TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9947(XX)0000-0

VARIETIES WITH FEW SUBALGEBRAS OF POWERS

JOEL BERMAN, PAWEŁ IDZIAK, PETAR MARKOVIĆ, RALPH MCKENZIE,
MATTHEW VALERIOTE, AND ROSS WILLARD

Abstract. The *Constraint Satisfaction Problem Dichotomy Conjecture* of Feder and Vardi [12] has in the last 10 years been profitably reformulated as a conjecture about the set $\mathsf{SP}_{\mathsf{fin}}(\mathbf{A})$ of subalgebras of finite Cartesian powers of a finite universal algebra $\mathbf{A}$ [20, 5]. One particular strategy, advanced by Dalmau in his doctoral thesis [8], has confirmed the conjecture for a certain class of finite algebras $\mathbf{A}$ which, among other things, have the property that the number of subalgebras of $\mathbf{A}^n$ is bounded by an exponential polynomial. In this paper we characterize the finite algebras $\mathbf{A}$ with this property, which we call *having few subpowers*, and develop a representation theory for the subpowers of algebras having few subpowers. Our characterization shows that algebras having few subpowers are the finite members of a newly discovered and surprisingly robust Maltsev class defined by the existence of a special term we call an *edge term*. We also prove some tight connections between the asymptotic behavior of the number of subalgebras of $\mathbf{A}^n$ and some related functions on the one hand, and some standard algebraic properties of $\mathbf{A}$ on the other. The theory developed here was applied to the Constraint Satisfaction Problem Dichotomy Conjecture in [18], completing Dalmau's strategy.

0. Introduction

One approach to assessing the complexity of a class of structures is to count the number of members according to some type of measure. The rate of growth of the associated counting function can then be used to gauge the complexity of the class. Ideally, there should be some strong correlation between classes with low complexity and nice structural properties of the members of the class.

Perhaps the most celebrated example of this type of phenomenon is due to Shelah [26]. For a class $\mathcal{C}$ of structures and κ a cardinal, $I(\mathcal{C}, \kappa)$, the spectrum function of $\mathcal{C}$, denotes the number of members of $\mathcal{C}$ of cardinality κ, up to isomorphism. The study of the spectra of first order definable classes has a rich history and a number of classic results of model theory can be expressed in terms of spectra. For example, in [24], Morley proves that if $\mathcal{C}$ is a class defined by a countable first order theory and $I(\mathcal{C}, \kappa) = 1$ for some uncountable κ, then $I(\mathcal{C}, \kappa) = 1$ for all uncountable κ. For such a first order class, it is not hard to see that $I(\mathcal{C}, \kappa) \leq 2^{2^\kappa}$

Received by the editors January, 2008.
2000 *Mathematics Subject Classification.* 08B05, 08B10, 08A30, 08A70, 68Q25, 68Q32 68W30.
Key words and phrases. Maltsev condition, variety, constraint satisfaction problem.
The second author was supported by grant no. N206 2106 33 of the Polish Ministry of Science, the third author was supported by grant no. 144011G of the Ministry of Science and Environment of Serbia, the fourth author was supported by a grant from the US National Science Foundation, no. DMS-0245622, and the last two authors were supported by the NSERC of Canada.

for all infinite κ. In [26], Shelah provides a complete list of structural properties that captures those first order classes whose spectra fail to attain this maximum for some uncountable cardinal. It turns out that for these classes there is a useful, albeit abstract, notion of dimension that can be applied to their models. In the realm of general algebra a much stronger structural result has been obtained. In [16], Hart, Starchenko, and Valeriote show that if the spectrum function of a variety over a countable language (a variety is a class of algebras of the same type defined by a set of equations) fails to attain the maximum possible value for some infinite cardinal then the variety decomposes in a strong sense as the product of a variety of essentially unary multi-sorted algebras and a variety of modules over some ring.

If one is interested in gauging the complexity of a variety by the number of its finite members then a successful approach has been developed by Berman and Idziak [2] using the G-spectrum. For a variety $\mathcal{V}$ and natural number k, $G_{\mathcal{V}}(k)$ is defined to be the number of at most k-generated members of $\mathcal{V}$, up to isomorphism. In general this function counts finitely generated members, not finite members, but if $\mathcal{V}$ is locally finite (i.e., all finitely generated members of $\mathcal{V}$ are finite), then the function $G_{\mathcal{V}}$ does indeed count finite members and is in addition integer-valued. Berman and Idziak establish strong connections between the rate of growth of the G-spectrum of a locally finite variety and structural properties (both local and global) of its members. In [19] Idziak, McKenzie, and Valeriote show that if $\mathcal{V}$ is a locally finite variety whose G-spectrum is bounded above by a polynomial then a decomposition similar to that mentioned in the previous paragraph is obtained.

In this paper we develop another approach to counting finite algebras and use it to define a novel and deeply interesting class of algebras that is closely tied to some more familiar sorts of algebras and varieties. We also point out the surprising connection that this class of algebras has to two current topics in computer science: constraint satisfaction, and learnability. This connection is fully developed in the companion paper [18]. For the necessary background in general algebra the reader is referred to [23] or [6] and for an overview of the theory of Maltsev conditions, Chapter 5 of [14].

Definition 0.1. Let $\mathbf{A}$ be a finite algebra and n a positive integer. $\mathrm{s}_{\mathbf{A}}(n)$ is defined to be the logarithm, base 2, of the cardinality of the set of subuniverses of $\mathbf{A}^n$.

We note that for a finite algebra $\mathbf{A}$ there are at most $2^{|A|^n}$ subuniverses of $\mathbf{A}^n$ and so $\mathrm{s}_{\mathbf{A}}(n) \leq |A|^n$ for all $n > 0$.

Definition 0.2. We say that a finite algebra $\mathbf{A}$ has *few subpowers* iff $\mathrm{s}_{\mathbf{A}}(n) \in O(n^k)$ for some $k \in N$. We say that $\mathbf{A}$ has *many subpowers* if there exists a real number $c > 1$ such that $c^n \in O(\mathrm{s}_{\mathbf{A}}(n))$.

Closely related to the function $\mathrm{s}_{\mathbf{A}}$ are the following two functions.

Definition 0.3. For a finite algebra $\mathbf{A}$ and positive integer n,

- $\mathrm{g}_{\mathbf{A}}(n)$ is defined to be the least integer κ such that every subuniverse of $\mathbf{A}^n$ has an at most κ-element generating set.
- $\mathrm{i}_{\mathbf{A}}(n)$ is the least integer κ such that every independent subset of $\mathbf{A}^n$ has at most κ elements (where $X \subseteq A^n$ is independent iff no proper subset of X generates the same subalgebra of $\mathbf{A}^n$ as does X).

The growth rates of $\mathrm{s}_{\mathbf{A}}(n)$, $\mathrm{g}_{\mathbf{A}}(n)$, and $\mathrm{i}_{\mathbf{A}}(n)$ are closely linked (Proposition 1.2); in particular, if any one of them is bounded above by a polynomial (bounded below

by an exponential function), then so are the other two. Using this observation, we can quickly identify two special classes of finite algebras that have few subpowers. First, it is easy to see that $g_{\mathbf{G}}(n) \leq cn$ where $c = \log_2 |G|$ whenever $\mathbf{G}$ is a finite group. Thus every finite group has few subpowers, and the same argument holds for any expansion of a finite group by additional operations. By much more complicated arguments, and motivated by problems in theoretical computer science, Bulatov and Dalmau [4] have shown that this result can be extended to any finite algebra which has a so-called "Maltsev term" (see the comment following Theorem 4.8 for the definition; $\mathbf{A}$ having a Maltsev term is equivalent to every algebra in the variety $\mathsf{HSP}(\mathbf{A})$ generated by $\mathbf{A}$ having permuting congruences).

Second, the Baker-Pixley theorem easily implies that $s_{\mathbf{A}}(n) \leq \binom{n}{k-1}|A|^{k-1}$ whenever $\mathbf{A}$ is a finite algebra having a k-ary "near unanimity term" (for the definition, see Example 2.2(2); this is a special class of algebras generalizing lattices and boolean algebras). Thus every finite algebra having a near unanimity term has few subpowers. Extending these two classes, Dalmau [9] introduced a novel but somewhat ad hoc common generalization of Maltsev term and near unanimity term, called a *gmm term*, and showed that any finite algebra having such a term has few subpowers.

One of the chief results of our paper is the discovery of a simple Maltsev property that is a natural generalization of having a Maltsev term and having a near unanimity term, and is equivalent in finite algebras to having few subpowers (Corollary 3.11). We show that this property implies the fundamentally important property that congruence lattices are modular (Theorem 4.9 and Theorem 4.2) and point out that the converse does not hold (see Section 6). We also show that the subalgebra functions and their growth rates have surprising connections to other properties traditionally studied in general algebra. For example, we show that for a finite algebra $\mathbf{A}$, $i_{\mathbf{A}}(n) \in O(n)$ iff $\mathsf{HSP}(\mathbf{A})$ has permuting congruences; and if $\mathsf{HSP}(\mathbf{A})$ does not have permuting congruences, then $i_{\mathbf{A}}(n) \in \Omega(n^2)$ (Theorem 4.9). Furthermore, $\mathsf{HSP}(\mathbf{A})$ is arithmetical (i.e., the congruence lattices of algebras in $\mathsf{HSP}(\mathbf{A})$ are distributive and permutable) iff $s_{\mathbf{A}}(n) =_\Theta n\log(n)$; and if $\mathsf{HSP}(\mathbf{A})$ is not arithmetical, then $s_{\mathbf{A}}(n) \in \Omega(n^2)$ (Theorem 4.10).

We shall see that the subalgebra functions exhibit sharp dichotomies. Perhaps the most striking result of this paper is Theorem 3.12, which implies that for a finite nontrivial algebra $\mathbf{A}$, either $i_{\mathbf{A}}(n) =_\Theta n^k$ for some (unique) integer $k \geq 1$, or $i_{\mathbf{A}}(n) \in \Omega(c^n)$ for some $c > 1$, and we show that every possibility is realized by a 2-element algebra.

The paper [18] applies our main results to two areas of computer science: the constraint satisfaction problem (CSP), and learnability. While the collection of all constraint satisfaction problems is known to form an NP-complete class, there are natural subclasses, parametrized by finite algebras, or more generally, constraint languages, that turn out to be tractable. Feder and Vardi [12] conjecture that any subclass of the CSP defined by a constraint language is either NP-complete or can be solved in polynomial time. Determining whether this dichotomy holds is one of the main objectives in current research on the CSP. Using Corollary 3.11 and the theory of compact representations that we develop in Section 3 it is shown in [18] that the CSP and learnability problem classes that arise from finite algebras with few subpowers can be solved in polynomial time. These results provide support for the Dichotomy Conjecture and extend earlier work on the CSP and learnability by

Bulatov, Chen, Dalmau, and Jeavons [3, 4, 7, 8, 9, 10] and also settle conjectures of Chen and Dalmau. We note that their work anticipates the theory we develop in Section 3.

In Section 5 of this paper we introduce and study companion functions to the three subalgebra functions defined earlier. These invariants deal with congruences and congruence generation and, as we show, their behaviour is closely correlated with the types of congruence identities that the variety generated by an algebra satisfies. The final section of the paper presents examples of algebras over the set $\{0, 1\}$ to illustrate the types of functions that can arise as one of our six invariants.

1. Basic results

Since we are interested in the rate of growth of functions we introduce some useful notation.

Definition 1.1. Let $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$ and suppose $f, g : \mathbb{N}^+ \to [0, \infty)$.

- $f \in O(g)$ denotes (as usual) that for some positive c, $f(n) \leq cg(n)$ for all sufficiently large $n \in \mathbb{N}^+$.
- $f \in \Omega(g)$ signifies $g \in O(f)$, and $f =_\Theta g$ signifies that $f \in O(g)$ and $g \in O(f)$.
- $f \in L(g)$ denotes that for some positive integer ℓ, $f(n) \leq g(\ell n)$ for all sufficiently large $n \in \mathbb{N}^+$. $f =_L g$ signifies that $f \in L(g)$ and $g \in L(f)$.

It may be easily shown that for a fixed $k \in \mathbb{N}^+$ we have (i) $O(n^k) = L(n^k)$, (ii) $n^k \in O(f)$ implies $n^k \in L(f)$ for any function f, and (iii) the converse holds if f is non-decreasing. Furthermore, for any functions f, g,

(iv) $f \in L(g)$ iff $L(f) \subseteq L(g)$;
(v) $2^n \in L(f)$ iff $c^n \in O(f)$ for some real number $c > 1$, if f is non-decreasing.

The following proposition lists some of the easily established, basic connections between the three subalgebra functions. Throughout the paper, $\lg(x)$ denotes the logarithm of x, base 2.

Proposition 1.2. *For any finite algebra* $\mathbf{A}$ *with* $|A| > 1$*, and for any* $n \in \mathbb{N}^+$ *we have*:

(0) $\mathrm{s}_\mathbf{A}, \mathrm{g}_\mathbf{A}, \mathrm{i}_\mathbf{A}$ *are non-decreasing functions.*
(1) $\mathrm{g}_\mathbf{A}(n) \leq \mathrm{i}_\mathbf{A}(n) \leq \mathrm{s}_\mathbf{A}(n)$.
(2) $c \cdot n \lg(n) \leq \mathrm{s}_\mathbf{A}(n) \leq d \cdot n\, \mathrm{g}_\mathbf{A}(n)$ *where* c *is a positive constant and* $d = \lg(|A|)$*, and* $n - 1 \leq \mathrm{i}_\mathbf{A}(n)$.
(3) $\mathrm{s}_\mathbf{A}(n) \leq |A|^n$ (*and* $\mathrm{s}_\mathbf{A}(n) = \mathrm{i}_\mathbf{A}(n) = \mathrm{g}_\mathbf{A}(n) = |A|^n$ *if* $\mathbf{A}$ *has no operations*).
(4) *If* $\mathbf{B}$ *is any finite algebra in* $\mathsf{HSP}(\mathbf{A})$ *then* $\mathrm{s}_\mathbf{B} \in L(\mathrm{s}_\mathbf{A})$, $\mathrm{g}_\mathbf{B} \in L(\mathrm{g}_\mathbf{A})$*, and* $\mathrm{i}_\mathbf{B} \in L(\mathrm{i}_\mathbf{A})$.

For statement (2), notice that the number of subuniverses of $\mathbf{A}^n$ is no less than the nth Bell number $B(n)$ — the number of equivalence relations on n — and it is known that $\lg(B(n)) =_\Theta n \lg(n)$. That $n - 1 \leq \mathrm{i}_\mathbf{A}(n)$ can be proved by picking distinct $0, 1 \in A$, defining $\overline{u}^{(i)}$ to be the element of A^n which is equal to 1 at coordinate i and 0 at all other coordinates, and noting that $\{\overline{u}^{(2)}, \ldots, \overline{u}^{(n)}\}$ is necessarily an independent subset of $\mathbf{A}^n$.

Note that it follows from Proposition 1.2(4) that the $=_L$ equivalence class of each function $\mathrm{s}_\mathbf{A}$, $\mathrm{g}_\mathbf{A}$, $\mathrm{i}_\mathbf{A}$ is an invariant of the variety generated by $\mathbf{A}$.

2. Edge term identities and related identities

We begin this section by introducing the Maltsev property that we will later see characterizes having few subpowers.

Definition 2.1. Suppose $\mathcal{V}$ is a variety and k is an integer, $k \geq 2$. A term t in $k+1$ variables is called a *k-edge term* for $\mathcal{V}$ if the following k identities are true in $\mathcal{V}$:

$$\begin{aligned} t(y,y,x,x,x,\ldots,x) &\approx x \\ t(y,x,y,x,x,\ldots,x) &\approx x \\ t(x,x,x,y,x,\ldots,x) &\approx x \\ t(x,x,x,x,y,\ldots,x) &\approx x \\ &\vdots \\ t(x,x,x,x,x,\ldots,y) &\approx x. \end{aligned}$$

A term is a k-edge term for an algebra $\mathbf{A}$ iff it is a k-edge term for the variety $\mathcal{V}(\mathbf{A}) = \mathsf{HSP}(\mathbf{A})$ generated by $\mathbf{A}$.

