ON THE NUMBER OF FINITE ALGEBRAIC STRUCTURES

ERHARD AICHINGER, PETER MAYR, AND RALPH MCKENZIE

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.

1. Introduction

An algebraic structure (or *algebra*, for short) is usually represented as a non-void 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 $\langle B, \wedge, \vee, \neg \rangle$ 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] published that there are only countably many term inequivalent algebras of size two (modulo renaming of the elements), and he described them all explicitely. In

Date: May 7, 2010.

2000 *Mathematics Subject Classification.* 08A62 (08A40, 08B05).

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 countably infinite. In particular, Theorem 6.2 yields that for every finite algebra $\mathbf{A}$ with a Malcev term there is an $n \in \mathbb{N}$ and a single subalgebra R of $\mathbf{A}^n$ such that $\mathbf{A}$ 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], a finite algebra $\mathbf{A}$ has a Malcev term if and only if there is a positive real c such that every independent subset of $\mathbf{A}^n$ has at most cn elements (Here a subset X is independent if no proper subset of X generates the same subalgebra of $\mathbf{A}^n$ as X). This condition immediately yields that $\mathbf{A}^n$ has at most $|A|^{cn^2}$ subalgebras. In general, a finite algebra $\mathbf{A}$ for which there exist a polynomial p such that $\mathbf{A}^n$ has at most $2^{p(n)}$ subalgebras is said to have *few subpowers* (Note that the number of subalgebras of $\mathbf{A}^n$ is certainly bounded by $2^{|A|^n}$. The adjective 'few' refers to the fact that the number of subalgebras does not grow doubly exponential in n). In [BIM$^+$10] algebras with few subpowers are characterized 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 comprises, 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 yields that every finite algebra with few subpowers is finitely related (see Section 2). Hence on a finite set A, modulo term equivalence, the number of algebras with few subpowers is at most countably infinite.

Algebras with few subpowers recently appeared in connection with the constraint satisfaction problem (CSP) in computer science. By [IMM$^+$07] 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. A special case of this, which had earlier been conjectured by L. Zádori, has been established recently by L. Barto [Bar09] (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 $\mathbf{A} := \langle A, F\rangle$ as a set A together with a set of finitary operations F on A. For a non-void 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 $e_i^n(x_1, \dots, x_n) = x_i$ for all positive integers n and for all $i \in \{1, \dots, n\}$. The set of term operations of an algebra $\mathbf{A}$ 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

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

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

$$t(x, \dots, x, y, x, \dots, x) = x, \text{ with } y \text{ in position } i.$$

We note that 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 $t(x_1, \dots, x_{k+1}) := f(x_2, \dots, x_{k+1})$ is a k-edge operation. Thus the class of clones with edge operations contains all clones with Malcev or near unanimity operations. From [KS09] we know that an algebra has an edge term if and only if it has a socalled parallelogram term.

A clone C on A is *finitely related* if there exist subalgebras $R_1, \dots, R_k$ of finitary powers of $\langle A, C\rangle$ such that every function on A that preserves every R_i for $i \in \{1, \dots, k\}$ is in C. We call an algebra *finitely related* if its clone of term functions is finitely related. Clones containing a near-unanimity operation are finitely related by the Baker-Pixley Theorem [BP75]. In [Aic09] 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 [Aic09] were given, for example, by P. Idziak [Idz99], A. Bulatov [Bul01], K. Kearnes and

Á. Szendrei [KS05], the second author [May08], 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 [Aic09]. 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 in the sequel. The partially ordered set $\langle X, \leq\rangle$ 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 $\langle x_k \mid k \in \mathbb{N}\rangle$ is *good* if there are $i, j \in \mathbb{N}$ with $i < j$ and $x_i \leq x_j$; a sequence is *bad* if it is not good. Using Ramsey's Theorem, one can prove that $\langle X, \leq\rangle$ is well partially ordered if and only if every sequence in X is good. If $\langle X, \leq\rangle$ 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 $\langle X, \leq\rangle$, 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 $A = \{1, 2, \ldots, t\}$, we will use the lexicographic ordering on A^n. For $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$, we say $\mathbf{a} \leq_{\text{lex}} \mathbf{b}$ if

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

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 $\mathbf{a} = (a_1, \ldots, a_n) \in A^+$ and $b \in A$, we define the *index of the first occurrence of* b *in* $\mathbf{a}$, $\mathsf{firstOcc}(\mathbf{a}, b)$, by $\mathsf{firstOcc}(\mathbf{a}, b) := 0$ if $b \notin \{a_1, \ldots, a_n\}$, and $\mathsf{firstOcc}(\mathbf{a}, b) := \min\{i \in \{1, \ldots, n\} \mid a_i = b\}$ otherwise.

