ON THE COMPLEXITY OF SOME MALTSEV CONDITIONS

RALPH FREESE, MATTHEW A. VALERIOTE

Abstract. This paper studies the complexity of determining if a finite algebra generates a variety that satisfies various Maltsev conditions, such as congruence distributivity or modularity. For idempotent algebras we show that there are polynomial time algorithms to test for these conditions but that in general these problems are EXPTIME complete. In addition, we provide sharp bounds in terms of the size of two-generated free algebras on the number of terms needed to witness various Maltsev conditions, such as congruence distributivity.

1. Introduction

Many important features of an algebra and the variety it generates are determined by the idempotent term operations of the algebra. In particular several well studied properties of a variety, such as congruence permutability, distributivity, and modularity, are governed by the presence of systems of idempotent term operations that satisfy prescribed identities. Such systems are examples of idempotent Maltsev conditions. This paper is concerned with determining the complexity of deciding if a finite algebra $\mathbf{A}$ generates, for example, a congruence distributive variety, and, if so, of finding a system of idempotent term operations that witness this. (Jónsson's Maltsev condition for congruence distributivity is given in Section 7.)

Our strongest results are obtained for idempotent algebras. In this case we produce polynomial time algorithms that determine, for $\mathbf{A}$ idempotent, if $\boldsymbol{V}(\mathbf{A})$, the variety generated by $\mathbf{A}$, has any of the above properties, as well as several others. The key to this is that we don't need to look at large cartesian powers of $\mathbf{A}$ to determine if the property in question holds. For example, for $\mathbf{A}$ finite and idempotent $\boldsymbol{V}(\mathbf{A})$ is

2000 *Mathematics Subject Classification.* 08B05, 08B10, 68Q25, 03C05.

Key words and phrases. Maltsev condition, tame congruence theory, idempotent algebra, computational complexity, congruence distributive, congruence modular.

The second author acknowledges the support of the NSERC of Canada.

congruence distributive if and only if every 3-generated subalgebra of $\mathbf{A}^2$ is; it is modular if every 4-generated subalgebra of $\mathbf{A}^2$ is.

On the other hand for non-idempotent algebras we show that there is no polynomial time algorithm to determine if $\boldsymbol{V}(\mathbf{A})$ is congruence distributive or modular. In fact in Section 9 we show that these, and several other problems, are EXPTIME complete. In essence these results demonstrate that in general, it is very difficult to extract from a given finite algebra information about the nature of its idempotent term operations.

We also investigate the number of terms needed to witness various Maltsev conditions for a variety. For example, in Section 7 we define the *Jónsson level* of a congruence distributive variety $\mathcal{V}$ to be the least k such that $\mathcal{V}$ has terms satisfying (7.1). We show that, if $m = |\mathbf{F}_{\mathcal{V}}(x, y)|$, then the Jónsson level of $\mathcal{V}$ is at most $2m-2$ and give an example where this bound is obtained. Similar results are obtained for Gumm terms for modularity and Hagemann-Mitschke terms for k-permutability.

The necessary background on the universal algebra used in this paper can be found in [2] or [22]. One class of algebras that we pay particular attention to are the idempotent algebras.

Definition 1.1.

(1) An operation $f(x_1, \dots, x_n)$ on a set A is idempotent if for all $a \in A$, $f(a, a, \dots, a) = a$.
(2) An algebra $\mathbf{A}$ is idempotent if all of its basic operations are idempotent.

Note that since the composition of idempotent operations is idempotent, it follows that all term operations of an idempotent algebra are idempotent. The proof of the following proposition is elementary and is left as an exercise.

Proposition 1.2. *Let $\mathbf{A}$ be an algebra.*

(1) *$\mathbf{A}$ is idempotent if and only if for each $a \in A$, $\{a\}$ is a subuniverse of $\mathbf{A}$.*
(2) *If $\mathbf{A}$ is idempotent and C is a congruence class of some congruence α of $\mathbf{A}$, then C is a subuniverse of $\mathbf{A}$.*

2. Tame Congruence Theory

We make use of the structure theory of finite algebras called Tame Congruence Theory that Hobby and McKenzie developed in the 1980s. Details of this theory can be found in [11] or [3]. As basic tame congruence theoretic terminology and results arise in this paper we will refer the reader to the relevant parts of [11].

According to tame congruence theory, given a covering pair of congruences $\alpha \prec \beta$ of a finite algebra $\mathbf{A}$, the local behaviour of the β-classes is captured by the so-called (α, β)-traces (Definition 2.15 of [11]) and that modulo α, the induced structure on them is limited to one of five possible types:

(1) A unary algebra whose basic operations are all permutations (unary type);
(2) A one-dimensional vector space over some finite field (affine type);
(3) A 2-element boolean algebra (boolean type);
(4) A 2-element lattice (lattice type);
(5) A 2-element semilattice (semilattice type).

This allows us to assign a type from $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$ to each covering pair $\alpha \prec \beta$ of a finite algebra $\mathbf{A}$ (Definition 5.1 of [11]); we denote this type by $\mathrm{typ}(\alpha, \beta)$. The set of all types that are realized by covering pairs of congruences of a finite algebra $\mathbf{A}$ is denoted by $\mathrm{typ}\{\mathbf{A}\}$ and if $\mathcal{K}$ is a class of algebras, then $\mathrm{typ}\{\mathcal{K}\}$ denotes the union of all of the typesets of the finite algebras in $\mathcal{K}$.

The set of types is ordered by the *lattice of types* given in Figure 1.

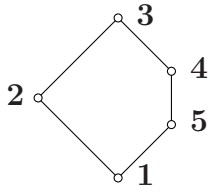

FIGURE 1. The Pentagon of Types

The following results demonstrate that for a finite idempotent algebra $\mathbf{A}$, whether or not $\boldsymbol{V}(\mathbf{A})$ omits one of the order ideals of the lattice of types can be determined locally.

Proposition 2.1. *If* $\mathbf{A}$ *is a finite idempotent algebra and* $\mathbf{i} \in \mathrm{typ}(\boldsymbol{V}(\mathbf{A}))$ *then there is a finite strictly simple algebra* $\mathbf{S}$ *of type* $\mathbf{j}$ *for some* $\mathbf{j} \leq \mathbf{i}$ *in* $\boldsymbol{HS}(\mathbf{A})$. *If*

(1) $\mathbf{j} = \mathbf{1}$ *then* $\mathbf{S}$ *is term equivalent to a 2-element set;*
(2) $\mathbf{j} = \mathbf{2}$ *then* $\mathbf{S}$ *is term equivalent to the idempotent reduct of a module;*
(3) $\mathbf{j} = \mathbf{3}$ *then* $\mathbf{S}$ *is functionally complete ;*
(4) $\mathbf{j} = \mathbf{4}$ *then* $\mathbf{S}$ *is polynomially equivalent to a 2-element lattice;*
(5) $\mathbf{j} = \mathbf{5}$ *then* $\mathbf{S}$ *is term equivalent to a 2-element semilattice.*

Proof. This is a combination of Proposition 3.1 from [27] and Theorem 6.1 from [25]. □

Corollary 2.2. *Let* $\mathbf{A}$ *be a finite idempotent algebra and* T *an order ideal in the lattice of types. Then* $\boldsymbol{V}(\mathbf{A})$ *omits* T *if and only if* $\boldsymbol{S}(\mathbf{A})$ *does. In particular,* $\boldsymbol{V}(\mathbf{A})$ *omits* $\mathbf{1}$ *and* $\mathbf{2}$ *if and only if* $\boldsymbol{S}(\mathbf{A})$ *omits* $\mathbf{1}$ *and* $\mathbf{2}$*.*

The following lemma ties in with the previous proposition and will be used in Section 6. An algebra is strictly simple if it is simple (i.e., has no non-trivial congruences) and has no non-trivial subalgebras (i.e., has no proper subalgebras with more than one element).

Lemma 2.3. *Let* $\mathbf{A}$ *be a finite idempotent algebra and let* $\mathbf{S} \in \boldsymbol{H}\boldsymbol{S}(\mathbf{A})$ *be strictly simple. Then there are elements* a, $b \in A$ *such that, if* $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(a, b)$*, then* $1_B = \mathrm{Cg}^{\mathbf{B}}(a, b)$ *and is join irreducible with unique lower cover* ρ *such that* $\mathbf{S} = \mathbf{B}/\rho$*.*

Proof. Choose $\mathbf{B} \in \boldsymbol{S}(\mathbf{A})$ as small as possible having $\mathbf{S}$ as a homomorphic image, say $\mathbf{S} = \mathbf{B}/\rho$. We claim that if $a, b \in B$ with $(a, b) \notin \rho$ then then they generate $\mathbf{B}$. To see this, let $\mathbf{B}' = \mathrm{Sg}^{\mathbf{B}}(a, b)$ and let h be the quotient map from $\mathbf{B}$ to $\mathbf{S}$ with kernel ρ. Then $h(B')$ is a non-trivial subuniverse of $\mathbf{S}$ and so must equal S. Thus $B' = B$.

Now let $a, b \in B$ with $(a, b) \notin \rho$. Since the block of $\mathrm{Cg}^{\mathbf{B}}(a, b)$ containing a and b is a subuniverse of B then from the previous paragraph, we conclude that $\mathrm{Cg}^{\mathbf{B}}(a, b) = 1_B$ and that ρ is its unique lower cover. □

3. Congruence Modular Idempotent Varieties

Corollary 2.2 is the starting point of our development of a polynomial-time algorithm that determines if a given finite idempotent algebra generates a congruence modular variety. According to the characterization of locally finite congruence modular (distributive) varieties found in Chapter 8 of [11], a finite algebra $\mathbf{A}$ generates a congruence modular (distributive) variety $\mathcal{V}$ if and only if the typeset of $\mathcal{V}$ is contained in $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ ($\{\mathbf{3}, \mathbf{4}\}$) and all minimal sets of prime quotients of finite algebras in $\mathcal{V}$ have empty tails (Definition 2.15 of [11]). Note that in the congruence distributive case the empty tails condition is equivalent to the minimal sets all having exactly two elements.

It follows from Corollary 2.2, that if $\mathbf{A}$ is idempotent then one can test the first condition, on omitting types $\mathbf{1}$ and $\mathbf{5}$ (or $\mathbf{1}$, $\mathbf{2}$, and $\mathbf{5}$) by searching for a 2-generated subalgebra of $\mathbf{A}$ whose typeset is not contained in $\{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ ($\{\mathbf{3}, \mathbf{4}\}$). As noted in Section 6, this test can be performed in polynomial time, as a function of the size of $\mathbf{A}$.

The following sequence of lemmas establishes that when $\mathbf{A}$ is finite, idempotent and $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ omits types **1** and **5**, then to test for the existence of tails in $\mathcal{V}$ we need only look for them in the 3-generated subalgebras of $\mathbf{A}^2$.