Examples 2.2.

(1) A 2-edge term for a variety is a term $t(x,y,z)$ satisfying $t(y,y,x) \approx x$ and $t(y,x,y) \approx x$. Modulo interchanging the first and second variables, these are the identities that define a Maltsev term. Hence every variety (or algebra) with a Maltsev term has a 2-edge term and vice versa.

(2) For $k \geq 3$, a k-ary term $m(x_1,\ldots,x_k)$ is a *near unanimity term* for a variety $\mathcal{V}$ if for each $i = 1,2,\ldots,k$, we have

$$\mathcal{V} \models m(x,x,\ldots,x,\underset{\substack{\uparrow \\ i}}{y},x,\ldots,x) \approx x$$

If $k \geq 3$ and $m(x_1,\ldots,x_k)$ is a k-ary near unanimity term for $\mathcal{V}$, then $t(x_1,x_2,\ldots,x_{k+1}) := m(x_2,\ldots,x_{k+1})$ is a k-edge term for $\mathcal{V}$. Hence every variety (or algebra) having a k-ary near unanimity term has a k-edge term.

We see from the above examples that having a k-edge term (for some $k \geq 2$) simultaneously generalizes having a Maltsev term and having a near unanimity term. As noted in the Introduction, these two examples also happen to be classes of finite algebras previously known to have few subpowers.

Proposition 2.3. *Suppose $\mathbf{A}$ is a finite algebra.*

(1) *If $\mathbf{A}$ has a Maltsev term, then $\mathrm{g}_{\mathbf{A}}(n) \in O(n)$.*
(2) *If $\mathbf{A}$ has a k-ary near unanimity term, then $\mathrm{s}_{\mathbf{A}}(n) \in O(n^{k-1})$.*

Proof. (1) follows from Lemma 3.1 of [4], while (2) follows from Theorem 2.1 of [1]. •

Maltsev terms, near unanimity terms, and k-edge terms are special cases of a more general class of terms we call *Δ-special cube terms*. Before defining them, we describe one further special case. For the remainder of this section,

- $\mathcal{V}$ is a fixed nontrivial variety,
- k is a fixed integer, $k \geq 2$,
- $\mathbf{F}$ is the free algebra in $\mathcal{V}$ freely generated by two distinct elements x, y.
- $[k] = \{1,2,\ldots,k\}$.

- Ω_k is the set of all non-void subsets of $[k]$.

Definition 2.4. For $S \subseteq [k]$, let $C_S : [k] \to \{x, y\}$ be the function defined by $C_S(i) = y \leftrightarrow i \in S$ for all $i \in [k]$. We regard C_S as an element of F^k.

Definition 2.5. Suppose $t(\overline{x})$ is a term in the language of $\mathcal{V}$ having $2^k - 1$ variables $\overline{x} = \langle x_S \rangle_{S \in \Omega_k}$ indexed by Ω_k. We say that t is a *k-dimensional cube term* (or a *k-cube term*) for $\mathcal{V}$ iff

$$(\dagger) \qquad t^{\mathbf{F}^k}(\langle C_S \rangle_{S \in \Omega_k}) = C_\varnothing.$$

Clearly the equation (†) can be reformulated in terms of the satisfaction of some identities in $\mathcal{V}$, by evaluating (†) at each coordinate $i \in [k]$ and applying the universal properties of $\mathbf{F}$ in $\mathcal{V}$. For $i \in [k]$ and $S \in \Omega_k$ set $v^i_S = C_S(i) \in \{x, y\}$, and let ε^i_t denote the identity

$$t(\langle v^i_S \rangle_{S \in \Omega_k}) \approx x.$$

Then the term $t(\overline{x})$ is a k-cube term for $\mathcal{V}$ iff each of the identities $\varepsilon^1_t, \ldots, \varepsilon^k_t$ is valid in $\mathcal{V}$. These identities are rather unwieldy; nonetheless, it may be instructive to display the k-cube identities for small values of k. To do this, we need to choose a linear ordering of Ω_k; we adopt the convention that S_1 precedes S_2 iff C_{S_1} precedes C_{S_2} lexicographically. Thus when $k = 2$, the definition of a 2-cube term requires that $t^{\mathbf{F}^2}(C_{\{2\}}, C_{\{1\}}, C_{\{1,2\}}) = C_\varnothing$, i.e., that $t^{\mathbf{F}^2}((x, y), (y, x), (y, y)) = (x, x)$, which is equivalent to the satisfaction in $\mathcal{V}$ of the identities

$$\begin{aligned} \varepsilon^1_t &: t(x, y, y) \approx x \\ \varepsilon^2_t &: t(y, x, y) \approx x. \end{aligned}$$

Thus a 2-cube term is just a 2-edge term (modulo switching its first and third variables) and hence is a Maltsev term (modulo switching its second and third variables). Similarly, a 3-cube term for $\mathcal{V}$ is a term t in seven variables satisfying $t^{\mathbf{F}^3}(C_{\{3\}}, C_{\{2\}}, C_{\{2,3\}}, C_{\{1\}}, C_{\{1,3\}}, C_{\{1,2\}}, C_{\{1,2,3\}}) = C_\varnothing$, i.e.,

$$t^{\mathbf{F}^3}((x, x, y), (x, y, x), (x, y, y), (y, x, x), (y, x, y), (y, y, x), (y, y, y)) = (x, x, x),$$

which is equivalent to the satisfaction in $\mathcal{V}$ of the identities

$$\begin{aligned} \varepsilon^1_t &: t(x, x, x, y, y, y, y) \approx x \\ \varepsilon^2_t &: t(x, y, y, x, x, y, y) \approx x \\ \varepsilon^3_t &: t(y, x, y, x, y, x, y) \approx x. \end{aligned}$$

And a 4-cube term for $\mathcal{V}$ is a term t in 15 variables satisfying the identities

$$\begin{aligned} \varepsilon^1_t &: t(x, x, x, x, x, x, x, y, y, y, y, y, y, y, y) \approx x \\ \varepsilon^2_t &: t(x, x, x, y, y, y, y, x, x, x, x, y, y, y, y) \approx x \\ \varepsilon^3_t &: t(x, y, y, x, x, y, y, x, x, y, y, x, x, y, y) \approx x \\ \varepsilon^4_t &: t(y, x, y, x, y, x, y, x, y, x, y, x, y, x, y) \approx x. \end{aligned}$$

Proposition 2.6. *Assume that $\mathcal{V}$ is 2-finite (i.e., $\mathbf{F} = \mathbf{F}_\mathcal{V}(2)$ is finite) and $k \geq 2$.*

1. *If $\mathrm{i}_\mathbf{F}(k) < 2^k$, then $\mathcal{V}$ has a k-cube term.*
2. *If there exists $m \geq k$ such that $\mathrm{i}_\mathbf{F}(m) < \binom{m}{k}$, then $\mathcal{V}$ has a k-cube term.*

Proof. The subset $X = \{C_S : S \subseteq [k]\}$ of $\mathbf{F}^k$ has size 2^k. Hence if $\mathrm{i}_{\mathbf{F}}(k) < 2^k$, then X is too large to be independent, so there exists $S_0 \subseteq [k]$ such that $C_{S_0} \in \mathrm{Sg}^{\mathbf{F}^k}(\{C_S : S \subseteq [k], S \neq S_0\})$. Since $\mathrm{Aut}(\mathbf{F}^k)$ acts transitively on $\{C_S : S \subseteq [k]\}$, we can assume that $S_0 = \varnothing$. Hence

$$C_\varnothing \in \mathrm{Sg}^{\mathbf{F}^k}(\{C_S : S \in \Omega_k\}),$$

which implies $\mathcal{V}$ has a k-cube term, proving item (1).

To prove (2), we modify the above argument. Assume $m \geq k$ and $\mathrm{i}_{\mathbf{F}}(m) < \binom{m}{k}$. Let Φ be the set of all k-element subsets of $[m]$, and for each $T \in \Phi$ define $D_T \in \{x, y\}^m$ by $D_T(i) = x$ iff $i \in T$. The set $\{D_T : T \in \Phi\}$ is a subset of $\mathbf{F}^m$ of size $\binom{m}{k}$, so by assumption it cannot be independent. Hence there exists $T_0 \in \Phi$ such that

$$D_{T_0} \in \mathrm{Sg}^{\mathbf{F}^m}(\{D_T : T \in \Phi, T \neq T_0\}).$$

Under any identification of T_0 with $[k]$, the projection $\mathrm{proj}_{T_0} : \mathbf{F}^m \to \mathbf{F}^{T_0}$ sends D_{T_0} to $C_\varnothing$ and $\{D_T : T \in \Phi, T \neq T_0\}$ to $\{C_S : S \in \Omega_k\}$. Hence

$$C_\varnothing \in \mathrm{Sg}^{\mathbf{F}^k}(\{C_S : S \in \Omega_k\}),$$

which again implies that $\mathcal{V}$ has a k-cube term. •

We now define the general notion of Δ-special cube term for a variety.

Definition 2.7. Recall that $k \geq 2$ and Ω_k is the set of all non-void subsets of $[k]$.

(1) Suppose Δ is a nonempty subset of Ω_k, and $t(\overline{x})$ is a term whose variables are indexed by Δ. We say that t is a Δ-*special cube term for* $\mathcal{V}$ iff

$$t^{\mathbf{F}^k}(\langle C_S \rangle_{S \in \Delta}) = C_\varnothing.$$

(2) Define $\Delta^\star = \{S \subseteq [k] : |S| = 1 \text{ or } S = \{1, i\} \text{ for some } 2 \leq i \leq k\}$.
(3) Define $\Delta^e = \{\{1, 2\}, \{1\}, \{2\}, \{3\}, \{4\}, \ldots, \{k\}\}$.

Observe that $\Delta^e \subseteq \Delta^\star \subseteq \Omega_k$ (with equalities iff $k = 2$), and that a k-cube term is a Δ-special cube term where $\Delta = \Omega_k$. Just as was the case for k-cube terms, the notion of a Δ-special cube term can be reformulated in terms of k identities satisfied in $\mathcal{V}$. In particular, using the ordering of Δ^e implicit in its definition, a term t in $k + 1$ variables is a Δ^e-special cube term iff it satisfies

$$t^{\mathbf{F}^k}(C_{\{1,2\}}, C_{\{1\}}, C_{\{2\}}, C_{\{3\}}, C_{\{4\}}, \ldots, C_{\{k\}}) = C_\varnothing,$$

which is precisely equivalent to $\mathcal{V}$ satisfying the k-edge identities in Definition 2.1. In other words, a k-edge term is just a Δ^e-special cube term. (This explains our name for k-edge terms: the set Δ^e consists of the singletons and one *edge* $\{1, 2\}$.) Note also that a k-ary near unanimity term (for $k \geq 3$) is a Δ_{nu}-special cube term where $\Delta_{nu} = \{\{1\}, \{2\}, \ldots, \{k\}\}$.

In general, given $\varnothing \neq \Delta \subseteq \Omega_k$, let M_Δ denote the $(k \times \Delta)$ matrix whose (i, S)-entry $(i \in [k], S \in \Delta)$ is

$$v_S^i = C_S(i) = \begin{cases} y & \text{if } i \in S \\ x & \text{otherwise.} \end{cases}$$

Thus the Sth column of M_Δ is C_S, $S \in \Delta$. For $1 \leq i \leq k$ let $R_\Delta(i) = \langle v_S^i \rangle_{S \in \Delta}$ denote the ith row of M_Δ. Then a term t is a Δ-special cube term for $\mathcal{V}$ iff its variables are indexed by Δ and $\mathcal{V} \models t(R_\Delta(i)) \approx x$ for all $1 \leq i \leq k$.

Obviously if $\varnothing \neq \Delta \subseteq \Gamma \subseteq \Omega_k$ and $\mathcal{V}$ has a Δ-special cube term, then $\mathcal{V}$ has a Γ-special cube term. Our next goal is to prove the converse implication under suitable hypotheses. If $\varnothing \neq \Gamma \subseteq \Omega_k$, we say that Γ is an *order ideal of* $(\Omega_k, \subseteq)$ iff $\varnothing \neq T \subseteq S \in \Gamma$ implies $T \in \Gamma$.

Lemma 2.8. *Suppose Γ is an order ideal of $(\Omega_k, \subseteq)$ and $\Delta^\star \subseteq \Gamma$. Fix $2 \leq \ell \leq k$ and define*

$$\Gamma_\ell = \{S \in \Gamma \,:\, \ell \notin S\} \cup \Delta^\star.$$

If $\mathcal{V}$ has a Γ-special cube term, then $\mathcal{V}$ has a Γ_ℓ-special cube term.

Proof. We may assume with no loss of generality that $\ell = 2$. We first introduce some notation. If $a, b \in F$ then we use $\eta_{a,b}$ to denote the endomorphism of $\mathbf{F}$ which sends $x \mapsto a$ and $y \mapsto b$. We let $\eta_{a,b}$ act on powers of F in the natural way. We also write u^{dual} for $\eta_{y,x}(u)$, and $u^{a/y}$ for $\eta_{x,a}(u)$. Let $\widehat{x}$ and $\widehat{y}$ respectively denote the constant x-valued and y-valued members of F^Γ.

Now let t be a Γ-special cube term for $\mathcal{V}$. Thus the variables of t are indexed by Γ and $\mathcal{V}$ satisfies the identities $t(R_\Gamma(i)) \approx x$, $1 \leq i \leq k$, where $R_\Gamma(i) = \langle C_S(i) \rangle_{S \in \Gamma} \in \{x, y\}^\Gamma$. Hence for each $i \in [k]$:

(1) $t^{\mathbf{F}}(R_\Gamma(i)) = x$.
(2) $t^{\mathbf{F}}(R_\Gamma(i)^{\mathrm{dual}}) = y$.
(3) $t^{\mathbf{F}}(\widehat{x}) = x$.
(4) $t^{\mathbf{F}}(\widehat{y}) = y$.
(5) $t^{\mathbf{F}}(R_\Gamma(i)^{a/y}) = x$ for any $a \in F$.

Let $G = \{C_S \,:\, S \in \Gamma_2\}$ and $B = \mathrm{Sg}^{\mathbf{F}^k}(G)$. We will be done if we can prove $C_\varnothing \in B$. First, define $\overline{\delta} = \langle \delta_S \rangle_{S \in \Gamma} \in \{x, y\}^\Gamma$ by

$$\delta_S = \begin{cases} y & \text{if } S = \{2\} \\ x & \text{otherwise} \end{cases}$$

and define $a = t^{\mathbf{F}}(\overline{\delta}) \in F$. Next, for $T \subseteq [k]$ define $C_T^\circ \in F^k$ as follows:

$$C_T^\circ(i) = \begin{cases} a & \text{if } i = 2 \in T \\ C_T(i) & \text{otherwise.} \end{cases}$$

Claim 2.9. *If $T \in \Gamma$, then $C_T^\circ \in B$.*

The claim is proved via cases.

Case 1. $2 \notin T$. Then $T \in \Gamma_2$ and hence $C_T^\circ = C_T \in G \subseteq B$.