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

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

We will call such an h a function *witnessing* $\mathbf{a} \le_{\mathrm{E}} \mathbf{b}$.

Less formally, we have $\mathbf{a} \le_{\mathrm{E}} \mathbf{b}$ for words $\mathbf{a}, \mathbf{b}$ over the alphabet A if and only if $\mathbf{b}$ can be obtained from $\mathbf{a}$ by inserting additional letters anywhere after their first occurrence in $\mathbf{a}$. 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 $\langle A^+, \le_{\mathrm{E}} \rangle$ is well partially ordered.*

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

Seeking a contradiction we suppose we have a minimal bad sequence $\langle \mathbf{x}^{(k)} \mid k \in \mathbb{N} \rangle$ in A^+. For each $\mathbf{x} = (x_1, \dots, x_n) \in A^+$, let $\mathsf{Symbols}\,(\mathbf{x}) := \{x_1, \dots, x_n\}$ be the set of all elements of A that occur in the word $\mathbf{x}$, let $\mathsf{Last}\,(\mathbf{x}) := x_n$ denote the last letter of $\mathbf{x}$, and, if $n \ge 2$, let $\mathsf{Start}\,(\mathbf{x}) := (x_1, \dots, x_{n-1})$. Since A is finite, we have $a \in A$ and an infinite $T \subseteq \mathbb{N}$ such that for all $i \in T$, $\mathsf{Last}\,(\mathbf{x}^{(i)}) = a$ and the length of $\mathbf{x}^{(i)}$ is at least two.

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

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

$$\langle \mathbf{y}^{(k)} \mid k \in \mathbb{N} \rangle := \langle \mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \dots, \mathbf{x}^{(s_1 - 1)}, \mathsf{Start}\,(\mathbf{x}^{(s_1)}), \mathsf{Start}\,(\mathbf{x}^{(s_2)}), \dots \rangle.$$

We show that $\langle \mathbf{y}^{(k)} \mid k \in \mathbb{N}\rangle$ is bad by distinguishing three cases: If $i < j < s_1$, then clearly $\mathbf{x}^{(i)} \not\leq_{\mathrm{E}} \mathbf{x}^{(j)}$. If $i < s_1$ and $j \geq 1$, then $\mathbf{x}^{(i)} \leq_{\mathrm{E}} \mathsf{Start}\,(\mathbf{x}^{(s_j)})$ yields $\mathbf{x}^{(i)} \leq_{\mathrm{E}} \mathbf{x}^{(s_j)}$, contradicting the fact that $\langle \mathbf{x}^{(k)} \mid k \in \mathbb{N}\rangle$ is bad. If $i < j$, then $\mathsf{Start}\,(\mathbf{x}^{(s_i)}) \leq_{\mathrm{E}} \mathsf{Start}\,(\mathbf{x}^{(s_j)})$ implies $\mathbf{x}^{(s_i)} \leq_{\mathrm{E}} \mathbf{x}^{(s_j)}$ because $\mathsf{Last}\,(\mathbf{x}^{(s_i)}) = \mathsf{Last}\,(\mathbf{x}^{(s_j)}) = a$ and a already occurs both in $\mathsf{Start}\,(\mathbf{x}^{(s_i)})$ and in $\mathsf{Start}\,(\mathbf{x}^{(s_j)})$. This again contradicts the badness of $\langle \mathbf{x}^{(k)} \mid k \in \mathbb{N}\rangle$. Hence $\langle \mathbf{y}^{(k)} \mid k \in \mathbb{N}\rangle$ is bad. However, since $\mathbf{y}^{(s_1)} = \mathsf{Start}\,(\mathbf{x}^{(s_1)}) <_E \mathbf{x}^{(s_1)}$, this contradicts the choice of $\langle \mathbf{x}^{(k)} \mid k \in \mathbb{N}\rangle$ as a minimal bad sequence. Hence $\langle A^+, \leq_{\mathrm{E}}\rangle$ is well partially ordered. ☐

For $\mathbf{a}, \mathbf{b} \in A^+$ with $\mathbf{a} \leq_{\mathrm{E}} \mathbf{b}$ we observe a correspondence between the elements that are lexicographically smaller than $\mathbf{a}$ and certain elements that are lexicographically smaller than $\mathbf{b}$. But before that we need to introduce some notation.