Throughout the remainder of this section, let $\mathcal{S}$ be a finite set of finite, similar, idempotent algebras closed under the taking of subalgebras such that $\mathcal{V} = \boldsymbol{V}(\mathcal{S})$ omits **1** and **5**. We will suppose that some finite algebra $\mathbf{B}$ in $\mathcal{V}$ has a prime quotient whose minimal sets have non-empty tails and show that there is a 3-generated subalgebra of the product of two members of $\mathcal{S}$ with this property.

Since $\mathcal{S}$ is closed under the taking of subalgebras then we may assume that the algebra $\mathbf{B}$ from the previous paragraph is a subdirect product of a finite number of members of $\mathcal{S}$. Choose n minimal such that for some $\mathbf{A}_i \in \mathcal{S}$, the product $\prod_{i \leq n} \mathbf{A}_i$ has a subdirect product $\mathbf{B}$ that has a prime quotient with non-empty tails. Under the assumption that $n > 1$ we will prove that $n = 2$.

For this n, select the $\mathbf{A}_i$ and $\mathbf{B}$ so that $|B|$ is as small as possible. Let $\alpha \prec \beta$ be a prime quotient of $\mathbf{B}$ with non-empty tails and choose β minimal with this property. Let U be an $\langle \alpha, \beta \rangle$-minimal set and let N be an $\langle \alpha, \beta \rangle$ trace of U. Let 0 and 1 be two distinct members of N with $(0, 1) \notin \alpha$.

Lemma 3.1. *Let t be a member of the tail of U. Then β is the congruence of $\mathbf{B}$ generated by the pair $(0, 1)$ and $\mathbf{B}$ is generated by $\{0, 1, t\}$.*

Proof. Using Lemma 6.2 of [11] our assumptions on β imply that it is join irreducible and that α is its unique subcover. So, any pair $(a, b) \in \beta \setminus \alpha$ will generate the congruence β. In particular, β is generated by the pair $(0, 1)$.

Let $\mathbf{C}$ be the subalgebra of $\mathbf{B}$ generated by $\{0, 1, t\}$. We will obtain a contradiction under the assumption that $|C| < |B|$ and the minimal sets of $\mathbf{C}$ all have empty tails. Let β' and α' be the restrictions of β and α to C, respectively. Then $\alpha' < \beta'$ since $(0, 1) \in \beta' \setminus \alpha'$ and so there are $\delta \prec \gamma$ in $\mathrm{Con}(\mathbf{C})$ with $\alpha' \leq \delta \prec \gamma \leq \beta'$ and such that $(0, 1) \in \gamma \setminus \delta$.

Suppose that $|C| < |B|$ and all $\langle \delta, \gamma \rangle$ minimal sets have empty tails. Let V be a $\langle \delta, \gamma \rangle$ minimal set and let $p(x)$ be some polynomial of $\mathbf{C}$ with range V and with $(p(0), p(1)) \notin \delta$. Such a polynomial exists by Theorem 2.8 of [11] since $(0, 1) \in \gamma \setminus \delta$.

The polynomial $p(x)$ can be expressed in the form $s^{\mathbf{C}}(x, 0, 1, t)$ for some term $s(x, y, z, w)$ of $\mathcal{V}$ and so extends to a polynomial $p'(x) = s^{\mathbf{B}}(x, 0, 1, t)$ of $\mathbf{B}$. Since $(p(0), p(1)) \in \gamma \setminus \delta$ then $(p'(0), p'(1)) \in \beta \setminus \alpha$ and so p' must map the minimal set U onto a polynomially isomorphic set W. If the type of $\langle \delta, \gamma \rangle$ is **3** or **4** then by assumption, the minimal set

V has exactly 2 elements (since it has no tail) and so either $p(t) = p(0)$ or $p(t) = p(1)$. In either case, this implies that p' maps the tail element t of U to the body of the minimal set W. This is impossible, since U and W are polynomially isomorphic.

If the type of $\langle \delta, \gamma \rangle$ is **2** then $\mathbf{C}|_V$ has a Maltsev polynomial $s(x, y, z)$. Since $\{p(0), p(1), p(t)\} \subseteq V$ and since this polynomial has an extension to a polynomial of $\mathbf{B}$ it follows that there is a polynomial $f(x, y, z)$ of $\mathbf{B}$ that satisfies the Maltsev identities when restricted to the set $\{p'(0), p'(1), p'(t)\} \subseteq W$. This contradicts Lemma 4.26 of [11], since $p'(0)$ and $p'(1)$ are in the body of W and $p'(t)$ is in the tail, since p' is a polynomial isomorphism from U to W. □

For $i \leq n$, let π_i be the projection homomorphism from $\mathbf{B}$ onto $\mathbf{A}_i$ and let ρ_i be the kernel of π_i. By the minimality of n we know that the intersection of any proper subset of the ρ_i, $1 \leq i \leq n$ is strictly above 0_B.

Lemma 3.2. *Let ρ be the intersection of a proper subset of the ρ_i, $1 \leq i \leq n$. Either $\beta \leq \rho$ or $\alpha \vee \rho = 1_B$.*

Proof. Suppose that $\beta \not\leq \rho$ (or equivalently $(0, 1) \notin \rho$). Since β is join irreducible then $\beta \wedge \rho \leq \alpha$ and so $\beta \wedge \rho = \alpha \wedge \rho$. Furthermore, $\alpha \vee \rho = \beta \vee \rho$, or else we can find a prime quotient between these two congruences that is perspective with $\langle \alpha, \beta \rangle$. But then the algebra $\mathbf{B}/\rho$ has a prime quotient whose minimal sets have non-empty tails. Since this algebra is isomorphic to a subdirect product of fewer than n members of $\mathbb{S}$, we conclude, by the minimality of n, that indeed $\alpha \vee \rho = \beta \vee \rho$.

Thus the set

$$\mathcal{P} = \{\beta \wedge \rho, \rho, \alpha, \beta, \alpha \vee \rho\}$$

forms a pentagon in $\mathbf{Con}(\mathbf{B})$. Let C be the $(\alpha \vee \rho)$-class that contains 0 and let $M = C \cap U$. Note that C contains 1 and, since $\mathbf{B}$ is idempotent, that C is a subuniverse of $\mathbf{B}$. By Lemma 2.4 of [11], we conclude that the restriction to M is a surjective lattice homomorphism from the interval $I[0_B, \alpha \vee \rho]$ in $\mathbf{Con}(\mathbf{B})$ to the interval $I[0_M, (\alpha \vee \rho)|_M]$ in $\mathbf{Con}(\mathbf{B})|_M$. Note that since $(0, 1) \in \beta|_M \setminus \alpha|_M$, this restriction map separates α and β. Then, the image under the restriction map of the pentagon $\mathcal{P}$ is a pentagon in $\mathbf{Con}(\mathbf{B})|_M$. This implies that M contains some elements of the tail of U, since otherwise $\mathbf{Con}(\mathbf{B})|_M$ is modular (in the type **3** or **4** case, $|M| = 2$, and in the type **2** case, $\mathbf{B}|_M$ is Maltsev). Thus, there is some t in the tail of U with $(0, t) \in \alpha \vee \rho$. Using Lemma 3.1 we conclude that $C = B$ since it contains $\{0, 1, t\}$. Thus, $\alpha \vee \rho = 1_B$. □

Lemma 3.3. *$\alpha \vee \rho_i < 1_B$ for at least one i and $\alpha \vee \rho_j = 1_B$ for at least one j.*

Proof. Suppose that $\alpha \vee \rho_i = 1_B$ for all i. By Theorem 7.7 of [11] we know that modulo the solvability congruence, $\mathbf{Con}(\mathbf{B})$ is join semi-distributive and so 1_B is solvably related to

$$\alpha \vee (\bigwedge_{i \leq n} \rho_i) = \alpha \vee 0_B = \alpha.$$

Then, the algebra $\mathbf{B}/\alpha$ is solvable and so lies in the subvariety of all locally solvable algebras of $\mathcal{V}$. Since $\mathcal{V}$ omits type **1**, then this subvariety has typeset $\{\mathbf{2}\}$ and so, by Theorem 7.11 of [11], is congruence permutable. But then $\mathbf{B}/\alpha$ can't have any minimal sets with tails. So, for at least one i we must have that $\alpha \vee \rho_i < 1_B$.

Finally, suppose that $\alpha \vee \rho_i < 1_B$ for all $i \leq n$. Then $\beta \leq \rho_i$ for all $i \leq n$ and so $\beta \leq \bigwedge_{i \leq n} \rho_i = 0_B$, a contradiction. □

Theorem 3.4. *Let $\mathcal{V}$ be the variety generated by some finite set $\mathcal{S}$ of finite, idempotent algebras that is closed under taking subalgebras. If $\mathcal{V}$ omits types **1** and **5** and some finite member of $\mathcal{V}$ has a prime quotient whose minimal sets have non-empty tails then there is some 3-generated algebra $\mathbf{B}$ with this property that belongs to $\mathcal{S}$ or is a subdirect product of two algebras from $\mathcal{S}$.*

Proof. Choose $n > 0$, $\mathbf{A}_i \in \mathcal{S}$, for $1 \leq i \leq n$ and $\mathbf{B}$ as above. From Lemma 3.1 we know that $\mathbf{B}$ is 3-generated. If $n > 1$ then by the previous lemma we can choose i and $j \leq n$ with $\beta \leq \rho_i$ and $\alpha \vee \rho_j = 1_B$. If $n > 2$ then Lemma 3.2 applies to $\rho = \rho_i \wedge \rho_j$ and so we know that either $\beta \leq \rho$ or $\alpha \vee \rho = 1_B$. This yields a contradiction as the former is not possible, since $\beta \not\leq \rho_j$ and the latter can't hold since both α and ρ are below ρ_i.

So, the minimality of n forces $n \leq 2$ and the result follows. Note that in the case that $n = 2$, we have that the congruences $\{0_B, \alpha, \beta, \rho_i, 1_B\}$ form a sublattice of $\mathbf{Con}(\mathbf{B})$ that is isomorphic to the pentagon, for i such that $\alpha \vee \rho_i = 1_B$. □

By taking a suitable idempotent reduct of a 3-element algebra related to Polin's Variety [5], it is possible to find an idempotent algebra $\mathbf{A}$ such that $\boldsymbol{V}(\mathbf{A})$ is not congruence modular, omits types **1** and **5** (in fact has typeset $\{\mathbf{3}\}$), but with the algebras in $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ having minimal sets with empty tails. This demonstrates that in general one must look for tails in subalgebras of $\mathbf{A}^2$.

Day Quadruples. In this subsection we introduce Day quadruples which will play a role in our fastest algorithms for testing for congruence modularity, both in the idempotent and non-idempotent cases.

If a, b, c and d are elements of an algebra $\mathbf{A}$, the sublattice of $\mathbf{Con}(\mathbf{A})$ generated by

$$\alpha = \mathrm{Cg}^{\mathbf{A}}(c, d)$$
$$\beta = \mathrm{Cg}^{\mathbf{A}}((a, b), (c, d))$$
$$\gamma = \mathrm{Cg}^{\mathbf{A}}((a, c), (b, d))$$

is a homomorphic image of the lattice in Figure 2.