Case 2. $2 \in T \neq \{2\}$. In this case we let M denote the $(k \times \Gamma)$ matrix whose rows $M(1), \ldots, M(k)$ are given as follows:

$$\begin{aligned} M(1) &= \begin{cases} \widehat{y} & \text{if } 1 \in T \\ R_\Gamma(2) & \text{otherwise} \end{cases} \\ M(2) &= \overline{\delta} \\ M(i) &= \begin{cases} R_\Gamma(2)^{\mathrm{dual}} & \text{if } i \in T \\ \widehat{x} & \text{otherwise} \end{cases}, \ 3 \leq i \leq k. \end{aligned}$$

Observe that $t^{\mathbf{F}}(M(2)) = a$ while $t^{\mathbf{F}}(M(i)) = C_T(i)$ for $i \in [k] \setminus \{2\}$. Thus if M_S denotes the Sth column of M, then we have shown $t^{\mathbf{F}^k}(\langle M_S \rangle_{S \in \Gamma}) = C_T^\circ$. Hence we

will have proved the claim in Case 2 if we can show that each column of M is in B. One can check that for $S \in \Gamma$,

$$M_S = \begin{cases} C_{T\setminus\{2\}} & \text{if } 2 \notin S \\ C_{\{1\}} & \text{if } 2 \in S \neq \{2\} \\ C_{\{1,2\}} & \text{if } S = \{2\}. \end{cases}$$

As the hypotheses imply each of $T \setminus \{2\}, \{1\}, \{1,2\} \in \Gamma_2$, it follows that $M_S \in G \subseteq B$ for all $S \in \Gamma$, completing Case 2.

Case 3. $T = \{2\}$. Let N be the $(k \times \Gamma)$ matrix whose rows $N(1), \dots, N(k)$ are given by $N(2) = \overline{\delta}$ and $N(i) = R_\Gamma(i)$ for $i \neq 2$. By the same logic as in Case 2, it suffices to show that each column of N is in B. In fact,

$$N_S = \begin{cases} C_S & \text{if } 2 \notin S \\ C_{S\setminus\{2\}} & \text{if } 2 \in S \neq \{2\} \\ C_{\{2\}} & \text{if } S = \{2\}, \end{cases}$$

which is in $G \subseteq B$ in every case. This completes Case 3 and hence proves Claim 2.9.

Now let C° be the $(k \times \Gamma)$ matrix whose Sth column is C°_S $(S \in \Gamma)$. If $C^\circ(i)$ denotes the ith row of C°, then clearly $C^\circ(2) = R_\Gamma(2)^{a/y}$ while $C^\circ(i) = R_\Gamma(i)$ for $i \neq 2$. Thus $C_\varnothing = t^{\mathbf{F}^k}(\langle C^\circ_S \rangle_{S\in\Gamma}) \in B$ by Claim 2.9, proving that $\mathcal{V}$ has a Γ_2-special cube term. •

Lemma 2.10. *If $\mathcal{V}$ has a $\Delta^\star$-special cube term, then $\mathcal{V}$ has a k-edge term.*

Proof. Let t be a $\Delta^\star$-special cube term for $\mathcal{V}$. We argue as in the first two paragraphs of the proof of Lemma 2.8, using $\Gamma = \Delta^\star$. Thus we have for each $i \in [k]$:

(1) $t^{\mathbf{F}}(R_{\Delta^\star}(i)) = x$.
(2) $t^{\mathbf{F}}(R_{\Delta^\star}(i)^{b/y}) = x$ for any $b \in F$.

Let $G = \{C_S : S \in \Delta^e\}$ and $B = \mathrm{Sg}^{\mathbf{F}^k}(G)$. We will be done if we can prove $C_\varnothing \in B$. First, define $\overline{\varepsilon} = \langle \varepsilon_S \rangle_{S\in\Gamma}$ by

$$\varepsilon_S = \begin{cases} y & \text{if } S = \{1\} \\ x & \text{otherwise} \end{cases}$$

and define $b = t^{\mathbf{F}}(\overline{\varepsilon})$. Next, for $T \subseteq [k]$ define $C^\diamond_T \in F^k$ by

$$C^\diamond_T(i) = \begin{cases} b & \text{if } i = 1 \in T \\ C_T(i) & \text{otherwise.} \end{cases}$$

Claim 2.11. *If $T \in \Delta^\star$, then $C^\diamond_T \in B$.*

The claim is proved via cases.

Case 1. $1 \notin T$. Then $T \in \Delta^e$ and hence $C^\diamond_T = C_T \in G \subseteq B$.

Case 2. $T = \{1, i\}$, $i \geq 3$. In this case we let M denote the $(k \times \Delta^\star)$ matrix whose rows $M(1), \dots, M(k)$ are given as follows:

$$\begin{aligned} M(1) &= \overline{\varepsilon} \\ M(2) &= R_{\Delta^\star}(1) \\ M(i) &= R_{\Delta^\star}(1)^{\mathrm{dual}} \\ M(j) &= \widehat{x}, \text{ for } j \in [k] \setminus \{1, 2, i\}. \end{aligned}$$

Observe that $t^{\mathbf{F}}(M(1)) = b$ while $t^{\mathbf{F}}(M(j)) = C_T(j)$ for $j \geq 2$. Thus if M_S denotes the Sth column of M, then we have shown $t^{\mathbf{F}^k}(\langle M_S \rangle_{S \in \Delta^\star}) = C_T^\diamond$. Hence we will have proved the claim in Case 2 if we can show that each column of M is in B. One can check that for $S \in \Delta^\star$,

$$M_S = \begin{cases} C_{\{i\}} & \text{if } 1 \notin S \\ C_{\{2\}} & \text{if } 1 \in S \neq \{1\} \\ C_{\{1,2\}} & \text{if } S = \{1\}. \end{cases}$$

As each of $\{i\}, \{2\}, \{1,2\} \in \Delta^e$, it follows that $M_S \in G \subseteq B$ for all $S \in \Delta^\star$, completing Case 2.

Case 3. $T = \{1,2\}$. Let N be the $(k \times \Gamma)$ matrix whose rows $N(1), \ldots, N(k)$ are given by $N(1) = \overline{\varepsilon}$, $N(2) = \widehat{y}$, and $N(i) = \widehat{x}$ for $i \geq 3$. Clearly $t^{\mathbf{F}^k}(\langle N_S \rangle_{S \in \Delta^\star}) = C_T^\diamond$, and each column of N is either $C_{\{2\}}$ or $C_{\{1,2\}}$, both of which are in $G \subseteq B$ as required.

Case 4. $T = \{1\}$. Let P be the $(k \times \Gamma)$ matrix whose rows $P(1), \ldots, P(k)$ are given by $P(1) = \overline{\varepsilon}$, and $P(i) = R_{\Delta^\star}(i)$ for $i \neq 1$. Then for $S \in \Delta^\star$,

$$P_S = \begin{cases} C_S & \text{if } |S| = 1 \\ C_{S \setminus \{1\}} & \text{otherwise,} \end{cases}$$

which is in $G \subseteq B$ in either case. This completes Case 4 and hence proves Claim 2.11.

Now let $C^\diamond$ be the $(k \times \Delta^\star)$ matrix whose Sth column is $C_S^\diamond$ $(S \in \Delta^\star)$. If $C^\diamond(i)$ denotes the ith row of $C^\diamond$, then clearly $C^\diamond(1) = R_{\Delta^\star}(1)^{b/y}$ while $C^\diamond(i) = R_{\Delta^\star}(i)$ for $i > 1$. Thus $C_\varnothing = t^{\mathbf{F}^k}(\langle C_S^\diamond \rangle_{S \in \Delta^\star}) \in B$ by Claim 2.11, proving that $\mathcal{V}$ has a k-edge term. •

Theorem 2.12. *For $k \geq 2$ and a variety $\mathcal{V}$, the following are equivalent*:

(1) *$\mathcal{V}$ has a Δ-special cube term for some $\varnothing \neq \Delta \subseteq \Omega_k$;*
(2) *$\mathcal{V}$ has a k-cube term;*
(3) *$\mathcal{V}$ has a k-edge term.*

Proof. (3) $\Rightarrow$ (1) is trivially true, and (1) $\Rightarrow$ (2) follows from comments preceding Lemma 2.8, so assume that $\mathcal{V}$ has a k-cube term t. Then consecutive applications of Lemma 2.8 with $\ell = 2, 3, \ldots, k$ give the existence of a $\Delta^\star$-special cube term. Lemma 2.10 then gives a k-edge term, proving (2) $\Rightarrow$ (3). •

Using the equivalence of (2) and (3) in Theorem 2.12, Kearnes and Szendrei [21] have recently shown that every variety having a k-edge term also has what they call an (m,n)-*parallelogram term* for all $m, n \geq 1$ with $m + n = k$. An (m,n)-parallelogram term is a $(k+3)$-ary term $P_{m,n}$ that satisfies the k equations

corresponding to each row of the following equality:

$$P_{m,n}\left(\begin{array}{ccc|ccccccccc} y & y & x & y & x & \cdots & x & x & \cdots & x & x \\ y & y & x & x & y & & x & x & & x & x \\ & \vdots & & \vdots & & \ddots & & & & & \vdots \\ y & y & x & x & x & & y & x & & x & x \\ \hline x & y & y & x & x & & x & y & & x & x \\ & \vdots & & \vdots & & & & & \ddots & & \vdots \\ x & y & y & x & x & & x & x & & y & x \\ x & y & y & x & x & & x & x & & x & y \end{array}\right) = \left(\begin{array}{c} x \\ x \\ \vdots \\ x \\ x \\ \vdots \\ x \\ x \end{array}\right),$$

where the rightmost block of variables is a $k \times k$ array and the upper and lower leftmost blocks are $m \times 3$ and $n \times 3$ arrays, respectively. Observe that P is a Δ-special cube term P where

$$\Delta = \{[m], \{m+1, \ldots, k\}, [k], \{1\}, \{2\}, \ldots, \{k\}\}.$$

Kearnes and Szendrei use these terms in their study of critical relations in relational clones. The reader is referred to [21] for further details.

In case $\mathcal{V}$ is finitely generated, we can deduce one further consequence from the existence of a cube term. We will use this result in the next section.

Lemma 2.13. *Let* $\mathbf{A}$ *be a finite algebra with a* k*-edge term* t*. Then* $\mathbf{A}$ *also has terms* $d(x,y)$*,* $p(x,y,z)$ *and* $s(x_1, x_2, \ldots, x_k)$ *satisfying*

$$\begin{aligned} p(x,y,y) &\approx x \\ s(y,x,x,x,\ldots,x,x) &\approx p(x,x,y) \\ s(x,y,x,x,\ldots,x,x) &\approx x \\ s(x,x,y,x,\ldots,x,x) &\approx x \\ &\vdots \\ s(x,x,x,x,\ldots,x,y) &\approx x \\ d(x,y) &\approx p(x,x,y) \\ d(x,d(x,y)) &\approx d(x,y). \end{aligned}$$

Note the similarity between the above identities (ignoring those involving d) and those that Gumm terms satisfy. Just as Gumm terms can be thought of as "gluing a Maltsev term to Jónsson terms," so the above identities can be thought of as "gluing a Maltsev term to a near-unanimity term."

Proof. Define

$$\begin{aligned} r(x,y,z_3,\ldots,z_k) &= t(y,x,y,z_3,\ldots,z_k) \\ e(x,y) &= r(x,y,y,y,\ldots,y). \end{aligned}$$

For each $n \geq 0$ we define the nth *iterate* of r in its first variable in the usual way:

$$\begin{aligned} r^0_{(1)}(x,y;\overline{z}) &= x \\ r^{n+1}_{(1)}(x,y;\overline{z}) &= r(r^n_{(1)}(x,y;\overline{z}),y;\overline{z}). \end{aligned}$$

The iterates $e^n_{(1)}(x,y)$ of e are defined similarly. One can show inductively that for all $n \geq 0$,

$$\begin{aligned}
\mathbf{A} &\models r^n_{(1)}(x,y,y,y,\dots,y,y) &&\approx e^n_{(1)}(x,y)\\
\mathbf{A} &\models r^n_{(1)}(y,x,y,y,\dots,y,y) &&\approx y\\
\mathbf{A} &\models r^n_{(1)}(y,y,x,y,\dots,y,y) &&\approx y\\
&\qquad\qquad\qquad\qquad\qquad\vdots\\
\mathbf{A} &\models r^n_{(1)}(y,y,y,y,\dots,y,x) &&\approx y.
\end{aligned}$$

Because $\mathbf{A}$ is finite, we can use [17, Lemma 4.4] to get an integer $N > 1$ such that

$$r^N_{(1)}(x,y,\overline{z}) = r^{2N}_{(1)}(x,y,\overline{z}) = r^N_{(1)}(r^N_{(1)}(x,y,\overline{z}),y,\overline{z})$$

for all $x, y, z_i \in A$.

Define

$$\begin{aligned}
s(x_1,x_2,\dots,x_k) &= r^N_{(1)}(x_1,x_2,x_3,\dots,x_k)\\
d(x,y) &= e^N_{(1)}(y,x)\\
p(x,y,z) &= t(y,e^{N-1}_{(1)}(z,y),x,x,x,\dots x).
\end{aligned}$$

The identities required for s then follow from the identities for $r^n_{(1)}$ displayed above. We check the remaining identities:

$$\begin{aligned}
p(x,y,y) &\approx t(y,e^{N-1}_{(1)}(y,y),x,x,x,\dots,x) \approx t(y,y,x,x,x,\dots,x) \approx x\\
p(x,x,y) &\approx t(x,e^{N-1}_{(1)}(y,x),x,x,x,\dots,x) \approx e(e^{N-1}_{(1)}(y,x),x) \approx d(x,y)\\
d(x,d(x,y)) &\approx e^N_{(1)}(e^N_{(1)}(y,x),x) \approx e^N_{(1)}(y,x) \approx d(x,y).
\end{aligned}$$

This completes the proof of Lemma 2.13 •

3. Compact representations of subpowers

In this section we prove that a finite algebra has few subpowers if and only if it has a k-edge term for some $k \geq 2$. Much of the work has already been done; what remains to be shown is that $\mathbf{A}$ has few subpowers under the assumption that it has a k-edge term. Our main tools are the notion of a *compact representation* of an arbitrary subpower of $\mathbf{A}$ and the related notion of *quasi-representation* of an arbitrary subset of A^n. Our presentation closely follows the paper [4] of Bulatov and Dalmau, which proved the existence of compact representations in the Maltsev case (equivalently, the case of a 2-edge term), and is indebted to Dalmau's paper [9] which did the same for algebras having a so-called "generalized majority-minority operation" (see the definition preceding Theorem 4.7). The following generalizes a key definition from [9].

Definition 3.1. Suppose $\mathbf{A}$ is a finite algebra with k-edge term t and terms d, p, s as in Lemma 2.13. A pair $(a,b) \in A^2$ is a *minority* pair if $d(a,b) = b$.

Note that if $\mathbf{A}$ is a finite algebra with a k-edge term, then (a,c) is a minority pair whenever $a, b \in A$ and $c = d(a,b)$.

By an *index* (*of rank* n) we mean a triple (i,a,b) where $1 \leq i \leq n$ and $a, b \in A$. It is said to be a *minority* index if (a,b) is a minority pair. If $R, S \subseteq A^n$, we say that (i,a,b) is *witnessed* in $R \times S$ if there exist $f \in R$ and $g \in S$ satisfying

- $f(j) = g(j)$ for all $j < i$.
- $f(i) = a$ and $g(i) = b$.

In this case we call f, g *witnesses* to (i, a, b). We say that (i, a, b) is *witnessed* in R if (i, a, b) is witnessed in $R \times R$.

Definition 3.2. Let $\mathbf{A}$ be a finite algebra with k-edge term t and terms d, p, s as in Lemma 2.13, and suppose $R, S \subseteq A^n$.