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

$$T_{\mathbf{a},\mathbf{b},h}(\mathbf{x})\,(j) := x_i,$$

where $i \in \{1, \dots, m\}$ is such that $h(i) = j$. If $j \notin \mathrm{range}(h)$, then

$$T_{\mathbf{a},\mathbf{b},h}(\mathbf{x})\,(j) := x_i,$$

where $i := \mathsf{firstOcc}\,(\mathbf{a}, b_j)$.

Lemma 3.4. *Let $t \in \mathbb{N}$, let $A = \{1, 2, \dots, t\}$, and let $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$ with $h : \{1, \dots, m\} \to \{1, \dots, n\}$ witnessing $\mathbf{a} \leq_{\mathrm{E}} \mathbf{b}$. Let $\mathbf{c} \in A^m$ be such that $\mathbf{c} <_{\mathrm{lex}} \mathbf{a}$. Then we have*

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

Proof: (1) follows immediately from the definition of $T_{\mathbf{a},\mathbf{b},h}$. For proving (2), let k be the index of the first place in which $\mathbf{c}$ differs from $\mathbf{a}$. Hence $\mathbf{c} = (a_1, \dots, a_{k-1}, c_k, c_{k+1}, \dots)$, $\mathbf{a} = (a_1, \dots, a_{k-1}, a_k, a_{k+1}, \dots)$, and $c_k < a_k$.

We first show that for all $j < h(k)$, we have $T_{\mathbf{a},\mathbf{b},h}(\mathbf{c})(j) = T_{\mathbf{a},\mathbf{b},h}(\mathbf{a})(j)$. If j is in the range of h, there is an i with $h(i) = j$, and we have $T_{\mathbf{a},\mathbf{b},h}(\mathbf{c})(j) = c_i$ and $T_{\mathbf{a},\mathbf{b},h}(\mathbf{a})(j) = a_i$. Since $h(i) < h(k)$, we have $i < k$. Thus $c_i = a_i$, since k is the first index at which $\mathbf{c}$ and $\mathbf{a}$ differ. We now consider the case that

j is not in the range of h. Since $\{b_1, \ldots, b_n\} = \{a_1, \ldots, a_m\}$, we have that $i := \mathsf{firstOcc}\,(\mathbf{a}, b_j)$ satisfies $i > 0$. By the definition of $\leq_{\mathrm{E}}$ we have $h(i) = \mathsf{firstOcc}\,(\mathbf{b}, b_j)$ and therefore $h(i) \leq j$. Hence $h(i) < h(k)$ and $i < k$. Thus $c_i = a_i$. Since $T_{\mathbf{a},\mathbf{b},h}(x_1, \ldots, x_m)(j) := x_i$ for all $\mathbf{x} \in A^m$, we finally obtain $T_{\mathbf{a},\mathbf{b},h}(\mathbf{c})(j) = T_{\mathbf{a},\mathbf{b},h}(\mathbf{a})(j)$.

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

4. Algebras with edge term

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

$$\pi_T(\mathbf{a}) := \langle a_i \mid i \in T \rangle.$$

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

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

By [Aic09, Lemma 3.1] a subuniverse G of a Malcev algebra $\mathbf{A}^m$ 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 φ_i and projections π_T occur in the description of small generating sets for the subuniverses of $\mathbf{A}^m$ for a finite algebra $\mathbf{A}$ with edge term operation. These generating sets were then used to obtain a bound on the number of subuniverses of $\mathbf{A}^m$. 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 $\mathbf{A}$ be a finite algebra with k-edge term operation t, and let F, G be subuniverses of $\mathbf{A}^m$ 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 let d be the binary term function on $\mathbf{A}$ that is defined from t in Lemma 2.13 of [BIM+10]. We also need the notion of a *signature* Sig_R of a subset R of A^m,

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

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 $\mathrm{Sig}_F = \mathrm{Sig}_G$. Thus F is a representation of G. Since F, G are subuniverses of $\mathbf{A}^m$, 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 [Aic09], 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 $A = \{1, 2, \ldots, t\}$, and let $n \in \mathbb{N}$. Let $C^{[n]}$ denote the set of n-ary functions in C. As in [Aic09], for $\mathbf{a} \in A^n$, we define a binary relation $\varphi(C, \mathbf{a})$ on A by

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

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

$$\lambda(C, (c, d)) := \{\mathbf{a} \in A^+ \mid (c, d) \notin \varphi(C, \mathbf{a})\}.$$

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

Lemma 5.1. *Let $t, m, n \in \mathbb{N}$, let C be a clone on the t-element set $A = \{1, 2, \ldots, t\}$, and let $\mathbf{a} \in A^m$, $\mathbf{b} \in A^n$ such that $\mathbf{a} \leq_{\text{E}} \mathbf{b}$. Then $\varphi(C, \mathbf{b}) \subseteq \varphi(C, \mathbf{a})$.*