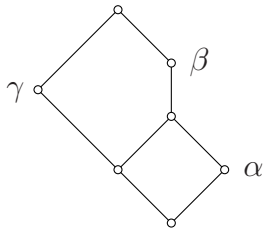

FIGURE 2. Day's Extended Pentagon

Of course if $\boldsymbol{V}(\mathbf{A})$ is congruence modular all such pentagons must collapse. Formalizing this, we call a quadruple (a, b, c, d) in an algebra $\mathbf{A}$ a *Day quadruple* if in the subalgebra $\mathbf{B}$ generated by $\{a, b, c, d\}$

$$(a, b) \notin \mathrm{Cg}^{\mathbf{B}}(c, d) \vee [\mathrm{Cg}^{\mathbf{B}}((a, b), (c, d)) \wedge \mathrm{Cg}^{\mathbf{B}}((a, c), (b, d))] \tag{3.1}$$

In his Master's thesis [4] Alan Day gave a Maltsev condition defining congruence modularity and proved the following.

Theorem 3.5. *Let $\mathcal{V}$ be a variety and let a, b, c and d be the free generators of $\mathbf{F}_{\mathcal{V}}(a, b, c, d)$. Then $\mathcal{V}$ is congruence modular if and only if (a, b, c, d) is not a Day quadruple.*

By modifying a construction of Kearnes and Kiss found in [16] we obtain the following characterization of finite idempotent algebras that generate congruence modular varieties.

Theorem 3.6. *Let $\mathbf{A}$ be a finite idempotent algebra and $\mathcal{V}$ be the variety it generates. Then $\mathcal{V}$ fails to be congruence modular if and only if there is a Day quadruple (a, b, c, d) in $\mathbf{A}^2$. Moreover, this Day quadruple can be chosen so that*

1. *$a = (x_0, x_1)$, $b = (x_0, y_1)$, $c = (y_0, x_1)$, and $d = (y_0, y_1)$ for some x_0, x_1, y_0, y_1 in $\mathbf{A}$;*

(2) *if* $\mathcal{V}$ *omits type* **1** *then these elements may be chosen so that* $d \in \mathrm{Sg}^{\mathbf{A^2}}(a, b, c)$*;*
(3) *if* $\mathcal{V}$ *omits both type* **1** *and type* **5** *then these elements may be chosen so that* $d \in \mathrm{Sg}^{\mathbf{A^2}}(a, b, c)$ *and* $c \in \mathrm{Sg}^{\mathbf{A^2}}(a, b, d)$*.*

Proof. One direction is trivial so assume that $\mathcal{V}$ is not congruence modular. If $\mathcal{V}$ admits type **1** or **5** then then there is a strictly simple algebra $\mathbf{B}$ in $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ that is term equivalent to a 2-element set or a 2-element semilattice. It is easy to see that in each case $\mathbf{B}^2$ has a Day quadruple satisfying (1). Now if under a homomorphism the elements a, b, c, d map to a', b', c', d', respectively, and (a', b', c', d') is a Day quadruple, then (a, b, c, d) is also a Day quadruple. Using this it follows that $\mathbf{A}^2$ has a Day quadruple satisfying (1). Using the fact that the square of a two-element semilattice is three generated, it is easy to see that (2) also holds. So we may assume $\mathcal{V}$ omits types **1** and **5**. Since $\mathcal{V}$ is not modular it must contain an algebra with a minimal set with a non-empty tail by Theorem 8.5 of [11].

By Theorem 3.4 there is a 3-generated subalgebra $\mathbf{B}$ of $\mathbf{A}$ or of $\mathbf{A}^2$ which has a minimal set with a non-empty tail. This gives two cases and we begin with the latter; that is, we assume there is a 3-generated subalgebra $\mathbf{B}$ of $\mathbf{A}^2$ which has a minimal set with a non-empty tail, but no 3-generated subalgebra of $\mathbf{A}$ has such a minimal set.

The proof of Theorem 3.4 and the lemmas leading to it show that we may assume that $\mathbf{B}$ is generated by $\{0, 1, t\}$, $\beta = \mathrm{Cg}^{\mathbf{B}}(0, 1)$ is join irreducible with lower cover α, and there is an $\langle\alpha, \beta\rangle$-minimal set U such that 0 and 1 are contained in a trace and t is in the tail. Moreover, by Lemma 3.1, $\mathbf{B}$ is generated by 0, 1, and *any* element of the tail. Also, $\beta \leq \rho_1$ and $\alpha \vee \rho_2 = 1_{\mathbf{B}}$, where ρ_i are the projection kernels.

First we show that we may assume $(0, t) \in \rho_2$. Since $\alpha \vee \rho_2 = 1_{\mathbf{B}}$, there is a α–ρ_2 path from 0 to 1. Since the minimal set is the image of $\mathbf{B}$ under an idempotent polynomial, we may assume this path lies in the minimal set. If the type of this minimal set is **3** or **4**, the body is just $\{0, 1\}$. These elements are ρ_1–related, hence not ρ_2–related (otherwise they would be equal). It follows that the first link of the path must relate 0 to a tail element and we can use this element in place of t.

If the type is **2** the body has a Maltsev term so if the path lies entirely in the body, there is a path of the form $0\ \alpha\ 0'\ \rho_2\ 1$ which implies $0'$ and 1 are related by both ρ_1 and ρ_2, and so equal which implies 0 and 1 are α related, a contradiction. Since α cannot connect a body element to a tail element, there must be body element ρ_2 related to a tail element.

In general, if a congruence θ contains some (a, c) with a in the body and c in the tail of a type **2** minimal set, then every element of the body is θ-related to something in the tail. To see this let $d(x, y, z)$ be a pseudo-Maltsev operation for the minimal set and let b be in the body. Then $f(x) = d(b, x, a)$ is a permutation of the minimal set and so must map the tail to the tail. Then $b = d(b, a, a)\ \theta\ d(b, c, a)$ and the latter is in the tail.

Thus we may assume $(0, t) \in \rho_2$, as asserted. These arguments also show that every element of the body is ρ_2 related to some tail element.

Let $\mathbf{A}_i = \mathbf{B}/\rho_i$, $i = 1, 2$. Then we can write $0 = \langle u, v\rangle$, $1 = \langle u, w\rangle$, $t = \langle r, v\rangle$ for some u and $r \in \mathbf{A}_1$ and v and $w \in \mathbf{A}_2$. As noted, $1 = \langle u, w\rangle$ is ρ_2 related to a tail element which must be $\langle s, w\rangle$, for some $s \in A_1$.

Since $\mathbf{B}$ is generated by 0, 1, and t, there is a ternary term g (necessarily idempotent since $\mathbf{B}$ is) such that $\langle s, w\rangle = g(\langle u, v\rangle, \langle u, w\rangle, \langle r, v\rangle)$. But then $\langle s, v\rangle = g(\langle u, v\rangle, \langle u, v\rangle, \langle r, v\rangle)$ is in $\mathbf{B}$. Since $\langle u, v\rangle$ and $\langle u, w\rangle$ are β-related, $\langle s, v\rangle$ and $\langle s, w\rangle$ are as well.

We claim $\langle s, v\rangle$ is in the minimal set U. To see this let e be the idempotent unary polynomial mapping $\mathbf{B}$ onto the minimal set. Then, since $\langle s, v\rangle$ is β (and hence ρ_1) related to $\langle s, w\rangle \in U$ and ρ_2 related to $0 = \langle u, v\rangle \in U$, $e(\langle s, v\rangle)\ \rho_1\ \langle s, w\rangle$ and $e(\langle s, v\rangle)\ \rho_2\ \langle u, v\rangle$. Hence $e(\langle s, v\rangle) = \langle s, v\rangle$; so $\langle s, v\rangle \in U$.

Now, since $\langle s, w\rangle$ is in the tail, $\langle s, w\rangle\ \alpha\ \langle s, v\rangle$. Let $a = 0 = \langle u, v\rangle$, $b = 1 = \langle u, w\rangle$, $c = \langle s, v\rangle$, and $d = \langle s, w\rangle$. Since $\mathrm{Cg}^{\mathbf{B}}((a, b), (c, d)) \leq \rho_1$ and $\mathrm{Cg}^{\mathbf{B}}((a, c), (b, d)) \leq \rho_2$ their intersection is $0_{\mathbf{B}}$. Since $\mathrm{Cg}^{\mathbf{B}}(c, d) \leq \alpha$, $\langle a, b\rangle \notin \mathrm{Cg}^{\mathbf{B}}(c, d)$ and thus (a, b, c, d) is a Day quadruple. Clearly item (1) holds and, since 0, 1 and any tail element generate $\mathbf{B}$, item (3) also holds.

Now we turn to the other case: we assume that some 3-generated subalgebra of $\mathbf{A}$ has minimal sets with non-empty tails with respect to some prime quotient $\langle\alpha, \beta\rangle$. As noted above (see Lemma 3.1), it follows that there is a subalgebra $\mathbf{B}$ of $\mathbf{A}$ generated by elements $\{0, 1, t\}$ such that these three elements belong to some minimal set U of $\mathbf{B}$ with $\{0, 1\}$ belonging to an $\langle\alpha, \beta\rangle$-trace contained in U and t in the tail of U. In addition, we may assume that no proper subalgebra of $\mathbf{B}$ has minimal sets with non-empty tails.

We may choose the $\langle\alpha, \beta\rangle$-minimal set U and elements 0 and 1 contained in some $\langle\alpha, \beta\rangle$-trace of U with $\mathbf{C} = \mathrm{Sg}^{\mathbf{B}}(\{0, 1\})$ as small as possible. Let $\nu = \mathrm{Cg}^{\mathbf{C}}((0, 1))$ and let μ be a congruence of $\mathbf{C}$ such that $\alpha|_C \wedge \nu \leq \mu \prec \nu$. Note that since $\mathbf{C}$ is a proper subalgebra of $\mathbf{B}$ (it is contained in the β-class of 0), all of its minimal sets have empty tails.

Let W be a minimal set of $\mathbf{C}$ with respect to this covering pair. Since $(0,1) \in \nu \setminus \mu$, there is a unary polynomial $p(x)$ of $\mathbf{C}$ with range W and with $(p(0), p(1)) \notin \mu$, and hence $(p(0), p(1)) \notin \alpha$. But then in $\mathbf{B}$, the set $\{p(0), p(1)\}$ is contained in the body of some $\langle \alpha, \beta \rangle$-minimal set U'. By the minimality of $\mathrm{Sg}^{\mathbf{B}}(\{0,1\})$, it follows that $\{p(0), p(1)\}$ is also a generating set for $\mathbf{C}$ and so we may assume that $\{p(0), p(1)\} = \{0,1\}$, i.e., that $\{0,1\}$ is also contained in some $\langle \mu, \nu \rangle$-trace $N \subseteq W$.