(1) The *signature* of R is the set Sig_R of all minority indices (i, a, b) witnessed in R.
(2) We say that R is a *representation* of S if
   - $R \subseteq S$,
   - for all $T \subseteq \{1, 2, \ldots, n\}$ with $|T| < k$, $\pi_T(R) = \pi_T(S)$, and
   - $\mathrm{Sig}_R = \mathrm{Sig}_S$.
(3) R is *compact* if $|R| \leq 2|\mathrm{Sig}_R| + \sum_{|T|=m} |\pi_T(R)|$ where $m = \min(k-1, n)$, and is *weakly compact* if $n < k$ or $|R| \leq 2n|A|^2 + \binom{n}{k-1}|A|^{k-1}$.

So, if $\mathbf{A}$ is a finite algebra with a k-edge term, then each of its subpowers has a representation and, clearly, (i) every subset of A^n has a compact representation, (ii) compact subsets of A^n are weakly compact, and (iii) weakly compact subsets of A^n are bounded in size by a polynomial in n of degree $k-1$. We will show that if $\mathbf{B} \leq \mathbf{A}^n$ and R is a representation of B, then $\mathrm{Sg}_{\mathbf{A}^n}(R) = B$, thus proving that $\mathrm{g}_{\mathbf{A}} \in O(n^{k-1})$ (and hence $\mathrm{s}_{\mathbf{A}}, \mathrm{i}_{\mathbf{A}} \in O(n^k)$). We will also define the more complicated notion of a *quasi-representation*, prove that every subset $S \subseteq A^n$ has a weakly compact quasi-representation, and prove that if R is a quasi-representation of $S \subseteq A^n$, then $\mathrm{Sg}_{\mathbf{A}^n}(R) = \mathrm{Sg}_{\mathbf{A}^n}(S)$. This will prove the sharper result that $\mathrm{i}_{\mathbf{A}} \in O(n^{k-1})$.

Definition 3.3. Let $\mathbf{A}$ be a finite algebra with k-edge term t and terms d, p, s as in Lemma 2.13, and suppose $R, S \subseteq A^n$. We say that R is a *quasi-representation* of S if $R \subseteq S$ and there exist subsets $R_1 \subseteq R_2 \subseteq \cdots \subseteq R_n = R$ such that:

- For all $T \subseteq \{1, 2, \ldots, n\}$ with $|T| < k$, $\pi_T(R_1) = \pi_T(S)$;
- For $2 \leq i \leq n$, if the index (i, a, b) is witnessed in $S \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})$, then (i, a, c) is witnessed in $\mathrm{Sg}_{\mathbf{A}^n}(R_i)$, where $c := d(a, b)$.

Lemma 3.4. *Let $\mathbf{A}$ be a finite algebra with k-edge term.*

(1) *Every $S \subseteq A^n$ has a weakly compact quasi-representation.*
(2) *If $\mathbf{B} \leq \mathbf{A}^n$, then every representation of B is a quasi-representation of B.*

Proof. (1) Assume $S \subseteq A^n$. If $n < k$ then S is a weakly compact quasi-representation of itself and we are done. If $n \geq k$, choose $R_1 \subseteq S$ with $|R_1|$ minimal so that $\pi_T(R_1) = \pi_T(S)$ for all $T \subseteq \{1, 2, \ldots, n\}$ with $|T| < k$. Then $|R_1| \leq \binom{n}{k-1}|A|^{k-1}$. For $2 \leq i \leq n$, if $R_{i-1} \subseteq S$ has been defined, let

$$\begin{aligned} \mathcal{S}_i \quad = \quad & \{(a, c) \in A^2 \,:\, (i, a, c) \text{ is not witnessed in } R_{i-1} \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1}), \text{ but } \exists b \in A \\ & \text{such that } c = d(a, b) \text{ and } (i, a, b) \text{ is witnessed in } S \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})\}. \end{aligned}$$

For each $(a, c) \in \mathcal{S}_i$, choose $(f_{a,c}, g_{a,c}) \in S \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})$ witnessing (i, a, b) for some $b \in A$ satisfying $c = d(a, b)$. Now define

$$R_i = R_{i-1} \cup \{f_{a,c} \,:\, (a, c) \in \mathcal{S}_i\}.$$

Finally let $R = R_n$. Clearly $|R| \leq (n-1)|A|^2 + |R_1|$ so R is weakly compact. We turn to showing that R is a quasi-representation of S via the sets $R_1, R_2, \ldots, R_n$.

Clearly R_1 satisfies the first condition of the definition. Suppose (i, a, b) is an index witnessed in $S \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})$ for some $2 \leq i \leq n$, and let $c = d(a, b)$. If (i, a, c) is witnessed in $R_{i-1} \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})$, then it is certainly witnessed in $\mathrm{Sg}_{\mathbf{A}^n}(R_i)$ as well, since $R_{i-1} \subseteq R_i$. On the other hand, if (i, a, c) is not witnessed in $R_{i-1} \times \mathrm{Sg}_{\mathbf{A}^n}(R_{i-1})$, then $(a, c) \in \mathcal{S}_i$. It follows that (i, a, c) is witnessed in $\mathrm{Sg}_{\mathbf{A}^n}(R_i)$ by $f_{a,c}, h$ where $h := d(f_{a,c}, g_{a,c})$, as required.

(2) Assume $\mathbf{B} \leq \mathbf{A}^n$ and R is a representation of B. Define $R^* = \mathrm{Sg}_{\mathbf{A}^n}(R) \subseteq B$ and $R_1 = R_2 = \cdots = R_n = R$ and check the definition of quasi-representation. What must be shown is that if $2 \leq i \leq n$ and (i, a, b) is witnessed in $B \times R^*$, then (i, a, c) is witnessed in R^* where $c = d(a, b)$. Choose $(f, g) \in B \times R^*$ witnessing (i, a, b), and let $h = d(f, g)$. Note that (a, c) is a minority pair and f, h witness (i, a, c) in B, so $(i, a, c) \in \mathrm{Sig}_B$. Since R is a representation of B we have $\mathrm{Sig}_R = \mathrm{Sig}_B$, so (i, a, c) is witnessed in $R \subseteq R^*$ as required. •

Lemma 3.5. *Let $\mathbf{A}$ be a finite algebra with k-edge term t and terms d, p, s as in Lemma 2.13. Suppose $\mathbf{B} \leq \mathbf{A}^n$ and (i, a, c) is a minority index witnessed in B. Then for all $f \in B$ with $f(i) = a$, there exists $g \in B$ such that f, g witness (i, a, c).*

Proof. Choose $f^*, g^* \in B$ witnessing (i, a, c). Define $g = p(f, f^*, g^*) \in B$. Because $\mathbf{A} \models p(x, y, y) \approx x$ we have $f(j) = g(j)$ for all $j < i$. And at coordinate i,

$$g(i) = p(a, a, c) \;=\; d(a, c) \;=\; c$$

where the last equality holds because (a, c) is minority. •

Theorem 3.6. *Suppose $\mathbf{A}$ is a finite algebra with k-edge term t and terms d, p, s as in Lemma 2.13. If R is a quasi-representation of $S \subseteq A^n$, then $\mathrm{Sg}_{\mathbf{A}^n}(R) = \mathrm{Sg}_{\mathbf{A}^n}(S)$.*

Proof. We may assume $n \geq k$, since otherwise $R = S$. Let $R^* = \mathrm{Sg}_{\mathbf{A}^n}(R)$ and let $h = (a_1, a_2, \ldots, a_n) \in S$ be fixed for the remainder of the proof. We wish to show that $h \in R^*$. Choose sets $R_1, \ldots, R_n = R$ satisfying the definition of quasi-representation. The proof will be completed by showing the following claim.

Claim 3.7. *For all $1 \leq m \leq n$ there exists $f_m \in \mathrm{Sg}_{\mathbf{A}^n}(R_m)$ with $f_m(j) = a_j$ for all $1 \leq j \leq m$.*

We prove the claim by induction on m. When $m \leq k-1$, the claim is true because $R_1 \subseteq R_{k-1}$ and $\pi_T(R_1) = \pi_T(S)$ where $T = \{1, 2, \ldots, m\}$. So assume that $m \geq k$ and we have already established the existence of $f_{m-1} \in \mathrm{Sg}_{\mathbf{A}^n}(R_{m-1})$ satisfying the stated condition. Let $a = a_m$, $b = f_{m-1}(m)$, and $c = d(a, b)$. Then h, f_{m-1} witness (m, a, b) in $S \times \mathrm{Sg}_{\mathbf{A}^n}(R_{m-1})$, so by the definition of quasi-representation, (m, a, c) is witnessed in $\mathrm{Sg}_{\mathbf{A}^n}(R_m)$. For the remainder of the proof of this claim, let $R_m^* = \mathrm{Sg}_{\mathbf{A}^n}(R_m)$.

The existence of $f_m \in R_m^*$ will follow from the next subclaim.

Claim 3.8. *For all $T \subseteq \{1, 2, \ldots, m-1\}$ there exists $f_m^T \in R_m^*$ such that $f_m^T(j) = a_j$ for all $j \in T$ and $f_m^T(m) = a$.*

We prove the subclaim by induction on $|T|$, starting with $|T| \leq k - 2$, where the subclaim is true because R_1 represents all projections of $h \in S$ onto $k - 1$ coordinates. Inductively, assume that $|T| \geq k - 1$ and the subclaim has been established for all T' with $|T'| < |T|$. List the elements of T as $i_1 < i_2 < \cdots < i_{|T|}$. For $1 \leq j \leq k - 1$ let $U_j = T \setminus \{i_j\}$ and note that inductively we have $f_m^{U_j} \in R_m^*$.

Define

$$g' \;=\; s(f_{m-1}, f_m^{U_1}, f_m^{U_2}, \ldots, f_m^{U_{k-1}}) \;\in\; R_m^*.$$

The identities for s imply that $g'(j) = a_j$ for $j \in T$, and that

$$g'(m) = s(b, a, a, \ldots, a) = d(a, b) = c.$$

If $a = c$ then we may set $f_m^T = g'$. If not, then since (i) (a, c) is a minority pair, (ii) (m, a, c) is witnessed in R_m^*, (iii) $f_m^{U_1} \in R_m^*$, and (iv) $f_m^{U_1}(m) = a$, we may use Lemma 3.5 to obtain $g \in R_m^*$ such that $f_m^{U_1}, g$ witness (m, a, c). Finally, put

$$f_m^T \;=\; t(g, g', f_m^{U_1}, f_m^{U_2}, \ldots, f_m^{U_{k-1}}) \;\in\; R_m^*.$$

The k-edge identities for t imply that f_m^T has the required properties. •

The following Corollary supplies a proof promised in [18, Theorem 3.9]. Dalmau [9] previously proved a version of it for finite algebras having a *generalized majority-minority operation* (see the definition preceding Theorem 4.7); these include all finite algebras having either a near-unanimity term or a Maltsev term.

Corollary 3.9. *Let* $\mathbf{A}$ *be a finite algebra with a* k*-edge term. If* $\mathbf{B} \leq \mathbf{A}^n$ *and* R *is a representation of* B*, then* $\mathrm{Sg}_{\mathbf{A}^n}(R) = B$*.*

Proof. By Lemma 3.4(2) and Theorem 3.6. •

We can now state our results characterizing finite algebras with few subpowers.

Theorem 3.10. *Let* $\mathbf{A}$ *be a finite algebra and* $k \geq 2$*. The following are equivalent*:

(1) $\mathbf{A}$ *has a* k*-cube term.*
(2) $\mathbf{A}$ *has a* k*-edge term.*
(3) $\mathrm{i}_{\mathbf{A}}(n) \in O(n^{k-1})$.
(4) $n^k \notin O(\mathrm{i}_{\mathbf{A}}(n))$.

Proof. (1) $\Leftrightarrow$ (2) holds by Theorem 2.12, while (2) $\Rightarrow$ (3) follows from Lemma 3.4(1) and Theorem 3.6 and the observation that weakly compact subsets of A^n are of size $O(n^{k-1})$. (3) $\Rightarrow$ (4) is clear. Finally, assume (4); then $n^k \notin L(\mathrm{i}_{\mathbf{A}}(n))$ by Proposition 1.2(0) and comment (iii) preceding it. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}(\mathbf{A})}(2)$ be the free algebra in $\mathcal{V}(\mathbf{A})$ on two generators. Then $L(\mathrm{i}_{\mathbf{F}}(n)) \subseteq L(\mathrm{i}_{\mathbf{A}}(n))$ by Proposition 1.2(4) and comment (iv) that precedes it, so $n^k \notin L(\mathrm{i}_{\mathbf{F}}(n))$ as well. Thus for every $\ell \in \mathbb{N}^+$ there exist arbitrarily large $n \in \mathbb{N}^+$ such that $\mathrm{i}_{\mathbf{F}}(\ell n) < n^k$. In particular, there exists $n \in \mathbb{N}^+$ with $\mathrm{i}_{\mathbf{F}}(kn) < n^k$. Since $n^k \leq \binom{kn}{k}$, we get that $\mathcal{V}(\mathbf{A})$ has a k-cube term by Proposition 2.6, proving (4) $\Rightarrow$ (1). •

Corollary 3.11. *A finite algebra* $\mathbf{A}$ *has few subpowers iff it has a* k*-edge term for some* $k \geq 2$*.*

Proof. If $\mathbf{A}$ has a k-edge term, then Theorem 3.10 yields $\mathrm{i}_{\mathbf{A}}(n) \in O(n^{k-1})$ and hence $\mathrm{s}_{\mathbf{A}}(n) \in O(n^k)$ by Proposition 1.2(2), proving that $\mathbf{A}$ has few subpowers. Conversely, if $\mathrm{s}_{\mathbf{A}}(n) \in O(n^k)$, then Proposition 1.2(1) yields $\mathrm{i}_{\mathbf{A}}(n) \in O(n^k)$ and so $\mathbf{A}$ has a $(k+1)$-edge term by Theorem 3.10. •

Note that the only direct use of the k-edge term t in the proof of Corollary 3.11 occurs in the penultimate sentence of the proof of Theorem 3.6. Therefore, one can ask whether or not the presence of terms p and s that satisfy the conditions of Lemma 2.13 would be enough to establish that $\mathbf{A}$ has few subpowers. Unfortunately, the 2 element implication algebra has such terms but fails to have few subpowers

by Theorem 4.4. In fact any finite algebra in CD(3)[1] has ternary terms s and p that satisfy the conditions of Lemma 2.13.

We can sharpen Theorem 3.10 to obtain the following "stratification result" concerning the asymptotic growth of $\mathrm{i}_{\mathbf{A}}(n)$.

Theorem 3.12. *Let* $\mathbf{A}$ *be a finite algebra with more than one element. Then either* (1) *or* (2) *below holds for* $\mathbf{A}$:

(1) $\mathrm{i}_{\mathbf{A}}(n) =_L n^k$ *for a (unique) positive integer* k*, in which case*
- $\mathrm{i}_{\mathbf{A}}(n) =_\Theta n^k$,
- $\mathrm{g}_{\mathbf{A}}(n) \in \Omega(n^{k-1}) \cap O(n^k)$,
- $\mathrm{s}_{\mathbf{A}}(n) \in \Omega(n^k) \cap O(n^{k+1})$,
- $\mathbf{A}$ *has an* ℓ*-edge term for all* $\ell > k$ *but for no* $\ell \leq k$*, and*
- $\mathbf{A}$ *has few subpowers.*

(2) $\mathrm{i}_{\mathbf{A}}(n) =_L 2^n$*, in which case*
- $\mathrm{s}_{\mathbf{A}}(n) =_L \mathrm{g}_{\mathbf{A}}(n) =_L 2^n$,
- $\mathbf{A}$ *has no* k*-edge term for any* $k \geq 2$*, and*
- $\mathbf{A}$ *has many subpowers.*

Proof. Suppose that $\mathbf{A}$ has few subpowers. Then $\mathbf{A}$ has a k-edge term and $n^k \notin O(\mathrm{i}_{\mathbf{A}}(n))$ for some $k \geq 2$, by Corollary 3.11 and Theorem 3.10. Let k be the least positive integer such that $n^k \notin O(\mathrm{i}_{\mathbf{A}}(n))$. Then $k \geq 2$ by Proposition 1.2(2). By Theorem 3.10, $\mathbf{A}$ has an ℓ-edge term for all $\ell \geq k$, and $\mathrm{i}_{\mathbf{A}}(n) \in O(n^{k-1})$. By the choice of k, we also have $n^{k-1} \in O(\mathrm{i}_{\mathbf{A}}(n))$, so $\mathrm{i}_{\mathbf{A}}(n) =_\Theta n^{k-1}$. The remaining items in (1) follow from Proposition 1.2 and comments preceding it.

