 of [BIM+10], $A$ has term operations $d: A^2 \to A$, $p: A^3 \to A$, and $s: A^k \to A$ such that for all $x, y \in A$:

\[
\begin{align*}
p(x, y, y) &= x, \\
s(x, y, x, \ldots, y, x) &= p(x, y, y), \\
s(x, y, x, \ldots, x, x) &= x, \\
&\vdots \\
s(x, x, x, \ldots, y, x) &= x, \\
d(x, y) &= p(x, x, y), \\
d(x, d(x, y)) &= d(x, y).
\end{align*}
\]

The signature $\text{Sig}_R$ of a subset $R$ of $A^m$ is defined as

\[
\text{Sig}_R := \{(i, u, v) \in \{1, \ldots, m\} \times A^2 \mid (u, v) \in \varphi_i(R) \text{ and } d(u, v) = v\}.
\]

For $R, S \subseteq A^n$ we say that $R$ is a representation of $S$ if

1. $R \subseteq S$,
2. $\pi_T(R) = \pi_T(S)$ for all $T \subseteq \{1, \ldots, n\}$ with $|T| < k$, and
3. $\text{Sig}_R = \text{Sig}_S$.

From $F \subseteq G$, it is immediate that $\varphi_i(F) \subseteq \varphi_i(G)$. Consequently, $\varphi_i(F) = \varphi_i(G)$ for all $i \in \{1, \ldots, m\}$. In particular $\text{Sig}_F = \text{Sig}_G$. Thus $F$ is a representation of $G$. Since $F, G$ are subuniverses of $A^m$, Corollary 3.9 of [BIM+10] yields $F = G$. □

The previous result has also been known in two special cases: For $A$ with a $k$-ary near unanimity term it follows from the Baker–Pixley Theorem [BP75]. For $A$ with a Malcev term, it occurs as Lemma 3.1 in [Aic10], and it is the central fact underlying Dalmau’s polynomial-time algorithm for solving CSPs which admit a Malcev polymorphism [BD06].

5. Encoding clones

Let $C$ be a clone on the $t$-element set $A = \{1, \ldots, t\}$, and let $n \in \mathbb{N}$. Let $C^{[n]}$ denote the set of $n$-ary functions in $C$. As in [Aic10], for $a \in A^n$, we define a binary relation $\varphi(C, a)$ on $A$ by

\[
\varphi(C, a) := \{(f(a), g(a)) \mid f, g \in C^{[n]}, \forall c \in A^n : c <_{\text{lex}} a \Rightarrow f(c) = g(c)\}.
\]

Intuitively, if $\varphi(C, a)$ is small, then the functions in $C$ are strongly restricted by their images on $c$ for $c <_{\text{lex}} a$. We also encode these relations in another way.

For $(c, d) \in A^2$, we define a subset $\lambda(C, (c, d))$ of $A^+$ by

\[
\lambda(C, (c, d)) := \{a \in A^+ \mid (c, d) \not\in \varphi(C, a)\}.
\]

We will later use the following straightforward connection between the relations $\varphi(C, a)$ and the sets $\lambda(C, (c, d))$. 

Lemma 5.1. Let $C, D$ be clones on a finite set $A$. Then the following are equivalent:

1. $\lambda(C, (c, d)) \subseteq \lambda(D, (c, d))$ for all $(c, d) \in A^2$.
2. $\varphi(D, a) \subseteq \varphi(C, a)$ for all $a \in A^+$.

Proof. Assume we have (1). Let $a \in A^+$, and let $(c, d) \in \varphi(D, a)$. Then $a \not\in \lambda(D, (c, d))$ and $a \not\in \lambda(C, (c, d))$ by (1). Hence $(c, d) \in \varphi(C, a)$, and (2) is proved.

Conversely, assume we have (2). Let $(c, d) \in A^2$, and let $a \in \lambda(C, (c, d))$. Then $(c, d) \not\in \varphi(C, a)$, which implies $(c, d) \not\in \varphi(D, a)$ by (2). Hence $a \in \lambda(D, (c, d))$, and (1) is proved. $\square$

From the order-theoretic observations in Section 3 we obtain the following lemmas.