Claim 3.7. *There is some element $t' \in B$ with $(t, t') \in \beta$ and with*

$$(1, t') \in \mathrm{Sg}^{\mathbf{B^2}}(\{(1,1), (0,1), (0,t')\}) \quad \textit{and}$$
$$(0, t') \in \mathrm{Sg}^{\mathbf{B^2}}(\{(1,1), (0,1), (1,t')\}).$$

We first consider the case when the type of $\langle \mu, \nu \rangle$ is **3** or **4**. Then $\{0,1\}$ is a $\langle \mu, \nu \rangle$-minimal set of $\mathbf{C}$ and so there are polynomials $j(x,y)$ and $m(x,y)$ of $\mathbf{C}$ that act as a lattice join and meet operations on $\{0,1\}$. Since $\mathbf{C}$ is generated by $\{0,1\}$, there are terms q and r such that $j(x,y) = q(x,y,0,1)$ and $m(x,y) = r(x,y,0,1)$. Since these can be viewed as polynomials on $\mathbf{B}$ it follows that β is not abelian over α and so the type of $\langle \alpha, \beta \rangle$ must also be **3** or **4**.

Lemma 4.17 of [11] shows that a minimal set of type **3** or **4** has a pseudo-meet and pseudo-join operation. (Pseudo-meet and join operations are define in Definition 4.16 of [11].) The proof of Lemma 4.15 shows that the pseudo-meet operation can be constructed starting with any polynomial that acts as a meet on $\{0,1\}$. Hence there are terms $q'(x,y,u,v)$ and $r'(x,y,u,v)$ such that $j'(x,y) = q'(x,y,0,1)$ and $m'(x,y) = r'(x,y,0,1)$ act as pseudo-join and pseudo-meet operations on U. We may choose the terms $q'(x,y,u,v)$ and $r'(x,y,u,v)$ so that both are idempotent in the variable x.

We define a sequence of elements and subuniverses as follows:

$$t_0 = t$$
$$t_{i+1} = \begin{cases} q'(t_i,1,1,1) & \text{if } i \text{ is even} \\ r'(t_i,1,1,1) & \text{if } i \text{ is odd} \end{cases}$$
$$S_i = \begin{cases} \mathrm{Sg}^{\mathbf{B^2}}(\{(0,1),(1,1),(0,t_i)\}) & \text{if } i \text{ is even} \\ \mathrm{Sg}^{\mathbf{B^2}}(\{(0,1),(1,1),(1,t_i)\}) & \text{if } i \text{ is odd} \end{cases}$$

Since $q'(x,1,1,1)\ \beta\ q'(x,0,0,1) = x$ and $r'(x,1,1,1)\ \beta\ r'(x,1,0,1)$ for all $x \in U$ it follows that $(t_i, t) \in \beta$ for all $i \geq 0$. For i even, we have that

$$(0, t_{i+1}) = q'((0,t_i),(0,1),(0,1),(1,1)) \text{ and}$$
$$(1, t_{i+1}) = q'((0,t_{i+1}),(1,1),(0,1),(1,1))$$

and so $S_{i+1} \subseteq S_i$ and $(0, t_{i+1}) \in S_i$. Similarly, for i odd, $S_{i+1} \subseteq S_i$ and $(1, t_{i+1}) \in S_i$. Since B is finite, it follows that $S_i = S_{i+1}$ for some $i > 0$ and from this we conclude that $(1, t_{i+1}) \in \mathrm{Sg}^{\mathbf{B^2}}(\{(1,1),(0,1),(0,t_{i+1})\})$ and $(0, t_{i+1}) \in \mathrm{Sg}^{\mathbf{B^2}}(\{(1,1),(0,1),(1,t_{i+1})\})$.

If the type of $\langle \mu, \nu \rangle$ is **2** then there is some polynomial $d(x, y, z)$ of $\mathbf{C}$ under which the minimal set W is closed and whose restriction to W is Maltsev. Since $\mathbf{C}$ is generated by $\{0, 1\}$, there is some term $s(x, y, z, u, v)$ such that $d(x, y, z) = s(x, y, z, 0, 1)$ for all x, y, z in C. Choose some $k > 0$ such that the term $s_x^{(k)}(x, y, z, u, v)$ is idempotent in the variable x for all algebras in $\mathcal{V}$ and let

$$r(x, y, y', z, u, v) = s_x^{(k-1)}(s(x, y, z, u, v), y', z, u, v).$$

Note that, if $f(x, y, z) = d(d(x, y, z), y, z)$, then $f(x, y, y) = x$ holds on W. Thus $r(0, 1, 1, 1, 0, 1) = 0$ and $r(1, 1, 1, 1, 0, 1) = 1$ and so the idempotent polynomial $r(x, 1, 1, 1, 0, 1)$ of $\mathbf{B}$ maps U onto some other $\langle \alpha, \beta \rangle$-minimal set U' that contains 0 and 1. Without loss of generality, we may assume that $U = U'$ and so $r(t, 1, 1, 1, 0, 1) = t$.

The element $t' = r(t, 1, 1, 1, 1, 1)$ of B is β-related to t and has the property that $r(t', 1, 1, 1, 1, 1) = t'$ since $r(x, 1, 1, 1, 1, 1)$ is an idempotent polynomial. Also,

$$r(0, 0, 1, 1, 0, 1) = s_x^{(k-1)}(s(0, 0, 1, 0, 1), 1, 1, 0, 1) = s_x^{(k-1)}(1, 1, 1, 0, 1) = 1$$

and so we have that

$$(1, t') = r((0, t'), (0, 1), (1, 1), (1, 1), (0, 1), (1, 1)).$$

This establishes that $(1, t')$ is in the subalgebra of $\mathbf{B}^2$ generated by $\{(1, 1), (0, 1), (0, t')\}$. A similar argument shows $r(1, 1, 0, 0, 0, 1) = 0$ and hence

$$(0, t') = r((1, t'), (1, 1), (0, 1), (0, 1), (0, 1), (1, 1)),$$

which finishes the proof of the claim.

We now follow the proof of Theorem 2.4 found in [16] up until Claim 2.6. We define $\mathbf{S}$ to be the subalgebra of $\mathbf{B}^2$ generated by the diagonal of B and the set $\{(0, 1), (0, t')\}$ and $\mathbf{D}$ to be the subalgebra of $\mathbf{S}$ generated by $\{(1, 1), (0, 1), (0, t')\}$. By the previous claim, we know that $(1, t') \in D$. Define γ to be the restriction of the congruence $0_B \times 1_B$ to S, δ to be the congruence of $\mathbf{S}$ generated by $\langle (0, t'), (1, t') \rangle$ and θ to be the join of δ with the congruence of $\mathbf{S}$ generated by $\langle (0, 1), (1, 1) \rangle$. A modest modification of the proof of their Claim 2.5 can be made to show that in $\mathbf{S}$, the congruences $\{\gamma, \delta, \theta\}$ are part of a pentagon in $\mathbf{Con}(\mathbf{S})$. In applying Lemma 2.2 of [16], a crucial fact is that $(t, t') \in \beta$.

The fact that $\{\gamma, \delta, \theta\}$ are part of a pentagon in $\mathbf{Con}(\mathbf{S})$ implies that $((1,1),(0,1),(0,t'),(1,t'))$ form a Day quadruple, which by the claim satisfies the conditions of the theorem. □

The two-element set and the two-element semilattice show the hypotheses in the last two conditions are necessary.

Corollary 3.8. *Let* $\mathbf{A}$ *be a finite idempotent algebra that generates a variety* $\mathcal{V}$ *that omits type* **1**. *Then* $\mathcal{V}$ *is congruence modular if and only if every 3-generated subalgebra of* $\mathbf{A}^2$ *is congruence modular.*

Combining this theorem and corollary with the following proposition leads to various characterizations of finite idempotent algebras that generate congruence modular varieties.

Proposition 3.9. *Let* $\mathcal{V}$ *be the variety generated by a finite idempotent algebra* $\mathbf{A}$. *If one of the following conditions holds then* $\mathrm{typ}(\mathcal{V})$ *is contained in* $\{\mathbf{2},\mathbf{3},\mathbf{4}\}$ *(*$\{\mathbf{3},\mathbf{4}\}$*):*

1. *Every 2-generated subalgebra of* $\mathbf{A}$ *omits types* **1** *and* **5** *(and* **2***).*
2. *The congruence lattice of the square of every 2-generated subalgebra of* $\mathbf{A}$ *is modular (distributive).*
3. *The congruence lattice of every 4-generated (3-generated) subalgebra of* $\mathbf{A}^2$ *is modular (distributive).*
4. *The prime quotients of every 3-generated subalgebra of* $\mathbf{A}^2$ *have minimal sets with empty tails.*
5. *The prime quotients of the square of every 2-generated subalgebra of* $\mathbf{A}$ *have minimal sets with empty tails.*

Proof. By Proposition 2.1, if $\mathcal{V}$ admits type **1** or **5** (or **2**) then there is a strictly simple algebra $\mathbf{B}$ in $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ that is of one of these types. Since $\mathbf{B}$ is 2-generated, the implication involving condition (1) holds.

If $\mathbf{B}$ is of type **1** or **5** then it is term equivalent to a 2-element set or a 2-element semilattice and so the 4 element algebra $\mathbf{B}^2$ fails to be congruence modular and it has prime quotients whose minimal sets have non-empty tails. In fact, some 3-generated subalgebra of $\mathbf{B}^2$ has minimal sets with non-empty tails and has a non-distributive, non-permutable congruence lattice. If $\mathbf{B}$ is of type **2** then it is term equivalent to the idempotent reduct of a module over some finite ring. In this case, $\mathbf{B}^2$ has a 3-generated subalgebra that fails to be congruence distributive. From this, the remaining implications follow. □

Corollary 3.10. *Let* $\mathbf{A}$ *be a finite idempotent algebra and* $\mathcal{V}$ *the variety generated by* $\mathbf{A}$. *Then* $\mathcal{V}$ *is congruence modular if and only if:*

1. *The minimal sets of the prime quotients of all 3-generated subalgebras of* $\mathbf{A}^2$ *have empty tails, or*

(2) *Every 4-generated subalgebra of* $\mathbf{A}^2$ *is congruence modular.*

$\mathcal{V}$ *is congruence distributive if and only if every 3-generated subalgebra of* $\mathbf{A}^2$ *is congruence distributive.*

Proof. If $\mathcal{V}$ is congruence modular (distributive) then the listed conditions must hold. Conversely, if the minimal sets of the prime quotients of all 3-generated subalgebras of $\mathbf{A}^2$ have empty tails then by the previous proposition we know that $\mathcal{V}$ omits types **1** and **5**. Then, by Theorem 3.4 we conclude that $\mathcal{V}$ has no tails and so is congruence modular.