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

$$\begin{aligned} f_1(\mathbf{x}) &:= f(T_{\mathbf{a},\mathbf{b},h}(\mathbf{x})) \\ g_1(\mathbf{x}) &:= g(T_{\mathbf{a},\mathbf{b},h}(\mathbf{x})) \end{aligned}$$

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

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

Lemma 5.2. *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 $\langle A^+, \leq_{\mathrm{E}}\rangle$.*

Proof: Let $\mathbf{a} \in \lambda(C,(c,d))$, and let $\mathbf{b} \in A^+$ such that $\mathbf{a} \leq_{\mathrm{E}} \mathbf{b}$. Since $(c,d) \notin \varphi(C,\mathbf{a})$, Lemma 5.1 yields $(c,d) \notin \varphi(C,\mathbf{b})$ and thus $\mathbf{b} \in \lambda(C,(c,d))$. □

6. Relations

A finitary *relation* ρ 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* ρ if ρ is a subuniverse of $\langle A, f\rangle^I$.

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

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

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

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

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 $\mathbf{A} := \langle A, C\rangle$. Let $m := \max\{|\mathbf{a}| \mid$ there exists $(c,d) \in A^2$ such that $\mathbf{a}$ is minimal with respect to $\leq_E$ in $\lambda(C,(c,d))\}$. Then m is finite, and C is the clone of functions that preserve the relation $C^{[m]}$ and every subuniverse of $\mathbf{A}^{k-1}$.*

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 functions our result resembles the Baker-Pixley Theorem (see Theorem 2.1 (5) in [BP75]) 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 maximum of finitely many natural numbers, m is finite.

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

$$\lambda(C,(c,d)) \subseteq \lambda(D,(c,d)). \tag{6.1}$$

Let $\mathbf{a}$ be minimal in $\lambda(C,(c,d))$. Then $(c,d) \notin \varphi(C,\mathbf{a})$. By definition, m is at least the length $|\mathbf{a}|$ of $\mathbf{a}$. Hence $C^{[|\mathbf{a}|]} = D^{[|\mathbf{a}|]}$, which implies that $\varphi(C,\mathbf{a}) = \varphi(D,\mathbf{a})$.

Thus $\mathbf{a} \in \lambda(D, (c, d))$. 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 5.2, 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 $\mathbf{a} \in A^n$ we have

$$\varphi(D, \mathbf{a}) \subseteq \varphi(C, \mathbf{a}) \tag{6.2}$$

by (6.1).

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

$$\pi_T(F) = \pi_T(G). \tag{6.3}$$

Clearly $\pi_T(F) \subseteq \pi_T(G)$. For proving the converse inclusion let $g \in G$, let $l := |T|$, and let $T = \{t_1, \ldots, t_l\} = \{(a_{11}, \ldots, a_{1n}), \ldots, (a_{l1}, \ldots, a_{ln})\}$. We know that g preserves the subuniverse B of $\mathbf{A}^l$ that is generated by $\{(a_{11}, \ldots, a_{l1}), \ldots, (a_{1n}, \ldots, a_{ln})\}$. From $(g(t_1), \ldots, g(t_l)) \in B$, we obtain an n-ary term function f of $\mathbf{A}$ 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 $F = G$. □

For a finite set A and a set S of finitary relations on A, we will write $\mathrm{Pol}\,(A, S)$ 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 we have:*

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

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 $C = \mathrm{Pol}\,(A, S)$. By [PK79, p. 50], there is a single finitary relation R on A with $\mathrm{Pol}\,(A, S) = \mathrm{Pol}\,(A, \{R\})$.

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

(3) Every finitary relation on the finite set A is a finite subset of the countable set A^+. Hence the claim follows from (1). □

7. Concluding remarks

Using [Idz99] and [KS09, Corollary 4.10] together with Theorem 6.2 (3), we obtain that the number of clones with k-edge term for a fixed integer $k > 1$ on a finite set A is finite if $|A| \leq 3$, and countably infinite if $|A| \geq 4$.

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.

8. Acknowledgments

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

[Aic09] E. Aichinger, *Constantive Mal'cev clones on finite sets are finitely related*, to appear in Proceedings AMS.

[AM10] E. Aichinger and N. Mudrinski, *Polynomial clones of Mal'cev algebras with small congruence lattices*, Acta Math. Hungar. **126** (2010), no. 4, 315–333.

[Bar09] L. Barto, *CD implies NU*, Manuscript, 2009.

[BD06] A. Bulatov and V. Dalmau, *A simple algorithm for Mal'tsev constraints*, SIAM J. Comput. **36** (2006), no. 1, 16–27 (electronic).