Lemma 5.2. Let $t, m, n \in \mathbb{N}$, let $C$ be a clone on the $t$-element set $A = \{1, \ldots, t\}$, and let $a \in A^m$ and $b \in A^n$ be such that $a \preceq_E b$. Then $\varphi(C, b) \subseteq \varphi(C, a)$.

Proof. Let $(x, y) \in \varphi(C, b)$. Then there are $f, g \in C^{[n]}$ such that $x = f(b)$, $y = g(b)$, and $f(c) = g(c)$ for all $c \in A^t$ with $c \preceq_{\text{lex}} b$. Let $h$ be a function from $\{1, \ldots, m\}$ to $\{1, \ldots, n\}$ witnessing $a \preceq_E b$. Now we define functions $f_1$ and $g_1$ from $A^m$ to $A$ by

$$f_1(x) := f(T_a, b, h(x)), \quad g_1(x) := g(T_a, b, h(x)),$$

for $x \in A^m$. By the definition of $T_a, b, h$, we see that for each $j \in \{1, \ldots, n\}$, the mapping that maps $x$ to the $j$-th component of $T_a, b, h(x)$ is a projection operation. Hence $f_1$ and $g_1$ lie in the clone $C$.

We will now show that $(f_1(a), g_1(a))$ is an element of $\varphi(C, a)$. To this end, let $c \in A^m$ be such that $c \preceq_{\text{lex}} a$. Then Lemma 3.4 yields $T_a, b, h(c) \preceq_{\text{lex}} b$. Hence we have $f_1(c) = f(T_a, b, h(c)) = g(T_a, b, h(c)) = g_1(c)$. From this we obtain $(f_1(a), g_1(a)) \in \varphi(C, a)$. Since $(f_1(a), g_1(a)) = (f(b), g(b)) = (x, y)$ by Lemma 3.4, we obtain $(x, y) \in \varphi(C, a)$. $\square$

Lemma 5.3. Let $C$ be a clone on a finite set $A$, and let $(c, d) \in A^2$. Then $\lambda(C, (c, d))$ is an upward closed subset of $(A^+, \preceq_E)$.

Proof. Let $a \in \lambda(C, (c, d))$, and let $b \in A^+$ such that $a \preceq_E b$. Since $(c, d) \not\in \varphi(C, a)$, Lemma 5.2 yields $(c, d) \not\in \varphi(C, b)$ and thus $b \in \lambda(C, (c, d))$. $\square$

6. Relations

A finitary relation $R$ on a set $A$ is a subset of $A^I$ for some finite set $I$. We say a function $f : A^k \to A$ preserves $R$ if $R$ is a subuniverse of $(A, f)^I$.

For a clone $C$ on a set $A$ and for $m \in \mathbb{N}$, the set of $m$-ary functions $C^{[m]}$ is a subset of $A^{A^m}$. In this sense, a function $f : A^k \to A$ preserves the relation $C^{[m]}$ if for all $g_1, \ldots, g_k \in C^{[m]}$ the function

$$A^m \to A, \quad x \mapsto f(g_1(x), \ldots, g_k(x)),$$

is in $C^{[m]}$ again.

For $a \in A^+$ let $|a|$ denote the length of $a$.

In the next result we give finitely many relations that determine a clone with edge operation.
Theorem 6.1. Let $A$ be a finite set, let $k \in \mathbb{N}$, $k > 1$, let $C$ be a clone on $A$ that contains a $k$-edge operation $t$, and let $\Lambda := (\Lambda, C)$. Then the set \{[a] | there exists $(c, d) \in A^2$ such that $a$ is minimal with respect to $\leq_E$ in $\lambda(C, (c, d))$\} has a supremum $m$ in $\mathbb{N}$, and $C$ is the clone of functions that preserve the relation $C^{[m]}$ and every subuniverse of $A^{k-1}$.

So by Theorem 6.1 the clone $C$ is determined by the finitely many relations of arity $\max(|A|^m, k-1)$. Apart from the condition on the $m$-ary operations our result resembles the Baker–Pixley Theorem (see [BP75, Theorem 2.1(5)]) for clones with near unanimity operations.