If every 4-generated (3-generated) subalgebra of $\mathbf{A}^2$ is congruence modular (distributive) then by the previous proposition, $\mathcal{V}$ omits types **1** and **5** (and **2**). Then by Corollary 3.8 it follows that $\mathcal{V}$ is congruence modular (distributive). □

4. Semidistributivity

For a, b and c in an algebra $\mathbf{A}$ let

$$\alpha = \mathrm{Cg}^{\mathbf{A}}(b, c)$$
$$\beta = \mathrm{Cg}^{\mathbf{A}}(a, c)$$
$$\gamma = \mathrm{Cg}^{\mathbf{A}}(a, b).$$

If $\mathbf{Con}(\mathbf{A})$ is modular then the subalgebra generated by these elements is a homomorphic image of the lattice in Figure 3.

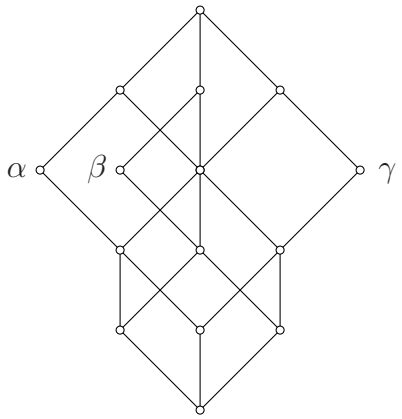

Figure 3. Jónsson's Extended Diamond

Of course, for the variety to be distributive, the copy of $\mathbf{M}_3$ at the top of the lattice must collapse. This will happen if either of the following

conditions hold:

$$(a,c) \in [\mathrm{Cg}^{\mathbf{A}}(a,c) \wedge \mathrm{Cg}^{\mathbf{A}}(b,c)] \vee [\mathrm{Cg}^{\mathbf{A}}(a,c) \wedge \mathrm{Cg}^{\mathbf{A}}(a,b)] \tag{4.1}$$

$$(a,b) \in \mathrm{Cg}^{\mathbf{A}}(b,c) \vee [\mathrm{Cg}^{\mathbf{A}}(a,c) \wedge \mathrm{Cg}^{\mathbf{A}}(a,b)] \tag{4.2}$$

Under congruence modularity these conditions are the same, but, if we do not assume modularity they are not. The first is the basis of Jónsson's Maltsev condition for congruence distributivity given in (7.1): a variety $\mathcal{V}$ is congruence distributive if and only if the first condition holds for $\mathbf{F}_{\mathcal{V}}(a,b,c)$. On the other hand, the second condition holds whenever $\mathbf{Con}(\mathbf{A})$ is join semidistributive since $\mathrm{Cg}^{\mathbf{A}}(b,c) \vee \mathrm{Cg}^{\mathbf{A}}(a,c) = \mathrm{Cg}^{\mathbf{A}}(b,c) \vee \mathrm{Cg}^{\mathbf{A}}(a,b) = \mathrm{Cg}^{\mathbf{A}}(a,b,c)$. In fact K. Kearnes and E. Kiss have shown in [15] that a variety $\mathcal{V}$ is congruence semidistributive if and only if the second equation holds for $\mathbf{F}_{\mathcal{V}}(a,b,c)$. The corresponding Maltsev condition for semidistributivity, from Hobby and McKenzie [11], is similar to Jónsson's except the second equation, $d_i(x,y,x) \approx x$ for all i, is replaced with $d_i(x,y,x) \approx d_{i+1}(x,y,x)$ for all even i.

For idempotent algebras with have the following easy analog to Theorem 3.6.

Theorem 4.1. *Let $\mathbf{A}$ be a finite idempotent algebra and $\mathcal{V}$ be the variety it generates. The following are equivalent.*

1. *$\mathcal{V}$ is congruence semidistributive.*
2. *$\mathcal{V}$ omits types $\mathbf{1}$, $\mathbf{2}$ and $\mathbf{5}$.*
3. *for all x and y in $\mathbf{A}$, if $a = (x,x)$, $b = (x,y)$ and $c = (y,x)$, then in the subalgebra $\mathbf{B}$ of $\mathbf{A}^2$ generated a, b and c*

$$(a,b) \in \mathrm{Cg}^{\mathbf{B}}(b,c) \vee [\mathrm{Cg}^{\mathbf{B}}(a,c) \wedge \mathrm{Cg}^{\mathbf{B}}(a,b)]$$

Proof. Combining results from [11] and [15], conditions (1) and (2) can be shown to be equivalent. As pointed out above condition (3) holds in a semidistributive variety so (1) implies (3).

If one of these types $\mathbf{1}$, $\mathbf{2}$ or $\mathbf{5}$ occurs in $\mathrm{typ}(\boldsymbol{V}(\mathbf{A}))$ then, by Proposition 2.1, $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ contains a strictly simple algebra $\mathbf{B}$ which is term equivalent to a 2-element set, a 2-element semilattice or the idempotent reduct of a module over some finite ring. It is elementary to show that in all cases, (3) fails. So (3) implies (2). □

In Corollary 5.6 of [17], Kearnes and Szendrei show that a locally finite variety $\mathcal{V}$ omits types $\mathbf{1}$ and $\mathbf{2}$ if and only if it satisfies the congruence inclusion

$$\alpha \wedge (\beta \circ \gamma) \subseteq \beta \vee (\alpha \wedge (\gamma \vee (\alpha \wedge \beta)))$$

and, by Theorem 9.10 of [11], this is equivalent to the members of $\mathcal{V}$ having meet semidistributive congruence lattices. From this we get the following theorem.

Theorem 4.2. *Let $\mathbf{A}$ be a finite idempotent algebra and $\mathcal{V}$ be the variety it generates. Then the following are equivalent.*

1. *$\mathcal{V}$ is congruence meet semidistributive.*
2. *$\mathcal{V}$ omits types $\mathbf{1}$ and $\mathbf{2}$.*
3. *for all x and y in $\mathbf{A}$, if $a = (x, x)$, $b = (x, y)$ and $c = (y, x)$, then in the subalgebra $\mathbf{B}$ of $\mathbf{A}^2$ generated a, b and c*
$$(a, c) \in \beta \vee (\alpha \wedge (\gamma \vee (\alpha \wedge \beta))),$$
where $\alpha = \mathrm{Cg}^{\mathbf{B}}(a, c)$, $\beta = \mathrm{Cg}^{\mathbf{B}}(a, b)$, and $\gamma = \mathrm{Cg}^{\mathbf{B}}(b, c)$.

Proof. Conditions (1) and (2) are shown to be equivalent in locally finite varieties in Theorem 9.10 of [11].

By the remarks above (1) implies (3).

If $\mathcal{V}$ admits type $\mathbf{1}$ or $\mathbf{2}$, then, by Proposition 2.1, $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ contains a strictly simple algebra $\mathbf{B}$ which is term equivalent to a 2-element set or the idempotent reduct of a module over some finite ring. It is elementary to show that in both cases, condition (3) fails. Thus (3) implies (2). □

5. Maltsev and Majority terms

We now turn our attention to more specialized Maltsev conditions, ones that are determined by the existence of special idempotent ternary terms. It is well known that a variety $\mathcal{V}$ is congruence permutable if and only if $\mathcal{V}$ has a term $p(x, y, z)$ that satisfies the equations: $p(x, x, y) \approx y$ and $p(y, x, x) \approx y$. The following theorem provides a local characterization of congruence permutable finitely generated idempotent varieties.

Theorem 5.1. *Let $\mathbf{A}$ be a finite idempotent algebra. Then $\mathbf{A}$ generates a congruence permutable variety $\mathcal{V}$ if and only if for every x_0, x_1, y_0, y_1 in A,*

$$(c, a) \in \mathrm{Cg}^{\mathbf{B}}(a, b) \circ \mathrm{Cg}^{\mathbf{B}}(b, c) \tag{5.1}$$

where $a = (x_0, y_0)$, $b = (x_0, y_1)$, $c = (x_1, y_1)$ and $\mathbf{B} = \mathrm{Sg}^{\mathbf{A^2}}(\{a, b, c\})$.

Proof. We claim that if the stated condition holds then $\mathbf{A}^2$ has no Day quadruple as described in Theorem 3.6 and so $\mathbf{A}$ generates a congruence modular variety. To see this, consider the pairs $a = (x_0, x_1)$, $b = (x_0, y_1)$, $c = (y_0, x_1)$, and $d = (y_0, y_1)$ for some x_0, x_1, y_0, y_1 from A. In the subalgebra $\mathbf{B}$ of $\mathbf{A}^2$ generated by $\{b, c, d\}$ we have, by (5.1), that $(b, c) \in \mathrm{Cg}^{\mathbf{B}}(c, d) \circ \mathrm{Cg}^{\mathbf{B}}(d, b)$. So there is some element $e = (u, v) \in B$

with $(b, e) \in \mathrm{Cg}^{\mathbf{B}}(c, d)$ and $(e, c) \in \mathrm{Cg}^{\mathbf{B}}(d, b)$. This forces $u = x_0$ and $v = x_1$ and so we conclude that $e = a$ and thus $(a, b) \in \mathrm{Cg}^{\mathbf{B}}(c, d)$. Therefore (a, b, c, d) is not a Day quadruple.

If $\boldsymbol{V}(\mathbf{A})$ is not congruence permutable then let $\mathbf{B}$ be a member of smallest size that is not congruence permutable. By a result of Idziak (see Theorem 3.2 in [28]), it follows that we can find congruences γ, α and β of $\mathbf{B}$ such that $\gamma \prec \alpha$, $\gamma \prec \beta$ and α and β fail to permute. By the minimality of $|B|$, we have that $\gamma = 0_B$ and so $\mathbf{B}$ is isomorphic to a subdirect product of the algebras $\mathbf{B}/\alpha$ and $\mathbf{B}/\beta$. Since $\mathcal{V}$ is congruence modular then we may use results from commutator theory as well as tame congruence theory to conclude that the types of $\langle 0_B, \alpha\rangle$ and $\langle 0_B, \beta\rangle$ are **3** or **4** (in fact we can easily rule out type **4**) for if either α or β is of type **2** (and hence solvable) then these two congruences permute (see Theorem 6.2 of [7]).

Choose a, $c \in B$ with $(a, c) \in \alpha \circ \beta$ and $(c, a) \notin \alpha \circ \beta$ and let $b \in B$ with $(a, b) \in \alpha$ and $(b, c) \in \beta$. Let $\mathbf{C}$ be the subalgebra of $\mathbf{B}$ generated by $\{a, b, c\}$ and let $\alpha' = \mathrm{Cg}^{\mathbf{C}}(a, b)$ and $\beta' = \mathrm{Cg}^{\mathbf{C}}(b, c)$. It follows that in $\mathbf{C}$, the congruences α' and β' fail to permute since $(a, c) \in \alpha' \circ \beta'$ and $(c, a) \notin \alpha' \circ \beta'$. Thus, by the minimality of $|B|$ we conclude that $\mathbf{B} = \mathbf{C}$ and so is generated by $\{a, b, c\}$.