Suppose that it is not the case that $\mathbf{A}$ has few subpowers. Then $\mathbf{A}$ has no k-edge term for any k, by Corollary 3.11. Let $\mathbf{F}$ be the free algebra in $\mathcal{V}(\mathbf{A})$ on two generators. As any k-edge term for $\mathbf{F}$ is also a k-edge term for $\mathbf{A}$, it follows that $\mathbf{F}$ has no k-edge term for any k. Hence by Proposition 2.6(1) and Theorem 3.10, $2^k \leq \mathrm{i}_{\mathbf{F}}(k)$ for all $k \geq 2$, and so by Proposition 1.2,

$$2^n \in L(\mathrm{i}_{\mathbf{F}}(n)) \subseteq L(\mathrm{i}_{\mathbf{A}}(n)) \subseteq L(\mathrm{s}_{\mathbf{A}}(n)).$$

By Proposition 1.2(2) and comment (v) preceding it, we also get $2^n \in L(\mathrm{g}_{\mathbf{A}}(n))$. On the other hand, if $\ell = \lceil \lg |A| \rceil$ then

$$\mathrm{g}_{\mathbf{A}}(n) \leq \mathrm{i}_{\mathbf{A}}(n) \leq \mathrm{s}_{\mathbf{A}}(n) \leq 2^{\ell n} \text{ for all } n \in \mathbb{N}$$

by Proposition 1.2(3), proving $\mathrm{g}_{\mathbf{A}}(n), \mathrm{i}_{\mathbf{A}}(n), \mathrm{s}_{\mathbf{A}}(n) \in L(2^n)$. Finally, since $2^n \in L(\mathrm{s}_{\mathbf{A}}(n))$ and $\mathrm{s}_{\mathbf{A}}(n)$ is a non-decreasing function, comment (v) preceding Proposition 1.2 implies that $\mathbf{A}$ has many subpowers. •

4. Connections with other Maltsev Conditions

In this section we explore the connections between some familiar Maltsev conditions and the Maltsev condition of having few subpowers. Our first result demonstrates that having few subpowers implies congruence modularity. We prove this by establishing that any algebra that has a k-edge term also has Day terms. In Section 5 we provide another proof of congruence modularity using the modular commutator.

[1] An algebra is in CD(3) if it has Jónsson terms p_0, p_1, p_2, p_3 satisfying the identities in Theorem 4.3 with $n = 3$.

Theorem 4.1 ([11])**.** *A variety $\mathcal{V}$ is congruence modular if and only if for some n there are terms $m_0(x,y,z,u)$, ..., $m_n(x,y,z,u)$ such that $\mathcal{V}$ satisfies*

$$\begin{aligned} m_0(x,y,z,u) &\approx x \\ m_n(x,y,z,u) &\approx u \\ m_i(x,y,y,x) &\approx x, \quad \textit{for all } i \leq n \\ m_i(x,x,y,y) &\approx m_{i+1}(x,x,y,y), \quad \textit{for all even } i < n \\ m_i(x,y,y,z) &\approx m_{i+1}(x,y,y,z), \quad \textit{for all odd } i < n. \end{aligned}$$

Terms that satisfy the above equations are called Day terms.

Theorem 4.2. *If a variety $\mathcal{V}$ has a k-edge term for some $k \geq 2$ then it has Day terms and so is congruence modular.*

Proof. Suppose that $t(x_1, \ldots, x_{k+1})$ is a k-edge term for $\mathcal{V}$. Define the terms $m_i(x,y,z,u)$ for $0 \leq i \leq 2k-2$ by:

$$\begin{aligned} m_0(x,y,z,u) &= x \\ m_1(x,y,z,u) &= t(z,u,y,x,x,\ldots,x) \\ m_2(x,y,z,u) &= t(z,u,z,x,x,\ldots,x) \\ m_3(x,y,z,u) &= t(u,u,u,y,x,\ldots,x) \\ m_4(x,y,z,u) &= t(u,u,u,z,x,\ldots,x) \\ &\vdots \\ m_{2k-3}(x,y,z,u) &= t(u,u,u,u,\ldots,u,y) \\ m_{2k-2}(x,y,z,u) &= t(u,u,u,u,\ldots,u,z) \end{aligned}$$

For $2 \leq i \leq k-1$, the terms m_{2i-1} and m_{2i} are obtained by substituting y and z for x_{i+2} in $t(u,u,\ldots,x_{i+2},x,\ldots,x)$, respectively. Using the definition of a k-edge term it is straightforward to verify that the m_i are Day terms for $\mathcal{V}$. •

We note that if $\mathbf{A}$ is finite and has a k-edge term then using the terms provided by Lemma 2.13, Gumm terms [13] for $\mathbf{A}$ can be constructed in a manner similar to that employed in the proof of the previous theorem.

We now investigate an intriguing connection between k-edge terms and congruence distributivity. As noted earlier, a near-unanimity term is a special type of k-edge term and it is well known that any algebra that possesses a near-unanimity term generates a congruence distributive variety. We prove that conversely, any algebra that generates a congruence distributive variety and that has a k-edge term must have a (k-ary) near-unanimity term. A conceptually different proof of this fact can be found in [22].

Theorem 4.3 (Jónsson)**.** *A variety is congruence distributive if and only if for some n it has terms $p_i(x,y,z)$, $0 \leq i \leq n$ that satisfy the equations*

$$\begin{aligned} p_0(x,y,z) &\approx x \\ p_n(x,y,z) &\approx z \\ p_i(x,y,x) &\approx x \textit{ for all } i \\ p_i(x,x,y) &\approx p_{i+1}(x,x,y) \textit{ for all } i \textit{ even} \\ p_i(x,y,y) &\approx p_{i+1}(x,y,y) \textit{ for all } i \textit{ odd} \end{aligned}$$

Terms that satisfy the above equations are called Jónsson terms. It is a straightforward exercise to show that from a k-ary near-unanimity term, one can construct a sequence of $2k-3$ Jónsson terms.

Following the approach introduced in [22], we define a subset S of A^n to be *totally symmetric* if for any $\mathbf{a} \in S$ and any permutation $\pi \in Sym(\{1,\dots,n\})$, we have that $\mathbf{a}_\pi \in S$, where $\mathbf{a}_\pi(i) := \mathbf{a}(\pi^{-1}(i))$. Clearly, if a subalgebra of $\mathbf{A}^n$ has a totally symmetric generating set, then it is totally symmetric.

Theorem 4.4. *A variety $\mathcal{V}$ is congruence distributive and has a k-edge term t iff $\mathcal{V}$ has a k-ary near-unanimity term s ($k \geq 3$).*

Proof. One direction of this theorem has already been noted. For the other, assume that $\mathcal{V}$ is congruence distributive with Jónsson terms $p_i(x,y,z)$, $0 \leq i \leq n$ and has a k-edge term $t(x_1,\dots,x_{k+1})$. Let $\mathbf{F} = \mathbf{F}(x,y)$ be the free algebra in $\mathcal{V}$ freely generated by $\{x,y\}$. For $1 \leq i \leq k$, let $\mathbf{y}_i$ be the element of F^k such that $\mathbf{y}_i(i) = y$ and $\mathbf{y}_i(j) = x$, for $j \neq i$ and let $\mathbf{G}$ be the subalgebra of $\mathbf{F}^k$ generated by $\{\mathbf{y}_i : 1 \leq i \leq k\}$. Since $\mathbf{G}$ has a totally symmetric generating set then as noted above, G is a totally symmetric subset of F^k. We aim to prove that $\mathbf{x} \in G$, where $\mathbf{x}(i) = x$ for all $1 \leq i \leq k$.

We now define the elements a_i, b_i, $c_i \in \mathbf{F}$ for $1 \leq i < n$ to be $a_i = p_i(y,x,x)$, $b_i = p_i(y,y,x)$ and $c_i = p_i(x,x,y)$. It will be convenient to represent k-tuples of these elements, along with x and y as words over this set of elements.

We first prove that for each $1 \leq i < n$, $a_i c_i x^{k-2}$ and $b_i c_i x^{k-2}$ are both in G. To see this, just notice that $a_i c_i x^{k-2} = p_i(\mathbf{y}_1, \mathbf{y}_3, \mathbf{y}_2)$ and that $b_i c_i x^{k-2} = p_i(\mathbf{y}_1, \mathbf{y}_1, \mathbf{y}_2)$. Next notice that $b_1 x^{k-1} = y x^{k-1} = \mathbf{y}_1 \in G$.

Claim 4.5. *For each i, $1 \leq i < n$, $a_i x^{k-1} \in G$ iff $b_i x^{k-1} \in G$.*

We prove one implication only, as the other one is analogous. So, assume that $a_i x^{k-1} \in G$. The symmetry of G implies that for each $j < k-1$, the elements $\mathbf{b}_j = b_i x^j c_i x^{k-2-j}$ are in G. Using the properties of the k-edge term t, we calculate that

$$b_i x^{k-1} = t(a_i c_i x^{k-2}, a_i x^{k-1}, \mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{k-2}),$$

as required. •

Now we proceed to prove by induction on i that for each $0 < i < n$, both $a_i x^{k-1}$ and $b_i x^{k-1}$ are in G. For $i = 1$ we have noted that $b_1 x^{k-1} = \mathbf{y}_1 \in G$, and so by Claim 4.5, we also have that $a_1 x^{k-1} \in G$. Assume that both $a_i x^{k-1}$ and $b_i x^{k-1}$ are in G. By the Jónsson equations, either $a_i = a_{i+1}$ or $b_i = b_{i+1}$ and therefore, at least one of the elements $a_{i+1} x^{k-1}$, $b_{i+1} x^{k-1}$ is in G. But, then by Claim 4.5, this means that both of them are in G.

Since one of the elements a_{n-1}, b_{n-1} must be equal to x (by Jónsson's equations), it follows that $\mathbf{x} \in G$. Now, as $\mathbf{x} \in G$, then there must exist a term p such that $p(\mathbf{y}_1,\dots,\mathbf{y}_k) = \mathbf{x}$. By examining the coordinates of this equation, we conclude that in $\mathbf{F}$,

$$p(y,x,\dots,x) = p(x,y,x,\dots,x) = \cdots = p(x,x,\dots,x,y) = x.$$

Finally, since $\mathbf{F}$ is the $\mathcal{V}$-free algebra, then p is a near-unanimity term for $\mathcal{V}$. •

Corollary 4.6. *Suppose $\mathbf{A}$ is a finite nontrivial algebra and $k \geq 4$. If $\mathbf{A}$ has a k-ary near unanimity term but no $(k-1)$-ary near unanimity term, then $\mathrm{i}_{\mathbf{A}}(n) =_\Theta \mathrm{s}_{\mathbf{A}}(n) =_\Theta n^{k-1}$.*

Proof. By Theorem 4.4, $\mathcal{V}(\mathbf{A})$ is congruence distributive and $\mathbf{A}$ has a k-edge term but not a $(k-1)$-edge term. Thus by Theorem 3.12, $\mathrm{i}_{\mathbf{A}}(n) =_\Theta n^{k-1}$ and $\mathrm{s}_{\mathbf{A}}(n) \in \Omega(n^{k-1})$. Since $\mathrm{s}_{\mathbf{A}}(n) \in O(n^{k-1})$ by Proposition 2.3(2), we get $\mathrm{s}_{\mathbf{A}}(n) =_\Theta n^{k-1}$. •

We note that another consequence of Theorem 4.4 is that in the lattice of interpretability types of varieties [14], the filter consisting of those varieties that possess a near-unanimity term is the proper intersection of two larger filters that both happen to consist of congruence modular varieties. This provides another proof of Corollary 3.18 from [25]. In that paper, Sequeira establishes the corollary by introducing a Maltsev condition that happens to be defined using a certain type of $2k$-ary Δ-special cube term, for Δ equal to the set of all singletons and complements of singletons of $[k]$.

A generalized majority-minority operation (or gmm operation) on a set A is an operation $g(x_1, \ldots, x_k)$ on A such that for all a, $b \in A$, either

$$g(y, x, \ldots, x) = g(x, y, x, \ldots, x) = \cdots = g(x, x, \ldots, x, y) = x \text{ for all } x,\ y \in \{a, b\}$$

or

$$g(y, x, \ldots, x) = g(x, x, \ldots, x, y) = y \text{ for all } x,\ y \in \{a, b\}.$$

A pair (a, b) of A is called a majority pair (with respect to g) if the first condition holds for $\{a, b\}$ and is called a minority pair if the second condition holds (compare with Definition 3.1).

In [3] and [9], Bulatov, Chen, and Dalmau introduced and studied gmm operations in the context of learnability and the constraint satisfaction problem. It follows from their work that finite algebras equipped with a gmm term operation have few subpowers. We provide a proof of this by showing that such algebras have k-edge term operations.

Theorem 4.7. *Let $g(x_1, \ldots, x_k)$ be a gmm term operation of the algebra $\mathbf{A}$. Then $\mathbf{A}$ has a k-edge term operation.*

Proof. Let $d(x, y)$ be the binary term operation $g(x, y, ..., y)$ of $\mathbf{A}$. It follows that a pair (a, b) from A is a majority pair with respect to g if $d(a, b) = b$ and is a minority pair if $d(a, b) = a$. It is elementary to show that the term operation

$$t(x_1, ..., x_{k+1}) = g(x_2, d(x_1, x_3), d(x_1, x_4), ..., d(x_1, x_k), d(x_3, x_{k+1}))$$

is a k-edge term operation of $\mathbf{A}$. •

Theorem 3.12 (with Proposition 1.2) establishes polynomial upper bounds for the functions $\mathrm{s}_{\mathbf{A}}$ and $\mathrm{i}_{\mathbf{A}}$ for finite algebras that have k-edge term operations. We conclude this section by providing lower bounds for these functions under the assumption that the variety generated by a finite algebra fails certain Maltsev conditions.

Theorem 4.8 (Maltsev)**.** *A variety is congruence permutable if and only if it has a term $p(x, y, z)$ that satisfies the equations*

$$p(y, x, x) \approx p(x, x, y) \approx y$$

A term that satisfies the equations from this theorem is called a Maltsev term.

Theorem 4.9. *Let $\mathbf{A}$ be a finite algebra with $|A| > 1$. If $\mathbf{A}$ has a Maltsev term, then $\mathrm{i}_{\mathbf{A}}(n) =_\Theta n$. If $\mathbf{A}$ has no Maltsev term then $n^2 \in O(\mathrm{i}_{\mathbf{A}}(n))$.*

Proof. This follows immediately from Proposition 1.2(2), Theorem 3.10, and the fact that a ternary term $t(x, y, z)$ of an algebra $\mathbf{A}$ is a 2-edge term if and only if the term $t(y, x, z)$ is a Maltsev term of $\mathbf{A}$. •

Theorem 4.10. *Let* $\mathbf{A}$ *be a finite algebra with* $|A| > 1$. *If* $\mathsf{HSP}(\mathbf{A})$ *is arithmetical, i.e., both congruence permutable and congruence distributive, then* $\mathrm{s}_{\mathbf{A}}(n) =_\Theta n \lg(n)$. *Conversely, if* $\mathsf{HSP}(\mathbf{A})$ *is not arithmetical or, more particularly, is not congruence distributive, then* $n^2 \in O(\mathrm{s}_{\mathbf{A}}(n))$.