Proof of Theorem 6.1. Let $(c, d) \in A^2$. Since $(A^+, \leq_E)$ has no infinite antichain by Lemma 3.2, $\lambda(C, (c, d))$ contains only finitely many minimal elements. Consequently, as the supremum of finitely many natural numbers, $m$ is finite. We note that the set \{[a] | there exists $(c, d) \in A^2$ such that $a$ is minimal with respect to $\leq_E$ in $\lambda(C, (c, d))$\} is empty if $\lambda(C, (c, d))$ is empty for all $(c, d) \in A^2$. In that case we have $m = 1$ as the supremum.

Let $D$ be the clone of functions that preserve $C^{[m]}$ and every subuniverse of $A^{k-1}$. Then $C \subseteq D$ and $C^{[i]} = D^{[i]}$ for all $i \in \{1, \ldots, m\}$. We claim that

$$\lambda(C, (c, d)) \subseteq \lambda(D, (c, d)).$$

(6.1)

If $\lambda(C, (c, d)) = \emptyset$, the assertion is clear. So let $a$ be minimal in $\lambda(C, (c, d))$. Then $(c, d) \notin \varphi(C, a)$. By definition, $m$ is at least the length $|a|$ of $a$. Hence $C^{[|a|]} = D^{[|a|]}$, which implies that $\varphi(C, a) = \varphi(D, a)$. Thus $a \in \lambda(D, (c, d))$. So we have just proved that every minimal element of $\lambda(C, (c, d))$ is contained in $\lambda(D, (c, d))$. Since $\lambda(C, (c, d))$ and $\lambda(D, (c, d))$ are upward closed subsets of the well partially ordered set $(A^+, \leq_E)$ by Lemma 5.3, this proves (6.1).

Next we will show that $D^{[n]} \subseteq C^{[n]}$ for all $n \in \mathbb{N}$. For fixed $n \in \mathbb{N}$ and $a \in A^n$ we have

$$\varphi(D, a) \subseteq \varphi(C, a)$$

(6.2)

by (6.1) and Lemma 5.1.

Note that $F := C^{[n]}$ and $G := D^{[n]}$ form subuniverses of $A^{[A]^n}$ with $F \subseteq G$. For every $T \subseteq A^n$ with $|T| < k$ we claim that

$$\pi_T(F) = \pi_T(G).$$

(6.3)

Clearly $\pi_T(F) \subseteq \pi_T(G)$. To prove the converse inclusion let $g \in G$, let $l := |T|$, and let $T = \{t_1, \ldots, t_l\} = \{(a_1, \ldots, a_{n_1}), \ldots, (a_{11}, \ldots, a_{1n})\}$. We know that $g$ preserves the subuniverse $B$ of $A^l$ that is generated by $\{(a_1, \ldots, a_{n_1}), \ldots, (a_{11}, \ldots, a_{1n})\}$. From $(g(t_1), \ldots, g(t_l)) \in B$, we obtain an $n$-ary term function $f$ of $A$ such that $(g(t_1), \ldots, g(t_l)) = (f(t_1), \ldots, f(t_l))$. Hence $f|_T = g|_T$, and thus $\pi_T(f) = \pi_T(g)$. Hence $\pi_T(F) \supseteq \pi_T(G)$ and we have (6.3). By (6.2) and (6.3) the assumptions of Lemma 4.1 are satisfied. Thus $F \equiv G$. □

For a finite set $A$ and a set $S$ of finitary relations on $A$, we will write $\text{Pol}(A, S)$ for the set of those functions on $A$ that preserve all relations in $S$ (cf. [PK79]).
Theorem 6.2. Let $A$ be a finite set, let $k \in \mathbb{N}$, $k > 1$, and let $\mathcal{M}_k$ be the set of all clones on $A$ that contain a $k$-edge operation. Then:

1. For every clone $C$ in $\mathcal{M}_k$, there is a finitary relation $R$ on $A$ such that $C = \text{Pol}(A, \{R\})$.
2. There is no infinite descending chain in $(\mathcal{M}_k, \subseteq)$.
3. The set $\mathcal{M}_k$ is finite if $|A| \leq 3$ and countably infinite otherwise.