[BIM+10] J. Berman, P. Idziak, P. Marković, R. McKenzie, M. Valeriote, and R. Willard, *Varieties with few subalgebras of powers*, Transactions of the American Mathematical Society **362** (2010), no. 3, 1445–1473.

[BP75] K.A. Baker and A.F. Pixley, *Polynomial interpolation and the Chinese remainder theorem for algebraic systems*, Math. Z. **143** (1975), no. 2, 165–174.

[BS81] S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Springer New York Heidelberg Berlin, 1981.

[Bul01] A. Bulatov, *On the number of finite Mal'tsev algebras*, Contributions to general algebra, 13 (Velké Karlovice, 1999/Dresden, 2000), Heyn, Klagenfurt, 2001, pp. 41–54.

[Hig52] G. Higman, *Ordering by divisibility in abstract algebras*, Proc. London Math. Soc. (3) **2** (1952), 326–336.

[HM88] D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemporary mathematics, vol. 76, American Mathematical Society, 1988.

[Idz99] P. M. Idziak, *Clones containing Mal'tsev operations*, Internat. J. Algebra Comput. **9** (1999), no. 2, 213–226.

[IMM+07] P. Idziak, P. Marković, R. McKenzie, M. Valeriote, and R. Willard, *Tractability and learnability arising from algebras with few subpowers*, Proceedings of the 22nd

Annual IEEE Symposium on Logic in Computer Science (LICS 2007), 2007, pp. 221–230.

[JM59] Ju. I. Janov and A. A. Mučnik, *Existence of k-valued closed classes without a finite basis*, Dokl. Akad. Nauk SSSR **127** (1959), 44–46.

[KP92] E. W. Kiss and P. Pröhle, *Problems and results in tame congruence theory. A survey of the '88 Budapest Workshop*, Algebra Universalis **29** (1992), no. 2, 151–171.

[KS05] K. A. Kearnes and Á. Szendrei, *Clones of finite groups*, Algebra Universalis **54** (2005), no. 1, 23–52.

[KS09] ______, *Clones of algebras with parallelogram terms*, Preprint, 2009.

[Lav76] Richard Laver, *Well-quasi-orderings and sets of finite sequences*, Math. Proc. Cambridge Philos. Soc. **79** (1976), no. 1, 1–10.

[Mal54] A. I. Mal'cev, *On the general theory of algebraic systems*, Mat. Sb. N.S. **35(77)** (1954), 3–20.

[May08] P. Mayr, *Polynomial clones on squarefree groups*, Internat. J. Algebra Comput. **18** (2008), no. 4, 759–777.

[MM08] P. Marković and R. McKenzie, *Few subpowers, congruence distributivity and near-unanimity terms*, Algebra Universalis **58** (2008), no. 2, 119–128.

[MMT87] R. N. McKenzie, G. F. McNulty, and W. F. Taylor, *Algebras, lattices, varieties, volume I*, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, California, 1987.

[NW63] C. St. J. A. Nash-Williams, *On well-quasi-ordering finite trees*, Proc. Cambridge Philos. Soc. **59** (1963), 833–835.

[PK79] R. Pöschel and L. A. Kalužnin, *Funktionen- und Relationenalgebren*, Mathematische Monographien [Mathematical Monographs], vol. 15, VEB Deutscher Verlag der Wissenschaften, Berlin, 1979, Ein Kapitel der diskreten Mathematik. [A chapter in discrete mathematics].

[Pos41] E. L. Post, *The two-valued iterative systems of mathematical logic.*, (Annals of Mathematics Studies. 5) Princeton, N.J.: Princeton University Press, VIII, 122 p., 1941.

[Sze86] Á. Szendrei, *Clones in universal algebra*, Séminaire de Mathématiques Supérieures [Seminar on Higher Mathematics], vol. 99, Presses de l'Université de Montréal, Montreal, QC, 1986.

Erhard Aichinger, Institut für Algebra, Johannes Kepler Universität Linz, 4040 Linz, Austria

E-mail address: erhard@algebra.uni-linz.ac.at

Peter Mayr, Centro de Álgebra da Universidade de Lisboa (CAUL), Av. Prof. Gama Pinto, 2, 1649-003 Lisboa, Portugal & Institut für Algebra, Johannes Kepler Universität Linz, 4040 Linz, Austria

E-mail address: stein@cii.fc.ul.pt

Ralph McKenzie, Department of Mathematics, Vanderbilt University, Nashville, Tennessee, U.S.

E-mail address: ralph.n.mckenzie@vanderbilt.edu