Let D be the $(\alpha \vee \beta)$-class that contains a. Then since $\mathbf{B}$ is idempotent, D is a subuniverse of $\mathbf{B}$ that contains $\{a, b, c\}$ and so, by the previous paragraph is equal to B. Thus, $\alpha \vee \beta = 1_B$ and so by the modularity of $\mathbf{Con}(\mathbf{B})$ it follows that $\alpha \prec 1_B$ and $\beta \prec 1_B$. But then $\mathbf{B}/\alpha$ and $\mathbf{B}/\beta$ are both simple, non-abelian algebras (since $\mathrm{typ}(\alpha, 1_B) = \mathrm{typ}(0_B, \beta)$, $\mathrm{typ}(\beta, 1_B) = \mathrm{typ}(0_B, \alpha) \in \{\mathbf{3}, \mathbf{4}\}$) and so, by Theorem 10.1 of [7] (or Theorem 14.5 of [11]), belong to $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$. We conclude that $\mathbf{B}$ belongs to $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A}^2)$ since it is a subdirect product of these two simple algebras. By pulling back a, b and c into $\mathbf{A}^2$ we end up with elements x_0, x_1, y_0, and y_1 for which (5.1) fails. □

Corollary 5.2. *A finite idempotent algebra generates a congruence permutable variety if and only if each 3-generated subalgebra of* $\mathbf{A}^2$ *is congruence permutable.*

The ternary term $m(x, y, z)$ of an algebra $\mathbf{A}$ is a majority term for $\mathbf{A}$ if it satisfies the identities: $m(x, x, y) \approx m(x, y, x) \approx m(y, x, x) \approx x$. Under the assumption that $\mathbf{A}$ is finite and idempotent, we will show that the presence of a majority term can be efficiently determined by ruling out a certain configuration amongst the 3-generated subalgebras of $\mathbf{A}^3$.

Definition 5.3. We will call a triple $\langle a, b, c\rangle$ of elements from an algebra $\mathbf{A}$, a majority triple of $\mathbf{A}$ if, with $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b, c\})$, there is some element $d \in B$ such that

$$(a, d) \in (\mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)) \text{ and } (d, c) \in (\mathrm{Cg}^{\mathbf{B}}(b, c) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)).$$

In this case, we say that the element d resolves the triple $\langle a, b, c\rangle$. If there is no element that resolves the triple, then we say that it is a non-majority triple of $\mathbf{A}$.

Proposition 5.4. *If $m(x, y, z)$ is a majority term of an algebra $\mathbf{A}$ then for every $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$ and all a, b, $c \in B$, $\langle a, b, c\rangle$ is a majority triple of $\mathbf{B}$ and is resolved by the element $m^{\mathbf{B}}(a, b, c)$. Conversely, if $\langle \mathbf{x}, \mathbf{y}, \mathbf{z}\rangle$ is a majority triple in the free algebra of $\boldsymbol{V}(\mathbf{A})$ generated by $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ then $\mathbf{A}$ has a majority term.*

Proof. Suppose that $m(x, y, z)$ is a majority term of $\mathbf{A}$ and $\mathbf{B} \in \boldsymbol{V}(\mathbf{A})$. It is elementary to verify that if a, b, $c \in B$ then the element $m^{\mathbf{B}}(a, b, c)$ resolves the triple $\langle a, b, c\rangle$.

Conversely, let $\mathbf{F}$ be the free algebra in $\boldsymbol{V}(\mathbf{A})$ generated by $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ and suppose that the element d of F resolves the majority triple $\langle \mathbf{x}, \mathbf{y}, \mathbf{z}\rangle$. Then d is of the form $m^{\mathbf{F}}(\mathbf{x}, \mathbf{y}, \mathbf{z})$ for some term $m(x, y, z)$ of $\mathbf{A}$. It is straightforward to verify that m must be a majority term for $\mathbf{A}$. □

Lemma 5.5. *Let $\vec{t} = \langle a, b, c\rangle$ be a majority triple in the algebra $\mathbf{A}$ that is resolved by the element d. Then all triples of $\mathbf{A}$ obtained by permuting the elements of $\vec{t}$ are majority and are resolved by d.*

Proof. Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{B}}(\{a, b, c\})$. Since d resolves $\langle a, b, c\rangle$ then $d \in B$ and $(a, d) \in \mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)$ and $(d, c) \in \mathrm{Cg}^{\mathbf{B}}(b, c) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)$. So, in order to show that d resolves $\langle b, a, c\rangle$ we need to show that $(b, d) \in \mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(b, c)$. Since (b, a) and $(a, d) \in \mathrm{Cg}^{\mathbf{B}}(a, b)$ then by transitivity we get that $(b, d) \in \mathrm{Cg}^{\mathbf{B}}(a, b)$. Similarly, (b, c) and $(c, d) \in \mathrm{Cg}^{\mathbf{B}}(b, c)$ implies that $(b, d) \in \mathrm{Cg}^{\mathbf{B}}(b, c)$, as required. By symmetry, the other 4 triples obtained from $\vec{t}$ are also majority and resolved by d. □

Theorem 5.6. *Let $\mathbf{A}$ be a finite idempotent algebra that generates a congruence distributive variety. Then, $\mathbf{A}$ has a majority term if and only if every triple $\langle a, b, c\rangle$ of elements from A^3 is a majority triple.*

Proof. One direction of this theorem follows from Proposition 5.4. For the other, let $\mathcal{V} = \boldsymbol{V}(\mathbf{A})$ and suppose that $\mathbf{A}$ does not have a majority term. Then by Proposition 5.4 there is some finite algebra $\mathbf{B} \in \mathcal{V}$ and elements a, b, $c \in B$ such that $\langle a, b, c\rangle$ is a non-majority

triple of $\mathbf{B}$. Without loss of generality, we may assume that $\mathbf{B}$ is generated by $\{a, b, c\}$. Choose $\mathbf{B}$ and the non-majority triple $\langle a, b, c\rangle$ so that the size of B is as small as possible in $\mathcal{V}$ and the congruence $\mathrm{Cg}^{\mathbf{B}}(\{a, b, c\})$ is as small as possible in $\mathbf{Con}(\mathbf{B})$. It follows that $\mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c) \wedge \mathrm{Cg}^{\mathbf{B}}(b, c) = 0_B$ and that $\mathrm{Cg}^{\mathbf{B}}(\{a, b, c\}) = 1_B$. This last claim makes use of the idempotency of $\mathbf{B}$ (and is the only point in the proof where idempotency is used). We can also conclude that $\mathbf{B}$ is isomorphic to a 3-generated subdirect product of the algebras $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(a, b)$, $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(a, c)$ and $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(b, c)$.

If we can show that $\mathrm{Cg}^{\mathbf{B}}(a, c) \prec 1_B$ then by the symmetry of the set up, it will follow that $\mathrm{Cg}^{\mathbf{B}}(a, b)$ and $\mathrm{Cg}^{\mathbf{B}}(b, c)$ are also subcovers of 1_B. We can then conclude that $\mathbf{B}$ is a subdirect product of three simple algebras: $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(a, c)$, $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(a, b)$, and $\mathbf{B}/\mathrm{Cg}^{\mathbf{B}}(b, c)$. By Jónsson's Theorem (see Corollary 6.10 of [2]) we have that these algebras belong to $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ and from this, it follows that there is a 3-generated subalgebra of $\mathbf{A}^3$ whose generators form a non-majority triple.

Using the congruence distributivity of $\mathbf{B}$ it follows that the 3 congruences $\mathrm{Cg}^{\mathbf{B}}(a, b)$, $\mathrm{Cg}^{\mathbf{B}}(a, c)$, and $\mathrm{Cg}^{\mathbf{B}}(b, c)$ generate a sublattice of $\mathbf{Con}(\mathbf{B})$ that is isomorphic to the 8 element boolean lattice. If these congruences were to generate a smaller sublattice then it is not hard to show that $\langle a, b, c\rangle$ must be a majority triple.

If $\mathrm{Cg}^{\mathbf{B}}(a, c)$ is not a subcover of 1_B then there is a congruence ϵ of $\mathbf{B}$ with $0_B \prec \epsilon < \mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(b, c)$. By the minimality of $|B|$ it follows that in the algebra $\mathbf{C} = \mathbf{B}/\epsilon$, $\langle \bar{a}, \bar{b}, \bar{c}\rangle$ is a majority triple and so is resolved by $\bar{d}$ for some $d \in B$ (for $x \in B$, $\bar{x}$ denotes the element x/ϵ of C).

Let $\mu = \mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)$ and $\nu = \mathrm{Cg}^{\mathbf{B}}(b, c) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c)$ and let $\bar{\mu} = \mu/\epsilon$ and $\bar{\nu} = \nu/\epsilon$ in $\mathrm{Con}(\mathbf{C})$. Since $\bar{d}$ resolves $\langle \bar{a}, \bar{b}, \bar{c}\rangle$ in $\mathbf{C}$ then $(\bar{a}, \bar{d}) \in \bar{\mu}$ and $(\bar{d}, \bar{c}) \in \bar{\nu}$. Pulling this back up to $\mathbf{B}$ we get that $(a, d) \in \mu \vee \epsilon$ and $(d, c) \in \nu \vee \epsilon$.

Consider the triple $\langle a, d, c\rangle$ of $\mathbf{B}$. Since $\mu \vee \nu \vee \epsilon \leq \mathrm{Cg}^{\mathbf{B}}(a, c) \vee \epsilon$ then $\mathrm{Cg}^{\mathbf{B}}(\{a, d, c\}) \leq \mathrm{Cg}^{\mathbf{B}}(a, c) \vee \epsilon < 1_B$. By the minimality of $|B|$ and of $\mathrm{Cg}^{\mathbf{B}}(\{a, b, c\})$ in $\mathbf{Con}(\mathbf{B})$ it follows that $\langle a, d, c\rangle$ is a majority triple of $\mathbf{B}$. Thus, there is some element $e \in B$ so that

$$(a, e) \in \mathrm{Cg}^{\mathbf{B}}(a, d) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c) \text{ and } (e, c) \in \mathrm{Cg}^{\mathbf{B}}(d, c) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c).$$

Since $(a, d) \in \mu \vee \epsilon \leq \mathrm{Cg}^{\mathbf{B}}(a, b)$ then

$$(a, e) \in \mathrm{Cg}^{\mathbf{B}}(a, b) \wedge \mathrm{Cg}^{\mathbf{B}}(a, c) = \mu.$$

Similarly, $(e, c) \in \nu$ and so the element e resolves the triple $\langle a, b, c\rangle$. This contradiction implies that $\mathrm{Cg}^{\mathbf{B}}(a, c) \prec 1_B$ and so we are done. $\square$

The following proposition shows that the hypothesis of congruence distributivity in the previous theorem is not necessary. In fact, the proposition provides another characterization of finite idempotent algebras that generate congruence distributive varieties.