Proof. Suppose first that $\mathsf{HSP}(\mathbf{A})$ is congruence distributive and congruence permutable. We shall find an appropriate constant E, and prove by induction on n that $\mathrm{s}_{\mathbf{A}}(n) \leq En \lg(n)$.

Let $n \geq 1$ and let T be any subalgebra of $\mathbf{A}^{n+1}$. Write T_n for the projection of T onto the first n-coordinates, write Q_i for the projection of T onto the ith coordinate, $0 \leq i \leq n$, and put $Q = Q_n$. Thus T_n is a subalgebra of $\mathbf{A}^n$ and Q is a subalgebra of $\mathbf{A}$. Since $\mathsf{HSP}(\mathbf{A})$ is congruence permutable then according to Fleischer's Lemma (Theorem 4.74 from [23]), T is an equalizer—there is a congruence θ of T_n and a congruence λ of Q, and an isomorphism $\phi : T_n/\theta \cong Q/\lambda$, so that

$$T = \{\langle a_0, \ldots, a_n\rangle : \langle a_0, \ldots, a_{n-1}\rangle \in T_n\,,\ a_n \in Q\,,\ \phi(\langle a_0, \ldots, a_{n-1}\rangle/\theta) = a_n/\lambda\}\,.$$

Since the congruence lattice of T_n is distributive, there are congruences θ_i on Q_i so that

$$\theta = \{(f, g) \in T_n^2 : (f_i, g_i) \in \theta_i \quad \text{for} \quad 0 \leq i < n\}\,.$$

Since the cardinality of T_n/θ is bounded by $|Q/\lambda|$, i.e., by $|A|$, then there is some $k \leq |A|$ and some $0 \leq i_0 < i_1 < \cdots < i_{k-1} < n$ so that

$$\theta = \{(f, g) \in T_n^2 : (f_{i_j}, g_{i_j}) \in \theta_{j_i} \quad \text{for} \quad 0 \leq j < k\}\,.$$

It follows that the algebra T is completely determined by the following data:

$$T_n; \{i_0, \ldots, i_{k-1}\}; \theta_{i_0}, \ldots, \theta_{i_{k-1}}; Q; \lambda; \phi\,.$$

It also follows that there is a constant C, determined independently of n and k, so that once given T_n and $\{i_0, \ldots, i_{k-1}\}$, the number of possible choices for all of $\theta_{i_0}, \ldots, \theta_{i_{k-1}}, Q, \lambda, \phi$ is no greater than C. If s_n denotes the number of subalgebras of $\mathbf{A}^n$, we then have

$$s_{n+1} \leq s_n \cdot \binom{n}{k} \cdot C\,.$$

We can choose other positive constants D, E so that for $n > 1$,

$$s_{n+1} \leq s_n \cdot n^{Dk} \leq s_n \cdot n^E$$

and so that $\mathrm{s}_{\mathbf{A}}(2) \leq E2\lg(2)$ $(= 2E)$. Now by induction, if $n \geq 2$ and $\mathrm{s}_{\mathbf{A}}(n) \leq En \lg(n)$, then taking logarithms in the displayed inequality yields:

$$\mathrm{s}_{\mathbf{A}}(n+1) \leq \mathrm{s}_{\mathbf{A}}(n) + E \cdot \lg(n) \leq E \cdot n \lg(n) + E \cdot \lg(n) \leq$$
$$E \cdot (n+1) \lg(n) \leq E \cdot (n+1) \lg(n+1)\,.$$

Thus $\mathrm{s}_{\mathbf{A}}(n) \in O(n \lg(n))$ and so $\mathrm{s}_{\mathbf{A}}(n) =_\Theta n \lg(n)$ since by Proposition 1.2 we have that $n \lg(n) \in O(\mathrm{s}_{\mathbf{A}}(n))$.

Now, for the other direction, suppose that $\mathsf{HSP}(\mathbf{A})$ is not arithmetical. In Theorem 4.9 we saw that if $\mathbf{A}$ has no Maltsev term, then $n^2 \in O(\mathrm{i}_{\mathbf{A}}(n)) \subseteq O(\mathrm{s}_{\mathbf{A}}(n))$ and so we can assume that $\mathbf{A}$ has a Maltsev term. Thus $\mathsf{HSP}(\mathbf{A})$ is congruence modular, but not congruence distributive. This implies that type **2** occurs in $\mathsf{HSP}(\mathbf{A})$ (see

[17], pages 126–127) and so there is a finite algebra $\mathbf{B} \in \mathsf{HSP}(\mathbf{A})$ with a minimal congruence β of type **2**.

Choosing a $(0_B, \beta)$-minimal set U and a $(0_B, \beta)$-trace $N \subseteq U$ we have that the induced algebra $V = \mathbf{B}|_N$ is polynomially equivalent to a 1-dimensional vector space over a finite field. It follows that for $n \geq 1$, $V^n \subseteq B^n$ is polynomially equivalent to an n-dimensional vector space over that field. For any vector subspace $W \subseteq V^n$, let $\mathbf{B}(W)$ be the subalgebra of $\mathbf{B}^n$ generated by W together with all the constant functions $\bar{b}$, $b \in B$. Using Lemma 6.14 of [17] it follows that the map $W \mapsto \mathbf{B}(W)$ is a one-to-one mapping of the lattice of vector subspaces of V^n into the lattice of subalgebras of $\mathbf{B}^n$. From the discussion of the subpowers of the 2-element Boolean group in Section 6 it follows that $n^2 \in O(\mathrm{s}_{\mathbf{B}}(n))$ and hence also in $O(\mathrm{s}_{\mathbf{A}}(n))$. •

Remark 4.11. *Observe that in the case where* $\mathbf{A}$ *has a Maltsev term and has no Pixley term, we actually have* $\mathrm{s}_{\mathbf{A}} =_\Theta n^2$*, as follows from the theorem just proved, Theorem 4.9, and Proposition 1.2.*

5. Congruence Functions

In parallel with the subalgebra functions defined in 0.1 and 0.3 we define the following congruence functions.

Definition 5.1. For a finite algebra $\mathbf{A}$ and positive integer n,

- $\mathrm{c}_{\mathbf{A}}(n)$ is defined to be the logarithm, base 2, of the maximum cardinality of a congruence lattice of a subalgebra of $\mathbf{A}^n$.
- $\mathrm{gc}_{\mathbf{A}}(n)$ is defined to be the least integer κ such that for every $\mathbf{S} \subseteq \mathbf{A}^n$, every congruence of $\mathbf{S}$ is generated by a set of at most κ ordered pairs of elements of $\mathbf{S}$.
- $\mathrm{ic}_{\mathbf{A}}(n)$ is defined to be the least integer κ such that for every $\mathbf{S} \subseteq \mathbf{A}^n$, every independent subset of S^2 has at most κ elements (where $X \subseteq S^2$ is independent iff no proper subset of X generates the same congruence of $\mathbf{S}$ as does X).

The following properties of these functions are easy to establish.

Proposition 5.2. *For any finite algebra* $\mathbf{A}$ *with* $|A| > 1$*, and for any* $n \in N$ *we have*:

(1) $\mathrm{c}_{\mathbf{A}}(n) \leq \mathrm{s}_{\mathbf{A}}(2n)$, $\mathrm{gc}_{\mathbf{A}}(n) \leq \mathrm{g}_{\mathbf{A}}(2n)$, $\mathrm{ic}_{\mathbf{A}}(n) \leq \mathrm{i}_{\mathbf{A}}(2n)$.
(2) $\mathrm{gc}_{\mathbf{A}}(n) \leq \mathrm{ic}_{\mathbf{A}}(n) \leq \mathrm{c}_{\mathbf{A}}(n)$.
(3) $n \leq \mathrm{c}_{\mathbf{A}}(n) \leq 2\lg(|A|) \cdot n \cdot \mathrm{gc}_{\mathbf{A}}(n)$.
(4) $\mathrm{ic}_{\mathbf{A}}(n) \leq |A|^n - 1$ *and* $\mathrm{c}_{\mathbf{A}}(n) \in O(n|A|^n)$ *(and the bounds are achieved if* $\mathbf{A}$ *has no operations).*
(5) *If* $\mathbf{B}$ *is any finite algebra in* $\mathsf{HSP}(\mathbf{A})$ *then* $\mathrm{c}_{\mathbf{B}} \in L(\mathrm{c}_{\mathbf{A}})$, $\mathrm{gc}_{\mathbf{B}} \in L(\mathrm{gc}_{\mathbf{A}})$*, and* $\mathrm{ic}_{\mathbf{B}} \in L(\mathrm{ic}_{\mathbf{A}})$.

The main result of this section establishes that the growth rate of the function $\mathrm{c}_{\mathbf{A}}$ reflects the congruence modularity and/or congruence distributivity of $\mathsf{HSP}(\mathbf{A})$.

Theorem 5.3. *Let* $\mathbf{A}$ *be any finite algebra.*

(i) *If* $\mathsf{HSP}(\mathbf{A})$ *is not congruence distributive, then* $n^2 \in L(\mathrm{c}_{\mathbf{A}}(n))$.
(ii) *If* $\mathsf{HSP}(\mathbf{A})$ *is congruence distributive, then* $\mathrm{c}_{\mathbf{A}}(n) \in L(n)$.
(iii) *If* $\mathsf{HSP}(\mathbf{A})$ *is not congruence modular, then* $2^n \in L(\mathrm{c}_{\mathbf{A}}(n))$.
(iv) *If* $\mathsf{HSP}(\mathbf{A})$ *is congruence modular, then* $\mathrm{c}_{\mathbf{A}}(n) \in L(n^2)$.

Proof. We first observe that in the case where $\mathsf{HSP}(\mathbf{A})$ is congruence modular but not congruence distributive, the considerations in the last paragraph of the proof of Theorem 4.10 establish that $n^2 \in O(\mathrm{c}_{\mathbf{A}}(n))$: Let $\mathbf{C}_n = \mathbf{B}(V^n)$. The mapping from subspaces W of V^n to congruences of $\mathbf{C}_n$, $W \mapsto \mathrm{Cg}_{\mathbf{C}_n}(W \times W)$, is in this case a one-to-one mapping from the lattice of subspaces of V^n to the congruence lattice of $\mathbf{C}_n$. Thus $n^2 \in O(\mathrm{c}_{\mathbf{A}}(n))$ (implying that $n^2 \in L(\mathrm{c}_{\mathbf{A}}(n))$).

Now suppose that $\mathsf{HSP}(\mathbf{A})$ is not congruence modular. Then by the Shifting Lemma (see the proof of Theorem 3.5 in [15]) we can choose a finite algebra $\mathbf{B} \in \mathsf{HSP}(\mathbf{A})$, congruences α, β, γ on $\mathbf{B}$ with $\alpha \wedge \beta \leq \gamma$, and elements $a, b, c, d \in B$ so that $(a, b), (c, d) \in \alpha$, $(a, c), (b, d) \in \beta$, $(c, d) \in \gamma$ and $(a, b) \notin \gamma$. (In fact, $\mathbf{B}$ can be taken to be the free algebra on four generators in this variety.)

We are going to show that for $n > 1$, $\mathbf{B}^{2n}$ has a subalgebra $\mathbf{C}$ that has a set of 2^n congruence-independent ordered pairs of elements. Thus $\mathrm{c}_{\mathbf{B}}(2n) \geq \mathrm{ic}_{\mathbf{B}}(2n) \geq 2^n$, showing that $2^n \in L(\mathrm{c}_{\mathbf{B}}(n)) \subseteq L(\mathrm{c}_{\mathbf{A}}(n))$.

To begin, we replace γ by $\alpha \wedge \gamma$, thus assuring that $\alpha \wedge \beta < \gamma < \alpha$. We define $\mathbf{C}$ to be the subalgebra of $\mathbf{B}^{2n}$ consisting of those functions f such that $(f(i), f(j)) \in \beta$ for all $0 \leq i, j < 2n$. Now let M be the collection of all subsets of $\{0, 1, \ldots, n-1\}$. For $X \in M$ we define two elements f_X, g_X in $\mathbf{C}$: f_X is the function that takes the value a at $2i$ and c at $2i+1$ for each $i \in X$, and takes the value a at $2i+1$ and c at $2i$ for $i \in \{0, \ldots, n-1\} \setminus X$. g_X is the function that takes the value b exactly where f_X has value a, and has the value d exactly where f_X has value c.

We put θ_X equal to the congruence of $\mathbf{C}$ generated by (f_X, g_X) and claim that for all $X \in M$,

$$(f_X, g_X) \notin \bigvee \{\theta_Y : Y \in M \setminus \{X\}\}.$$

The claim obviously will finish the proof of (i) and (iii).

To prove, it, suppose, otherwise. Then we have $X_0 \in M$ and a chain

$$f_{X_0} = g_0, \ldots, g_k = g_{X_0}$$

where for each $i < k$, $\{g_i, g_{i+1}\} = \{p_i(f_{Y_i}), p_i(g_{Y_i})\}$ where p_i is a polynomial of $\mathbf{C}$ and $Y_i \in M \setminus \{X_0\}$. Let us write

$$E = \{2i : i \in X_0\} \cup \{2i+1 : 0 \leq i \leq n-1, i \notin X_0\}.$$

We shall get a contradiction by showing that for all $0 \leq u \leq k$ $g_u(j)$ is γ-related to a for all $j \in E$. Since $g_k(j) = b$ for $j \in E$, we will have an obvious contradiction. The proof is by induction on $u \leq k$.

Note that g_0 is constantly equal to a on E. Now suppose that $u < k$ and $g_u|_E$ takes only values γ-related to a We have that

$$\{g_u, g_{u+1}\} = \{p_u(f_{Y_u}), p_u(g_{Y_u})\}.$$

Now f_{Y_u} and g_{Y_u} are α-related at every $j < 2n$, and so this also holds for g_{u+1} and g_u.

If $j \in E$ and $j = 2i$ for some $i \in X_0 \setminus Y_u$ then $g_u(j)$ and $g_{u+1}(j)$ are γ-related since $f_{Y_u}(j)$ and $g_{Y_u}(j)$ are. On the other hand, if $j = 2i+1$ for some $i \in Y_u \setminus X_0$ then we also have that $g_u(j)$ and $g_{u+1}(j)$ are γ-related.

If $j = 2i$ for some $i \in X_0 \cap Y_u$ then, by considering some element in the symmetric difference of X_0 and Y_u, we obtain a $k \in E$ with $k \neq j$ and $g_{u+1}(k)\ \gamma\ a$. Then

$$g_u(j)\ \gamma\ a\ \gamma\ g_u(k)\ \gamma\ g_{u+1}(k) \text{ and } g_u(j)\ \alpha\ g_{u+1}(j)$$

and so $g_{u+1}(k)\ \alpha\ g_{u+1}(j)$. Since these two elements are also β-related it follows that in fact they are γ-related. Thus $g_{u+1}(j)\ \gamma\ a$, as required. The remaining case, $j = 2i+1$ for some $i \notin X_0 \cup Y_u$, can be handled in a similar fashion and so we conclude that $g_{u+1}(j)\ \gamma\ a$ for all $j \in E$.

This completes our inductive proof that $g_u(j)\ \gamma\ a$ for all $u \leq k$ and all $j \in E$. We have now finished with (i) and (iii).

Now we tackle (ii). Suppose that $\mathsf{HSP}(\mathbf{A})$ is congruence distributive. Let $n \geq 1$ and $\mathbf{B}$ be any subalgebra of $\mathbf{A}^n$. Write p_i for the ith projection homomorphism mapping $\mathbf{B} \to \mathbf{A}$. As is well-known, congruence distributivity implies that every congruence of $\mathbf{B}$ is of the form

$$\bigwedge_{0 \leq i < n} p_i^{-1}(\theta_i)$$

for some system of congruences θ_i on $\mathbf{A}$. Thus the number of congruences of $\mathbf{B}$ is no greater than c^n where c is the number of congruences of $\mathbf{A}$. This shows that $\mathrm{c}_{\mathbf{A}}(n) \in O(n) = L(n)$.