Proof. (1) Let $C$ be a clone with $k$-edge term on the finite set $A$. By Theorem 6.1 there exists a finite set $S$ of finitary relations on $A$ such that $C = \text{Pol}(A, S)$. By [PK79, p. 50], there is a single finitary relation $R$ on $A$ with $\text{Pol}(A, S) = \text{Pol}(A, \{R\})$.

Now (2) follows from (1) using the implication (i)$' \Rightarrow$(ii)$'$ in [PK79, Charakterisierungssatz 4.1.3].

(3) From [Idz99] and [KS12, Corollary 4.10] we deduce that $\mathcal{M}_k$ is finite if $|A| \leq 3$, and infinite if $|A| \geq 4$. Every finitary relation on the finite set $A$ is a finite subset of the countable set $A^+$. Hence $\mathcal{M}_k$ is countable by (1), and the claim follows. $\square$

Corollary 6.3. Let $A$ be a finite set. Modulo term equivalence, the number of algebras on $A$ that have few subpowers is at most countably infinite.

Proof. By [BIM$^+$10, Corollary 3.11] every algebra on $A$ with few subpowers has an edge operation in its clone of term functions. Since the number of clones with edge operation on $A$ is at most countably infinite by Theorem 6.2(3), the assertion follows. $\square$

We can now formulate a consequence of Theorem 6.2 that was not known even for finite groups $A$.

Corollary 6.4. Let $A$ be a finite algebra with few subpowers. Then there exists a subalgebra $R$ of some finitary power of $A$ such that for every $n \in \mathbb{N}$, every subalgebra $S$ of $A^n$ is primitive-positive definable over $R$.

Proof. By [BIM$^+$10, Corollary 3.11] the clone $C$ of term operations of $A$ contains an edge operation. So, by Theorem 6.2(1), we have a finitary relation $R$ on $A$ such that $C = \text{Pol}(A, \{R\})$. Hence by [PK79, Folgerung 1.2.4, Hauptsatz 2.1.3] every finitary relation $S$...
on $A$ that is preserved by all functions in $C$ is primitive-positive definable over $R$. Since the finitary relations that are preserved by all term functions are exactly the subalgebras of finite powers of $A$, the result is proved. □

For the case of finite groups we restate the previous corollary and give some explicit bounds on the length of the primitive-positive formula necessary to describe an arbitrary relation.

**Corollary 6.5.** Let $G$ be a finite, nontrivial group. Then there exists $k \in \mathbb{N}$ and a subgroup $H$ of $G^k$ with the following property:

For each $n \in \mathbb{N}$ there are $l, m \in \mathbb{N}$ with $l \leq |G|^\lfloor \log_2(|G|) \rfloor$ and $m \leq l \cdot \log_2(|G|)$, and there is a mapping $\sigma : \{1, \ldots, m\} \times \{1, \ldots, k\} \to \{1, \ldots, l\}$ such that for every subgroup $S$ of $G^k$ there is a mapping $\tau : \{1, \ldots, n\} \to \{1, \ldots, l\}$ such that

$$S = \left\{ (g_1, \ldots, g_n) \in G^n \mid \exists a_1, \ldots, a_l \in G : \left( \bigwedge_{i \in \{1, \ldots, m\}} (a_{\sigma(i,1)}, \ldots, a_{\sigma(i,k)}) \in H \right) \land g_1 = a_{\tau(1)} \land \cdots \land g_n = a_{\tau(n)} \right\}. $$

**Proof.** As a subgroup of $G^n$, $S$ has a set of generators $\{s_1, \ldots, s_e\}$ with $e \leq \log_2(|G|^n)$. Let $C$ be the clone of term operations on $G$. Then

$$S = \{ f(s_1, \ldots, s_e) \mid f \in C^{[e]} \}. $$

(6.4)