Proposition 5.7. *Let* $\mathbf{A}$ *be a finite idempotent algebra such that*

$$(a,c) \in [\mathrm{Cg}^{\mathbf{E}}(a,b) \wedge \mathrm{Cg}^{\mathbf{E}}(a,c)] \vee [\mathrm{Cg}^{\mathbf{E}}(b,c) \wedge \mathrm{Cg}^{\mathbf{E}}(a,c)], \tag{5.2}$$

where $\mathbf{E} = \mathrm{Sg}^{\mathbf{A^3}}(\{a,b,c\})$*, for all elements* a*,* b*,* c *from* A^3 *of the form*

$$a = (0,1,1),\ b = (3,1,2),\ \text{and}\ c = (0,2,2)$$

for some $\{0,1,2,3\} \subseteq A$*. Then* $\boldsymbol{V}(\mathbf{A})$ *is congruence distributive.*

Proof. If one of the types **1**, **2**, and **5** occurs in $\mathrm{typ}(\boldsymbol{V}(\mathbf{A}))$ then by Proposition 2.1, $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A})$ contains a strictly simple algebra $\mathbf{B}$ that is, term equivalent to a 2-element set, a 2-element semilattice or the idempotent reduct of a module over some finite ring. It is elementary to show that in all cases, the hypotheses of our proposition fail to hold.

To complete the proof it is enough to show that $\boldsymbol{V}(\mathbf{A})$ is congruence modular since a locally finite, modular variety that omits type **2** is congruence distributive. If $\boldsymbol{V}(\mathbf{A})$ is not modular then, by Theorem 3.6, $\mathbf{A}$ has elements 0, 1, 2 and 3 such that if $u = (0,1)$, $v = (0,2)$, $w = (3,1)$ and $w' = (3,2)$ form a Day quadruple in $\mathbf{B} = \mathrm{Sg}^{\mathbf{A^2}}(u,v,w,w')$ and $w' \in \mathrm{Sg}^{\mathbf{A^2}}(u,v,w)$ and $w \in \mathrm{Sg}^{\mathbf{A^2}}(u,v,w')$. Let $\beta = \mathrm{Cg}^{\mathbf{B}}((u,v),(w,w'))$, $\gamma = \mathrm{Cg}^{\mathbf{B}}((u,w),(v,w'))$ and $\alpha = \mathrm{Cg}^{\mathbf{B}}(w,w') \vee (\beta \wedge \gamma)$. Then $(u,v) \notin \alpha$ since (u,v,w,w') is a Day quadruple. Let $a = (0,1,1)$, $b = (3,1,2)$, $c = (0,2,2)$ and $\mathbf{E} = \mathrm{Sg}^{\mathbf{A^3}}(\{a,b,c\})$ and let $\mu = \mathrm{Cg}^{\mathbf{E}}(a,b) \wedge \mathrm{Cg}^{\mathbf{E}}(a,c)$ and $\nu = \mathrm{Cg}^{\mathbf{E}}(b,c) \wedge \mathrm{Cg}^{\mathbf{E}}(a,c)$. The following claim shows that under these circumstances (5.2) fails for the elements a, b, and c.

Claim 5.8. *Let* $(0,0',0'') \in E$ *with* $(0,0')\ \alpha\ (0,0'')$ *in* $\mathbf{B}$*. If* $(r,s,t) \in E$ *with* $(0,0',0'')\ \mu\ (r,s,t)$ *or* $(0,0',0'')\ \nu\ (r,s,t)$ *then* $r = 0$ *and in* $\mathbf{B}$*,* $(0,0')\ \alpha\ (0,s)\ \alpha\ (0,t)$ *.*

Let's assume that $(0,0',0'')\ \mu\ (r,s,t)$. That $r = 0$ and $s = 0'$ follows from the fact that μ is contained in $\rho_1 \cap \rho_2$, where, for $1 \leq i \leq 3$, ρ_i is the kernel of the projection map of E onto its ith coordinate. Since $(0,0',t) \in E$ then there is some term $p(x,y,z)$ such that $p(b,a,c) = (0,0',t)$. By projecting this equality onto the first two components we get that $p(w,u,v) = (0,0')$. Projecting on to the first and last components gives $p(w',u,v) = (0,t)$. Thus $(0,0')\ \alpha\ (0,t)$.

The case that $(0,0',0'')\ \nu\ (r,s,t)$ can be handled in a similar fashion. □

Corollary 5.9. *A finite idempotent algebra* $\mathbf{A}$ *has a majority term if and only if for all* $0, 1, 2, 3, 4, 5 \in A$, $\langle (0,1,2),(3,1,4),(0,5,4)\rangle$ *is a majority triple of* $\mathbf{A}^3$.

Proof. As noted in Proposition 5.4, if $\mathbf{A}$ has a majority term then every triple of $\mathbf{A}$ is a majority triple. Conversely, if the stated condition holds, then the hypotheses of the previous proposition hold and so $\boldsymbol{V}(\mathbf{A})$ is congruence distributive. The proof of Theorem 5.6 shows that if $\boldsymbol{V}(\mathbf{A})$ is congruence distributive and fails to have a majority term then one can find a non-majority triple $\langle a, b, c\rangle$ of $\mathbf{A}^3$ such that (a, c) agree in the first coordinate, (a, b) in the second, and (b, c) in the third. The hypothesis of this corollary rules this out and so we conclude that $\mathbf{A}$ has a majority term. □

By examining the idempotent reduct of Polin's Variety (see [5, 13]) it can be seen that in general it is not sufficient to look for non-majority triples in the square of a generating algebra in order to determine if an idempotent variety has a majority term.

6. Polynomial-time Algorithms

The results from the previous sections easily lead to polynomial-time algorithms for testing if $\boldsymbol{V}(\mathbf{A})$ has various properties for a finite, idempotent algebra $\mathbf{A}$. In this section we give outlines of some of these algorithms and analyze their speeds.

If $\mathbf{A}$ is an algebra with underlying set (or universe) A, we let $|\mathbf{A}| = |A|$ be the cardinality of A and $||\mathbf{A}||$ be the *input size*; that is,

$$||\mathbf{A}|| = \sum_{i=0}^{r} k_i n^i$$

where, k_i is the number of basic operations of arity i and r is the largest arity. We let

$$n = |\mathbf{A}| \qquad m = ||\mathbf{A}||$$
$$r = \text{the largest arity of the operations of } \mathbf{A}$$

Of course if we assume the similarity type is fixed, r can be viewed as a constant and the next proposition shows that subalgebras and principal congruences can be computed in linear time. However, we do not make this assumption. Note that as long as $n > 1$, $r \leq \log_2 m$. We do, however, make the assumption that $r \geq 2$. Also note that $||\mathbf{A}^2|| \leq ||\mathbf{A}||^2$. Thus, if we let $m_2 = ||\mathbf{A}^2||$ and $m_3 = ||\mathbf{A}^3||$, we can improve the bounds given in Theorem 6.2 by replacing m^2 by m_2 and m^3 by m_3.

Throughout this section we let c denote a constant independent of these parameters.

Proposition 6.1. *Let* $\mathbf{A}$ *be a finite algebra with the parameters above.*

(1) *If* S *is a subset of* A*, then* $\mathrm{Sg}^{\mathbf{A}}(S)$ *can be computed in time*

$$c\,r\,||\mathrm{Sg}^{\mathbf{A}}(S)|| \leq c\,r\,||\mathbf{A}|| = crm$$

(2) *If* $a,\ b \in A$*, then* $\mathrm{Cg}^{\mathbf{A}}(a,b)$ *can be computed in* $c\,r\,||\mathbf{A}|| = crm$ *time.*

Proof. If f is an k–ary operation, to test if S is already closed under f, involves showing f applied to every k-tuple of elements of S lies in S. This can be done in cks^k time, where $s = |S|$.

Now for an arbitrary subset S, to show that $\mathrm{Sg}^{\mathbf{A}}(S)$ can be computed in the advertised time, we need an algorithm that for each k–ary operation f and each k–tuple only applies f to this k–tuple once. We leave the construction of such an algorithm to the reader.

The second statement is proved in [6]. □

Since the join of two congruences of $\mathbf{A}$ is the same as their join in the lattices of equivalence relations on A, join and meets can be computed in time cn^2 (in fact they can be computer in time $cn\log_2 n$). Now if $\mathbf{A}$ is idempotent we can use Theorem 3.6 to test if $\boldsymbol{V}(\mathbf{A})$ is congruence modular. Namely for each $x_0,\ x_1,\ y_0,\ y_1$ in A we form $a = (x_0, x_1)$, $b = (x_0, y_1)$, $c = (y_0, x_1)$, and $d = (y_0, y_1)$, find the subalgebra of $\mathbf{A}^2$ generated by them, and then test if (3.1) holds. By the proposition and the remarks above, this can be done in time at most a constant times rm^2. Since there are n^4 choices for $x_0,\ x_1,\ y_0,\ y_1$, this algorithm decides if $\boldsymbol{V}(\mathbf{A})$ is congruence modular in time at most a constant times rn^4m^2.

Theorem 6.2. *Let* $\mathbf{A}$ *be a finite idempotent algebra with parameters as above. Then each of the following can be determined in the time indicated:*

$\boldsymbol{V}(\mathbf{A})$ *is congruence modular:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence distributive:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence meet semidistributive:*	crn^2m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence permutable:*	crn^4m^2.
$\boldsymbol{V}(\mathbf{A})$ *is congruence* k*-permutable for some* k*:*	crn^3m.
$\mathbf{A}$ *has a majority term:*	crn^6m^3.

Proof. We've already established the first statement and the third and the fourth can be proved similarly using Theorem 4.1 and Theorem 4.2 or by referring to Theorem 6.3. The second follows from the first and third.

For permutability we can use Theorem 5.1. We test, for every x_0, x_1, y_0, $y_1 \in A$, if $(0,1) \in \mathrm{Cg}^{\mathbf{C}}(c,1) \circ \mathrm{Cg}^{\mathbf{C}}(0,c)$, where $0 = (x_0, x_1)$, $c = (x_0, y_1)$, $1 = (y_0, y_1)$ and $\mathbf{C} = \mathrm{Sg}^{\mathbf{A^2}}(0, c, 1)$. Thus permutability can be tested in time crn^4m^2. Using Corollary 5.9 a similar argument gives the bound for testing for a majority term. Finally, the k-permutability result follows from Theorem 6.3 since this condition is equivalent to omitting the types $\{\mathbf{1}, \mathbf{4}, \mathbf{5}\}$. □

Theorem 6.3. *Let* $\mathbf{A}$ *be a finite idempotent algebra with parameters as above and let* T *be a proper order ideal in the lattice of types. If* $\mathbf{2} \notin T$ *then there is an algorithm to determine if* $\boldsymbol{V}(\mathbf{A})$ *omits* T *with run-time* crn^3m*. If* $\mathbf{2} \in T$ *then there is an algorithm with run-time* crn^2m^2*.*

Proof. We first present the case $T = \{\mathbf{1}, \mathbf{4}, \mathbf{5}\}$. By Proposition 2.1 and Lemma 2.3 we know that $\boldsymbol{V}(\mathbf{A})$ omits T if and only if A does not contain elements a, b such that, if $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(a, b)$, then $1_B = \mathrm{Cg}^{\mathbf{B}}(a, b)$, is join irreducible with unique lower cover ρ with $\mathbf{S} = \mathbf{B}/\rho$ polynomially equivalent to a 2-element set, lattice, or semilattice. Moreover, we may assume that restriction of the natural map of $\mathbf{B}$ onto $\mathbf{B}/\rho$ to any proper subalgebra is not onto.