Finally, we prove (iv). Assume that $\mathsf{HSP}(\mathbf{A})$ is congruence modular. Let $n \geq 1$ and $\mathbf{B} \subseteq \mathbf{A}^n$. We first argue that the height of $\operatorname{Con}\mathbf{B}$ is at most cn where c is the maximal height of $\operatorname{Con}\mathbf{C}$ where $\mathbf{C}$ ranges over the subalgebras of $\mathbf{A}$. For $0 \leq i < n$, let η_i be the kernel of the projection homomorphism from $\mathbf{B}$ to $\mathbf{A}$ at the ith coordinate. Each interval $(\eta_0 \wedge \cdots \eta_{i-1})/(\eta_0 \wedge \cdots \wedge \eta_{i-1} \wedge \eta_i)$, $0 \leq i < n$ is isomorphic to a subinterval of the interval $1_B/\eta_i$ and hence has height $\leq c$. Thus the height of $\operatorname{Con}\mathbf{B}$ is at most cn.

Next, we find a bound for the number of polynomial equivalence classes of minimal sets for congruence covers in $\mathbf{B}$. Suppose that $\alpha \prec \beta$ are congruences of $\mathbf{B}$ with β covering α. Let β' be minimal among all congruences τ with $\tau \leq \beta$, $\tau \not\leq \alpha$. Put $\alpha' = \alpha \wedge \beta'$ so that $\alpha' \prec \beta'$. Choose a projection kernel η_i with $\eta_i \not\geq \beta'$. Thus $\eta_i \wedge \beta' \leq \alpha$. Now $\eta_i \wedge \beta' \leq \alpha'$ and hence, by modularity,

$$\eta_i \vee \alpha' = \alpha'' \neq \eta_i \vee \beta' = \beta''\,.$$

Thus we have $\alpha'' \prec \beta''$. Let U be any (α'', β'')-minimal set. Then since (α', β') and (α, β) are perspective to (α'', β''), we have that U is a (α, β)-minimal set. Let $\mathcal{W}$ be a family of subsets of B consisting of, for each $0 \leq i < n$ and for each congruence cover $\beta \succ \alpha \geq \eta_i$, one (α, β)-minimal set. Now the size of $\mathcal{W}$ is at most dn where d is the square of the maximal size of $\operatorname{Con}\mathbf{C}$, $\mathbf{C} \subseteq \mathbf{A}$; and as we have seen, for every $\alpha \prec \beta$ in $\operatorname{Con}\mathbf{B}$, there is an (α, β)-minimal set $U \in \mathcal{W}$.

Now we can bound the number of covers of any member of $\operatorname{Con}\mathbf{B}$. Let $\alpha_0 \in \operatorname{Con}\mathbf{B}$. We define a function t mapping the set of covers of α_0 into the set $\mathcal{W}$. Suppose that $\alpha_0 \prec \beta$. Choose $U \in \mathcal{W}$, an (α_0, β)-minimal set, and put $t(\beta) = U$. We claim that for each $U \in \mathcal{W}$, there are at most $|B|$ covers β of α_0 with $t(\beta) = U$. To see this, choose $u_0 \in U$. Given $\beta \succ \alpha_0$ with $t(\beta) = U$, we know that β is generated by α_0 together with any pair in $(\beta \setminus \alpha_0) \cap U^2$. Since the induced algebra on U has regular congruences, then there is $v \in U$ such that β is generated by $\alpha_0 \cup \{(u_0, v)\}$. This shows that the number of such β is at most $|U| \leq |B|$.

Now it follows that the number of covers of α_0 is at most

$$dn|B| \leq dn|A|^n\,.$$

Next, since the height of $\operatorname{Con}\mathbf{B}$ is at most cn, then the cardinality of $\operatorname{Con}\mathbf{B}$ is bounded by

$$1 + q + q^2 + \cdots + q^{cn} \leq \frac{q^{cn+1} - 1}{q - 1} \leq 2q^{cn}\,,\ q = dn|A|^n\,.$$

(In this formula, 1 counts the zero element of the lattice, q bounds the number of atoms, q^2 bounds the number of elements of height 2—covers of atoms—and so on.) This simplifies to

$$|\operatorname{Con}\mathbf{B}| \leq 2(dn)^{cn}|A|^{cn^2} \leq |A|^{2cn^2} = 2^{en^2}\,,\ \text{ for large } n\,,$$

where $e = 2c\lg|A|$. This formula shows that $\mathrm{c}_{\mathbf{A}} \in L(n^2)$, as required. •

From Theorem 4.2 and Corollary 3.11 it follows that if a finite algebra $\mathbf{A}$ has few subpowers then $\mathsf{HSP}(\mathbf{A})$ is congruence modular. This result also follows from Theorem 5.3 since, as noted in Proposition 5.2, $\mathrm{c}_{\mathbf{A}}(n) \leq \mathrm{s}_{\mathbf{A}}(2n)$ for all n.

6. Examples

In this section we present examples of algebras over the set $\{0,1\}$ to illustrate some of the functions that can occur as one of the invariants that we have been studying in this paper. In section 4 of [7], Chen uses Post's classification of the lattice of clones over a two element set to characterize those algebras with domain $\{0,1\}$ that have few subpowers (or, using his terminology, that are polynomially expressive). Our results from this section, summarized in Table 1, provide a refinement and extension of Chen's analysis. The examples that we consider are constructed from the following operations on $\{0,1\}$:

- $x \wedge y$ (the smaller of x and y),
- $x \vee y$ (the larger of x and y),
- $\pi(x) = 1 - x$,
- $x \to y = \pi(x) \vee y$,
- $x \oplus y$ (the sum of x and y, modulo 2).

Boolean algebra. The first algebra we consider is $\mathbf{A} = \langle\{0,1\}, \wedge, \vee, \pi\rangle$, the 2-element Boolean algebra. Let $\mathbf{B}$ be any subalgebra of $\mathbf{A}^n$. Every atom of $\mathbf{B}$ is a join of some of the n atoms of $\mathbf{A}^n$. So $\mathbf{B}$ partitions the atoms of $\mathbf{A}^n$. Conversely, each partition of the n atoms of $\mathbf{A}^n$ corresponds to a subuniverse $\mathbf{B}$ of $\mathbf{A}^n$. So $\mathrm{s}_{\mathbf{A}}(n)$ is $\lg(B(n))$, where $B(n)$ is the n-th Bell number. If $\{c_1, \ldots, c_m\}$ is an independent subset of $\mathbf{A}^n$, then

$$\{\bar{0}, \bar{1}\} \subset \operatorname{Sg}(\{c_1\}) \subset \operatorname{Sg}(\{c_1, c_2\}) \subset \cdots \subset \operatorname{Sg}(\{c_1, c_2, \ldots, c_m\}) \subseteq \mathbf{A}^n.$$

Any chain in the lattice of subuniverses of $\mathbf{A}^n$ has cardinality at most n, so $m < n$. Let the atoms of $\mathbf{A}^n$ be a_i, for $0 \leq i < n$, with $a_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ having a 1 in coordinate i. We claim that the set $M = \{a_0, a_1, \ldots, a_{n-2}\}$ is independent. For example, a_0 is not in $\operatorname{Sg}(\{a_1, \ldots, a_{n-2}\})$ because for each $1 \leq i \leq n-2$ we have $a_i(0) = a_i(n-1)$, and this property is preserved when forming the subalgebra generated by these $n-2$ atoms. Hence $\mathrm{i}_{\mathbf{A}}(n) = n - 1$.

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}^n$ then $\mathbf{B} \cong \mathbf{A}^m$ for some $1 \leq m \leq n$. If $k \geq \lg(m)$, then $\mathbf{B}$ is a surjective homomorphic image of $\mathbf{A}^{2^k}$, the k-generated free algebra in $\mathsf{HSP}(\mathbf{A})$, whence $\mathbf{B}$ is generated by at most k elements. On the other hand, if $k <$

Algebra	$\mathrm{s}_{\mathbf{A}}(n)$	$\mathrm{i}_{\mathbf{A}}(n)$	$\mathrm{g}_{\mathbf{A}}(n)$	$\mathrm{c}_{\mathbf{A}}(n)$	$\mathrm{ic}_{\mathbf{A}}(n)$	$\mathrm{gc}_{\mathbf{A}}(n)$
$\wedge$, $\vee$, π	$\lg(B(n))$	$n-1$	$\lceil \lg n \rceil$	n	n	1
$\oplus$	$=_\Theta n^2$	n	n	$=_\Theta n^2$	n	n
$\wedge$, $\vee$	$=_\Theta n^2$	$=_\Theta n^2$	$n+1$	n	n	$\lceil n/2 \rceil$
$\to$	$\geq \lg(\lvert \mathbf{F}_{\mathcal{D}}(n) \rvert)$	$\geq \binom{n}{\lceil n/2 \rceil}$	$\geq \binom{n}{\lceil n/2 \rceil}$	n	n	$\lceil n/2 \rceil$
$\vee$	$\geq \lg(\lvert \mathbf{F}_{\mathcal{D}}(n) \rvert)$	$\geq \binom{n}{\lceil n/2 \rceil}$	$\geq \binom{n}{\lceil n/2 \rceil}$	$\geq \lg(\lvert \mathbf{F}_{\mathcal{D}}(n) \rvert)$	$\geq \binom{n}{\lceil n/2 \rceil}$	$\geq \frac{1}{2} \cdot \binom{n}{\lceil n/2 \rceil}$
π	2^{n-1}	2^{n-1}	2^{n-1}	$=_\Theta n2^n$	$=_\Theta 2^n$	$=_\Theta 2^n$

TABLE 1. The six invariants for certain 2-element algebras $\mathbf{A}$.

$\lg(m)$, then $\mathbf{B}$ is larger than the free algebra on k generators, and hence cannot be generated by k or fewer elements. These considerations show that $\mathrm{g}_{\mathbf{A}}(n) = \lceil \lg(n) \rceil$.

If $\mathbf{B}$ is a subalgebra of $\mathbf{A}^n$ then the congruence lattice of $\mathbf{B}$ is isomorphic to $\mathbf{B}$: every congruence relation of $\mathbf{B}$ is a principal congruence of the form $\mathrm{Cg}(0, q)$ for $q \in B$. Hence $\mathrm{c}_{\mathbf{A}}(n) = n$ and $\mathrm{gc}_{\mathbf{A}}(n) = 1$. If $X \subseteq B^2$ is an independent subset of B^2, where $\mathbf{A}^m \cong \mathbf{B} \subseteq \mathbf{A}^n$, then distinct subsets of X generate distinct congruence relations on $\mathbf{B}$. So $2^{|X|} \leq |\mathrm{Con}\, \mathbf{B}| = 2^m$ and thus $\mathrm{ic}_{\mathbf{A}}(n) \leq n$. Since the ordered pairs $(0, a_i)$ for the atoms a_i of $\mathbf{A}^n$ form an independent set we conclude that $\mathrm{ic}_{\mathbf{A}}(n) = n$.

Boolean group. Next, we consider the group $\mathbf{A} = \langle \{0, 1\}, \oplus \rangle$. We have that $\mathrm{s}_{\mathbf{A}}(n) = \mathrm{c}_{\mathbf{A}}(n)$ since $\mathbf{A}$ is Abelian. Here the subalgebra of $\mathbf{A}^n$ generated by an element b corresponds to the congruence generated by $(0, b)$. Thus $\mathrm{i}_{\mathbf{A}}(n) = \mathrm{ic}_{\mathbf{A}}(n)$ and $\mathrm{g}_{\mathbf{A}}(n) = \mathrm{gc}_{\mathbf{A}}(n)$. The value of $\mathrm{s}_{\mathbf{A}}(n)$ is the number of subspaces of an n-dimensional vector space over the 2-element field. This is the sum over k of the Gaussian binomial coefficients $\{n, k\}_2$. Since $\{n, k\}_2$ is approximated by $2^{k(n-k)}$ we find that $\mathrm{s}_{\mathbf{A}}(n) =_\Theta n^2$. It is easily checked that $\mathrm{i}_{\mathbf{A}}(n) = \mathrm{g}_{\mathbf{A}}(n) = n$.

Lattice. Next let $\mathbf{A} = \langle \{0, 1\}, \wedge, \vee \rangle$ be the 2-element lattice. Then $\mathbf{A}$ has no Maltsev term but does have a 3-ary near unanimity term. By Theorem 4.9 and Proposition 2.3(2), we have $n^2 \in O(\mathrm{i}_{\mathbf{A}}(n))$ and $\mathrm{s}_{\mathbf{A}}(n) \in O(n^2)$. Thus by Proposition 1.2 (1), we conclude that $\mathrm{i}_{\mathbf{A}}(n) =_\Theta \mathrm{s}_{\mathbf{A}}(n) =_\Theta n^2$. Every sublattice $\mathbf{S}$ of $\mathbf{A}^n$ has height at most n and therefore the poset of join irreducible elements of $\mathbf{S}$ has cardinality at most n. Since the join irreducible elements, together with 0_S, generate $\mathbf{S}$, we have that $\mathrm{g}_{\mathbf{A}}(n) \leq n + 1$. As $\mathbf{A}^n$ has an $(n + 1)$-element chain as a sublattice and since no proper subset of an $(n + 1)$-element chain can generate it, we conclude that $\mathrm{g}_{\mathbf{A}}(n) = n + 1$.

The congruence lattice of $\mathbf{A}^n$ is isomorphic to $\mathbf{A}^n$, hence $\mathrm{c}_{\mathbf{A}}(n) \geq n$. If $\mathbf{S}$ is a sublattice of $\mathbf{A}^n$, then every congruence of $\mathbf{S}$ is equal to the kernel of a projection of $\mathbf{S}$ into $\mathbf{A}^m$ over some $m \leq n$ coordinates (by congruence distributivity); i.e., congruences of $\mathbf{S}$ extend to $\mathbf{A}^n$. Thus $\mathrm{c}_{\mathbf{A}}(n) = n$. These observations also imply that the height of $\mathrm{Con}\, \mathbf{S}$ is at most n, implying that $\mathrm{ic}_{\mathbf{A}}(n) \leq n$. Where $a_0, \ldots, a_{n-1}$ are the atoms of $\mathbf{A}^n$, the pairs $(\bar{0}, a_i)$ form an independent set in $(A^n)^2$ of n elements, hence $\mathrm{ic}_{\mathbf{A}}(n) = n$.

To calculate $\mathrm{gc}_{\mathbf{A}}(n)$, let $\mathbf{S} \subseteq \mathbf{A}^n$ and let $C = \{a_0, \dots, a_m\}$ be any maximal chain in $\mathbf{S}$, with say,

$$a_0 \prec a_1 \prec \cdots \prec a_m \,.$$

Here, $m \leq n$. Let θ be any congruence of $\mathbf{S}$. Then θ is generated by pairs (c, d) where $c \prec d$ (i.e., d covers c). For each such (c, d), there is a unique $i < m$ such that the intervals d/c and a_{i+1}/a_i are perspective in $\mathbf{S}$—in this situation, $\mathrm{Cg}_{\mathbf{S}}(c, d) = \mathrm{Cg}_{\mathbf{S}}(a_i, a_{i+1})$. Thus θ is generated by some subset of the pairs (a_i, a_{i+1}). Now if $a_i \equiv a_{i+1} \equiv a_{i+2} \pmod{\theta}$ then $\mathrm{Cg}_{\mathbf{S}}(a_i, a_{i+1}) \vee \mathrm{Cg}_{\mathbf{S}}(a_{i+1}, a_{i+2}) = \mathrm{Cg}_{\mathbf{S}}(a_i, a_{i+2})$. This leads us to look for the maximal intervals in C consisting of θ-equivalent elements. Assuming that $\theta \neq 0_S$, there are

$$x_0 < y_0 < x_1 < y_1 < \cdots < x_{k-1} < y_{k-1}$$

in C with $(x_i, y_i) \in \theta$ for $0 \leq i \leq k-1$, and $(y_i, x_{i+1}) \notin \theta$ for $0 \leq i < k-1$, and such that any $(c, d) \in C^2$ belongs to θ iff there is some $i < k$ with $x_i \leq c, d \leq y_i$. Our analysis shows that θ is generated by $\{(x_i, y_i) : 0 \leq i < k\}$. Obviously, $2k \leq m + 1 \leq n + 1$ and so we conclude that

$$\mathrm{gc}_{\mathbf{A}}(n) \leq \lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n}{2} \rceil \,.$$

To see that $\mathrm{gc}_{\mathbf{A}}(n) \geq \lceil \frac{n}{2} \rceil$, one can again consider an $(n+1)$-element subalgebra of $\mathbf{A}^n$ that is linearly ordered, and a certain congruence on it that divides all but at most one of the elements into 2-element equivalence classes (intervals).