By Theorem 6.2(1), we have $k \in \mathbb{N}$ and some subgroup $H$ of $G^k$ such that $C$ consists exactly of those functions that preserve $H$. In particular

$$C^{[e]} = \left\{ f \in G^{G^e} \mid \bigwedge_{(r_1, \ldots, r_e) \in H^e} f(r_1, \ldots, r_e) \in H \right\}, $$

$$= \bigcap_{(r_1, \ldots, r_e) \in H^e} \{ f \in G^{G^e} \mid f(r_1, \ldots, r_e) \in H \}. $$

Each of the $|H|^e$ sets in this intersection forms a subgroup of $G^{G^e}$. So we can choose $\log_2(|G|^{|G|^e})$ of them whose intersection is again equal to $C^{[e]}$. Hence we have $M \subseteq H^e$ with $|M| \leq |G|^{e \cdot \log_2(|G|)}$ such that

$$C^{[e]} = \left\{ f \in G^{G^e} \mid \bigwedge_{(r_1, \ldots, r_e) \in M} f(r_1, \ldots, r_e) \in H \right\}. $$

(6.5)

Combining (6.4) and (6.5) yields

$$S = \left\{ g \in G^n \mid \exists f \in G^{G^e} : \bigwedge_{(r_1, \ldots, r_e) \in M} f(r_1, \ldots, r_e) \in H \land f(s_1, \ldots, s_e) = g \right\}. $$

(6.6)

It only remains to rewrite (6.6). Let $l := |G|^e$, and let $\lambda : G^e \to \{1, \ldots, l\}$ be a bijection. For $i \in \{1, \ldots, l\}$ define $a_i := f(\lambda^{-1}(i))$. Let $m := |M|$, let $\mu : \{1, \ldots, m\} \to M$ be a bijection, and let $\sigma : \{1, \ldots, m\} \times \{1, \ldots, k\} \to \{1, \ldots, l\}$, $(i, j) \mapsto \lambda((\mu(i))_j)$. Note that $l, m$ and $\sigma$ only depend on $n$ but not on $S$. Finally, define $\tau : \{1, \ldots, n\} \to \{1, \ldots, l\}$ by $\tau(i) := \lambda(s_1, \ldots, s_{ei})$. Then the result follows from (6.6). □
7. Concluding remarks

Given a set $F$ of functions on a finite set $A$ such that $F$ generates a clone $C$ with edge operation, Theorem 6.2 guarantees the existence of a single relation $R$ that determines $C$; however, even if $F$ is finite, it is not yet clear how to find $R$ algorithmically.

K. Kearnes and Á. Szendrei [KS12] proved a result that is stronger than the one in this paper for algebras in residually small varieties. Namely, Theorem 4.3 of [KS12] shows that for every finite algebra $A$ with $k$-edge term in a residually small variety, the clone of term operations of $A$ is determined by relations of arity $\max(k, |A|^{k+1}B(|A|+1)−1)$ where $B(n)$ denotes the $n$-th Bell number. Hence these algebras are finitely related. Moreover on a fixed set $A$ and for a fixed $k > 1$ there are only finitely many of them up to term equivalence.

In [Koz08] M. Kozik considered the question whether a function can be obtained as composition of some fixed functions. More precisely, for a fixed set of functions $F$ on a finite set $A$ the problem $ISTERMFUNCTION(F)$ is the following:

Input: a function $f: A^n \rightarrow A$,
Problem: decide if $f$ is in the clone $C$ on $A$ that is generated by $F$.

He showed that in general this decision problem is EXPTIME-complete. If we assume that $F$ contains an edge operation, then there exists some fixed $k$-ary relation $R$ on $A$ such that $C = \text{Pol}(A, \{R\})$. Whether $f$ preserves $R$ can be checked by evaluating $f$ in $k \cdot |R|^n$ places and performing $|R|^n$ tests whether a given $k$-tuple is an element of $R$. The input of $ISTERMFUNCTION(F)$ is the graph of $f$ which basically has size $|A|^n$. Consequently, $ISTERMFUNCTION(F)$ is solvable in polynomial time if the algebra $\langle A, F \rangle$ has few subpowers.

Acknowledgements. The authors thank J. Farley and C. Pech for helpful discussions. The second author acknowledges support from Portuguese Project ISFL-1-143 of CAUL financed by FCT and FEDER.

References