Implication algebra. Now we consider the algebra $\mathbf{A} = \langle \{0, 1\}, \to \rangle$. Like the lattice, this 2-element algebra generates a congruence distributive variety. Whence the same considerations as above show that $\mathrm{c}_{\mathbf{A}}(n) = \mathrm{ic}_{\mathbf{A}}(n) = n$. This algebra is interesting because, although it does generate a congruence distributive variety, it has no near unanimity term or Maltsev term, and so by Theorem 4.4 fails to have few subpowers. Before turning our attention to $\mathrm{s}_{\mathbf{A}}(n)$ we first show that $\mathrm{gc}_{\mathbf{A}}(n) = \lceil \frac{n}{2} \rceil$. Note that the argument we present is general enough to apply to our previous example, the 2-element lattice.

We remark that $x \vee y = (x \to y) \to y$, and the term operations of $\mathbf{A}$ are exactly those operations $f(x_0, \dots, x_{m-1})$ for which there is some i, $0 \leq i < m$ such that for all $a_0, \dots, a_{m-1} \in \{0, 1\}$, $f(a_0, \dots, a_{m-1}) \geq a_i$. (This fact is easily proved, and implies, for example, that $\mathbf{A}$ has no near unanimity term or Maltsev term.)

Now let $\mathbf{S} \subseteq \mathbf{A}^n$ and let θ be any congruence on $\mathbf{S}$ distinct from the equality relation. If $x, y \in S$ then $x \to x = \bar{1}$, so if $(x, y) \in \theta$ then $(x \to y, \bar{1}), (y \to x, \bar{1}) \in \theta$. Conversely, if $x \to y \equiv \bar{1} \equiv y \to x \pmod{\theta}$ then

$$x = (x \to y) \to x \equiv_\theta (y \to x) \to x = y \vee x \,,$$

$$y = (y \to x) \to y \equiv_\theta (x \to y) \to y = x \vee y = y \vee x \,;$$

and so $x \equiv y \pmod{\theta}$. Thus θ is generated by a set of pairs of the form $(a, \bar{1})$.

Let $\eta_i = \{(f, g) \in S^2 : f(i) = g(i)\}$ for $0 \leq i < n$. For any $C \subseteq S^2$, put $N_C = \{i : C \not\subseteq \eta_i\}$ and $E_C = \{i : C \subseteq \eta_i\}$. It follows from the congruence distributivity of $\mathsf{HSP}(\mathbf{A})$ and the fact that $|\mathbf{A}| = 2$ that $\theta = \bigcap\{\eta_i : i \in E_\theta\}$ and that θ is the smallest congruence ψ such that $N_\theta \subseteq N_\psi$. Furthermore, if $C \subseteq S^2$ then $\mathrm{Cg}_{\mathbf{S}}(C)$ is the smallest congruence ψ with $N_C \subseteq N_\psi$. Consequently $\theta = \mathrm{Cg}_{\mathbf{S}}(C)$ iff $C \subseteq \theta$ and $N_C \supseteq N_\theta$

Let us pick, for each $i \in N_\theta$, $a_i \in S$ so that $(a_i, \bar{1}) \in \theta$ and $a_i(i) = 0$. We claim that if $\{i, j\} \subseteq N_\theta$, there is $(c, d) \in \theta$ such that $\{i, j\} \subseteq N_{\{(c,d)\}}$. This is obvious

if $a_i(j) = 0$ (just take $(c,d) = (a_i, \bar{1})$) or if $a_j(i) = 0$ (take $(c,d) = (a_j, \bar{1})$). So suppose that $a_i(j) = 1$ and $a_j(i) = 1$. In this case, take $(c,d) = (a_i, a_j)$. Clearly, $(a_i, a_j) \in \theta$, and $(a_i(i), a_j(i)) = (0,1) = (a_j(j), a_i(j))$, so that $\{i,j\} \subseteq N_{\{(c,d)\}}$.

Finally, where $\hat{n} = \lceil \frac{n}{2} \rceil$, we can write,

$$N_\theta = \bigcup \{\{i_r, j_r\} : 0 \leq r < \hat{n}\}$$

for some i_r, j_r (where possibly $i_r = j_r$ for some r). For $0 \leq r < \hat{n}$, choose $(c_r, d_r) \in \theta$ with $\{i_r, j_r\} \subseteq N_{\{(c_r,d_r)\}}$. The set $\{(c_r, d_r) : 0 \leq r < \hat{n}\}$ is now guaranteed to generate θ.

We have proved that $\mathrm{gc}_{\mathbf{A}}(n) \leq \lceil \frac{n}{2} \rceil$. To show that this bound is exact, let S be the subset of $\{0,1\}^n$ consisting of all functions that take value 0 at most once. This set of $n+1$ functions constitutes a subalgebra $\mathbf{S}$ of $\mathbf{A}^n$. Let $\theta = S \times S$. Since any pair of elements of S differ on at most two coordinates, it requires $\lceil \frac{n}{2} \rceil$ pairs in S^2 to generate θ.

We now consider the number of subalgebras of $\mathbf{A}^n$. It follows from our characterization of the term operations of $\mathbf{A}$ that every nonvoid order-filter in A^n is a subalgebra of $\mathbf{A}^n$; and that every nonvoid anti-chain in A^n is an independent set and is the unique minimal generating set for the subalgebra it generates. The number of nonvoid order-filters and the number of nonvoid anti-chains are both equal to the cardinality of $\mathbf{F}_{\mathcal{D}}(n)$, the free distributive lattice on n generators. The largest anti-chain in A^n is the set of functions f with $|f^{-1}(\{1\})| = \lceil \frac{n}{2} \rceil$, a set of cardinality $\binom{n}{\lceil \frac{n}{2} \rceil}$. Thus we have

$$\mathrm{s}_{\mathbf{A}}(n) \geq \lg(|\mathbf{F}_{\mathcal{D}}(n)|) \geq \binom{n}{\lceil \frac{n}{2} \rceil} \geq \frac{2^n}{n}, \quad \mathrm{i}_{\mathbf{A}}(n) \geq \binom{n}{\lceil \frac{n}{2} \rceil}, \quad \mathrm{g}_{\mathbf{A}}(n) \geq \binom{n}{\lceil \frac{n}{2} \rceil}.$$

Note that these lower bounds also hold for the next example—the 2-element semilattice. Theorem 3.2 of [7] can be used to establish these lower bounds as well.

Semilattice. Next, we consider the semilattice $\mathbf{A} = \langle \{0,1\}, \vee \rangle$. Since $x \vee y$ is a term operation of the implication algebra, it is clear that all the numbers we seek to calculate or bound will be not less for the semilattice than for the implication algebra. In fact, we cannot improve the lower bounds we gave above for $\mathrm{s}_{\mathbf{A}}$, $\mathrm{i}_{\mathbf{A}}$, $\mathrm{g}_{\mathbf{A}}$. The congruence functions, on the other hand, grow much more rapidly for this algebra.

Let Z be any nonvoid anti-chain in A^n, and $Z^{\geq}$ be the order-filter generated by Z. Then Z is the set of minimal members of $Z^{\geq}$; and the equivalence relation with one non-singleton class, namely, $Z^{\geq}$, is a congruence relation, θ_Z, of $\mathbf{A}^n$. This gives the lower bound for $\mathrm{c}_{\mathbf{A}}(n)$ figured in the table. The set $\{(z, \bar{1}) : z \in Z\}$ is an independent generating set of θ_Z. This gives the lower bound for $\mathrm{ic}_{\mathbf{A}}(n)$ written in the table. Now let X be any generating set for θ_Z. Clearly, we must have $Z \subseteq \bigcup \{\{x,y\} : (x,y) \in X\}$, thereby giving the lower bound for $\mathrm{gc}_{\mathbf{A}}(n)$ found in the table.

G-set. Finally, consider the algebra $\langle \{0,1\}, \pi \rangle$. For $f \in A^{n-1}$ let $f_0 \in A^n$ be the function that extends f with $f_0(n-1) = 0$, and let $f_1 = \pi \circ f_0$. The subuniverses of $\mathbf{A}^n$ are the subsets X such that for all $f \in A^{n-1}$, $f_0 \in X \leftrightarrow f_1 \in X$. For any subuniverse X, the minimal generating sets all have the same cardinality; they are the sets $Y \subseteq X$ such that for every $f \in A^{n-1}$ with $f_0 \in X$, $|\{f_0, f_1\} \cap Y| = 1$. With these facts in hand, the reader can easily establish the first three entries in our table, for this algebra.

Of course, $\mathrm{c}_{\mathbf{A}}(n) \leq \lg(B(2^n)) =_\Theta n2^n$. But also, it is easy to see that

$$(n-1)2^{n-1} =_\Theta \lg(B(2^{n-1})) \leq \mathrm{c}_{\mathbf{A}}(n)\,.$$

Thus, $\mathrm{c}_{\mathbf{A}}(n) =_\Theta n2^n$ follows from the observation that $(n-1)2^{n-1} =_\Theta n2^n$. The calculations for $\mathrm{ic}_{\mathbf{A}}(n)$ and $\mathrm{gc}_{\mathbf{A}}(n)$ are straightforward; we leave them to the reader.

Finally, we note that for every $k \geq 2$ there exists a finite algebra $\mathbf{A}$ with universe $A = \{0,1\}$ such that $\mathrm{i}_{\mathbf{A}}(n) =_\Theta \mathrm{s}_{\mathbf{A}}(n) =_\Theta n^k$. Indeed, if $k = 2$, then we can use the 2-element lattice as shown above, while if $k \geq 3$, then we can use the algebra $\mathbf{A} = \langle \{0,1\}, F_{k+1} \rangle$ where F_{k+1} is the operation in $k+1$ variables defined by $F_{k+1}(a_0, \ldots, a_k) = 1$ if $a_i = 1$ for at least two $i \in \{0, 1, \ldots, k\}$, and $F_{k+1}(a_0, \ldots, a_k) = 0$ otherwise. F_{k+1} is a near unanimity term for $\mathbf{A}$, and it is known that $\mathbf{A}$ has no near unanimity term of arity $\leq k$. Hence $\mathrm{i}_{\mathbf{A}}(n) =_\Theta \mathrm{s}_{\mathbf{A}}(n) =_\Theta n^k$ by Corollary 4.6.

References

1. Kirby A. Baker and Alden F. Pixley. Polynomial interpolation and the Chinese remainder theorem for algebraic systems. *Math. Z.*, 143(2):165–174, 1975.
2. Joel Berman and Paweł M. Idziak. Generative complexity in algebra. *Mem. Amer. Math. Soc.*, 175(828):viii+159, 2005.
3. Andrei Bulatov, Hubie Chen, and Víctor Dalmau. Learning intersection-closed classes with signatures. *Theor. Comput. Sci.*, 382(3):209–220, 2007.
4. Andrei Bulatov and Víctor Dalmau. A simple algorithm for Mal'tsev constraints. *SIAM J. Comput.*, 36(1):16–27 (electronic), 2006.
5. Andrei Bulatov, Peter Jeavons, and Andrei Krokhin. Classifying the complexity of constraints using finite algebras. *SIAM J. Comput.*, 34(3):720–742 (electronic), 2005.
6. Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1981.
7. Hubie Chen. The expressive rate of constraints. *Ann. Math. Artif. Intell.*, 44(4):341–352, 2005.
8. Víctor Dalmau. *Computational complexity of problems over generalized formulas*. PhD thesis, Universitat Politécnica de Catalunya, 2000.
9. Víctor Dalmau. Generalized majority-minority operations are tractable. In *LICS '05: Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science (LICS' 05)*, pages 438–447, Washington, DC, USA, 2005. IEEE Computer Society.
10. Víctor Dalmau and Peter Jeavons. Learnability of quantified formulas. *Theoret. Comput. Sci.*, 306(1-3):485–511, 2003.
11. Alan Day. A characterization of modularity for congruence lattices of algebras. *Canad. Math. Bull.*, 12:167–173, 1969.
12. Tomás Feder and Moshe Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: a study through Datalog and group theory. *SIAM J. Comput.*, 28(1):57–104 (electronic), 1999.
13. R. Freese and R. McKenzie. *Commutator Theory for Congruence Modular Varieties*, volume 125 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1987.
14. O. C. García and W. Taylor. The lattice of interpretability types of varieties. *Mem. Amer. Math. Soc.*, 50(305):v+125, 1984.
15. H. Peter Gumm. Geometrical methods in congruence modular algebras. *Mem. Amer. Math. Soc.*, 45(286):viii+79, 1983.
16. Bradd Hart, Sergei Starchenko, and Matthew Valeriote. Vaught's conjecture for varieties. *Trans. Amer. Math. Soc.*, 342(1):173–196, 1994.
17. David Hobby and Ralph McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988. Revised edition: 1996.
18. Paweł Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard. Tractability and learnability arising from algebras with few subpowers. In *LICS '07: Proceedings of the 22nd Annual IEEE Symposium on Logic in Computer Science*, pages 213–224, Washington, DC, USA, 2007. IEEE Computer Society.

19. Paweł Idziak, Ralph McKenzie, and Matthew Valeriote. The structure of locally finite varieties with polynomially many models. to appear in the Journal of the American Mathematical Society, 2008.
20. Peter Jeavons. On the algebraic structure of combinatorial problems. *Theoret. Comput. Sci.*, 200(1-2):185–204, 1998.
21. Keith Kearnes and Ágnes Szendrei. Clones of parallelogram algebras. preprint, 2007.
22. Petar Marković and Ralph McKenzie. Few subpowers, congruence distributivity and near-unanimity. *Algebra Universalis*, 58(2):119–128, 2008.
23. Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. *Algebras, lattices, varieties. Vol. I*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.
24. Michael Morley. Categoricity in power. *Trans. Amer. Math. Soc.*, 114:514–538, 1965.
25. Luís Sequeira. Near-unanimity is decomposable. *Algebra Universalis*, 50(2):157–164, 2003.
26. S. Shelah. *Classification theory and the number of nonisomorphic models*, volume 92 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, second edition, 1990.

Department of Mathematics, University of Illinois at Chicago
E-mail address: jberman@uic.edu

Department of Theoretical Computer Science, Jagiellonian University, Krakow, Poland
E-mail address: idziak@tcs.uj.edu.pl

Department of Mathematics and Informatics, University of Novi Sad, Serbia
E-mail address: pera@im.ns.ac.yu

Department of Mathematics, Vanderbilt University, Nashville, U.S.A.
E-mail address: mckenzie@math.vanderbilt.edu

Department of Mathematics, McMaster University, Hamilton, Ontario
E-mail address: matt@math.mcmaster.ca

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario
E-mail address: rdwillar@uwaterloo.ca