Thus in order to rule out the types in T we need to determine, for each subset $\{a, b\}$ of A, first whether $1_B = \mathrm{Cg}^{\mathbf{B}}(a, b)$ has a unique lower cover ρ with exactly two classes, where $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(a, b)$. So we compute $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(a, b)$ in time crm and then compute $\mathrm{Cg}^{\mathbf{B}}(a, b)$ also in time crm, by Proposition 6.1. If this is not 1_B we abandon a, b and go to the next pair. So we assume $1_B = \mathrm{Cg}^{\mathbf{B}}(a, b)$.

Assume for a moment that $1_B = \mathrm{Cg}^{\mathbf{B}}(a, b)$ is join irreducible with lower cover ρ, where ρ has exactly two blocks. If $c \in B$ is in the ρ-block of a, then the minimality of $\mathbf{B}$ implies $\mathrm{Sg}^{\mathbf{B}}(b, c)$ is $\mathbf{B}$ and this implies $\mathrm{Cg}^{\mathbf{B}}(b, c) = 1_B$. Thus we can test if 1_B is join irreducible and find its lower cover ρ by forming $\mathrm{Cg}^{\mathbf{B}}(a, c)$ and $\mathrm{Cg}^{\mathbf{B}}(b, c)$ for each $c \in B$. Exactly one of these should be less than 1_B. (If not we abandon this a, b.) If $\mathrm{Cg}^{\mathbf{B}}(a, c) < 1_B$, c is in the ρ-block of a; otherwise of b. This produces a partition of B into two blocks. We can check that this is a congruence in time crm; see [6]. Thus the total time for testing if 1_B is join irreducible and finding ρ is $cnrm$.

At this point $\mathbf{S} = \mathbf{B}/\rho$ is a two element algebra and we take $\{0, 1\}$ as its universe, with $0 = a/\rho$ and $1 = b/\rho$. By Proposition 2.1 the

type of $\mathbf{S}$ will be in $\{\mathbf{1}, \mathbf{4}, \mathbf{5}\}$ if and only if all the operations respect the ordering $0 < 1$. If f is a basic operation of $\mathbf{S}$ with arity j, we can check if it preserves the order by testing if $f(v) \leq f(u)$ for each $v \prec u$ in $\{0,1\}^j$. There are $j2^{j-1}$ covers in the Boolean lattice $\{0,1\}^j$. Since $j \leq r$ and $2^{j-1} \leq n^j$, the total time required to check that the operations respect order is bounded by crm.

Thus the total time for a fixed a, b is bounded by $cnrm$, and thus the total time is bounded by crn^3m.

For the cases $T = \{\mathbf{1}\}$ and $T = \{\mathbf{1}, \mathbf{5}\}$, first note that during the test to see if f respects order, we can also find which coordinates f depends on. Namely, if $v \prec u$ then they agree in all but one coordinate and if $f(v) \neq f(u)$ then f depends on that coordinate and the loop described above can be modified to find all such dependencies. $\mathbf{S}$ is of type $\mathbf{1}$ if each operation depends on one variable. Assuming the type is not $\mathbf{1}$, it will be type $\mathbf{5}$ if either 0 or 1 is an absorbing element. To test the former, we test if $f(1, \dots, 1, 0, 1, \dots, 1) = 0$, where 0 is in the i^{th} position, for all i such that f depends on i. Using these modifications to the algorithm, we can test if $\boldsymbol{V}(\mathbf{A})$ omits $T = \{\mathbf{1}\}$ or $T = \{\mathbf{1}, \mathbf{5}\}$ in time bounded by crn^3m.

To determine if $\boldsymbol{V}(\mathbf{A})$ omits an order ideal T that contains $\mathbf{2}$ we first determine if $\boldsymbol{V}(\mathbf{A})$ omits $T \setminus \{\mathbf{2}\}$. If it does, then we use Theorem 4.2 to test if it also omits type $\mathbf{2}$. The first part can be done in time bounded by crn^3m and the second by crn^2m^2. Since $m \geq n$, the time is bounded by the later. □

7. Jónsson Terms

By Jónsson's famous result [12], a variety $\mathcal{V}$ has distributive congruence lattices (is *congruence distributive*, for short) if and only if there are 3-ary terms $d_0, \dots, d_k$ (called *Jónsson terms*) such that

$$
\begin{aligned}
& d_0(x,y,z) \approx x && \\
& d_i(x,y,x) \approx x && \text{for } 0 \leq i \leq k \\
& d_i(x,x,y) \approx d_{i+1}(x,x,y) && \text{for all even } i < k \\
& d_i(x,y,y) \approx d_{i+1}(x,y,y) && \text{for all odd } i < k \\
& d_k(x,y,z) \approx z. &&
\end{aligned} \tag{7.1}
$$

Let $\mathrm{CD}(k)$ be the class of all varieties having terms that satisfy (7.1). Clearly $\mathrm{CD}(k-1) \subseteq \mathrm{CD}(k)$. If a variety $\mathcal{V}$ is in $\mathrm{CD}(k)$ but not in $\mathrm{CD}(k-1)$, we say $\mathcal{V}$ has *Jónsson level* k. The Jónsson level of a single algebra $\mathbf{A}$ is the level of $\boldsymbol{V}(\mathbf{A})$.

In this section we present a straightforward method to calculate the Jónsson level of a finite algebra $\mathbf{A}$ and find the corresponding Jónsson terms. This is an exponential time algorithm, but, as we will show in Corollary 9.3, there is no way to avoid this. A consequence of this method is that the Jónsson level of a variety $\mathcal{V}$ is at most $2m-2$, where $m = |\mathbf{F}_{\mathcal{V}}(x, y)|$. Moreover, we will give an example where this bound is achieved.

We also present similar results for Gumm terms for modularity and Hagemann-Mitschke terms for k-permutability.

The ALVIN variant. In [22], a slight variant of Jónsson's condition for distributivity is used. Namely in (7.1), "even" and "odd" are interchanged. While both conditions define congruence distributivity, they are not quite the same. Let $\mathrm{CD}'(k)$ be the class of all varieties that satisfy (7.1) with "even" and "odd" interchanged. We say a variety has *alvin level* k if it is in $\mathrm{CD}'(k)$ but not in $\mathrm{CD}'(k-1)$. The *distributivity level* of a variety is the minimum of its Jónsson level and its alvin level. It is easy to see that $\mathrm{CD}(k) \subseteq \mathrm{CD}'(k+1)$ and $\mathrm{CD}'(k) \subseteq \mathrm{CD}(k+1)$ so these notions differ by at most 1. In addition we have the following.

Proposition 7.1. *With* $\mathrm{CD}(k)$ *and* $\mathrm{CD}'(k)$ *defined as above, we have*

(1) $\mathrm{CD}(k) = \mathrm{CD}'(k)$ *when* k *is odd.*
(2) $\mathcal{V} \in \mathrm{CD}(2)$ *if and only if it has a majority term.*
(3) $\mathcal{V} \in \mathrm{CD}'(2)$ *if and only if it has a Pixley term.*
(4) $\mathrm{CD}'(2) \subsetneq \mathrm{CD}(2)$.
(5) $\mathrm{CD}'(2k) \nsubseteq \mathrm{CD}(2k)$ *and* $\mathrm{CD}'(2k) \nsubseteq \mathrm{CD}(2k)$ *for* $k > 1$.

Proof. One can check that letting $d'_i(x, y, z) = d_{k-i}(z, y, x)$ gives terms of the other type when k is odd. A Pixley term $p(x, y, z)$ is defined by the equations $p(x, x, y) \approx p(y, x, x) \approx y$ and $p(x, y, x) \approx x$. For such a term, $m(x, y, z) = p(x, p(x, y, z), z)$ is a majority term. Lattices are a variety with a majority term but without a Pixley term. A method to construct examples proving the last statement is given in Section 8. □

Let $\mathbf{F}_2 = \mathbf{F}_{\mathcal{V}}(x, y)$ be the free algebra with generators x and y over a variety $\mathcal{V}$. The variable patterns that occur in (7.1) are (x, x, y), (x, y, x) and (x, y, y). (The pattern (x, y, z) occurs in the first and last equation, but the first equation can be replace by the equations $d_0(x, x, y) \approx x$ and $d_0(x, y, y) \approx x$ and the resulting condition is equivalent; so (7.1) may be viewed as a system of equations in two variables.) It is convenient to interchange x and y in the last equation and consider the subuniverse, S, of $\mathbf{F}_2^3$ generated by the transpose of the three

patterns; that is, by (x,x,y), (x,y,x) and (y,x,x). A typical element of S looks like

$$f((x,x,y),(x,y,x),(y,x,x)) = (f(x,x,y), f(x,y,x), f(y,x,x)), \tag{7.2}$$

where f is a 3-variable term. Let T be the subset of S consisting of those triples whose middle coordinate is x. Let ρ_i, $i = 1, 2, 3$, be the kernel of the i^{th} coordinate projection and define ρ on T by $\rho = \rho_1 \cup \rho_3$ so that $(a,x,c)\ \rho\ (a',x,c')$ if $a = a'$ or $c = c'$. Using $f = d_i$ and $f = d_{i+1}$ in the above equation, we get the triples

$$(d_i(x,x,y), d_i(x,y,x), d_i(y,x,x))$$
$$(d_{i+1}(x,x,y), d_{i+1}(x,y,x), d_{i+1}(y,x,x))$$

which by (7.1) are in T and ρ-related. Thus the d_i's witness a ρ-path of length k in T starting at (x,x,y) and ending at (y,x,x). Conversely, if we have such a ρ-path in T, then the terms that give the corresponding elements (as elements of S) are easily seen to be Jónsson terms or the alvin variant of Jónsson terms, depending on whether the first link in the path is ρ_1 or ρ_3.

Theorem 7.2. *Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x,y)$ generated by (x,x,y), (x,y,x) and (y,x,x). Let T be the subset of S consisting of triples whose middle coordinate is x. $\mathcal{V}$ is congruence distributive if and only if there is a ρ-path in T from (x,x,y) to (y,x,x). If $\mathcal{V}$ is congruence distributive then the distributivity level of $\mathcal{V}$ is the length of the shortest such path. Moreover, if $\mathcal{V}$ is congruence distributive and $m = |\mathbf{F}_{\mathcal{V}}(x,y)|$ then*

1. *the distributivity level is at most $2m-2$,*
2. *the Jónsson level is at most $2m-2$,*
3. *the alvin level is at most $2m-1$,*

and these are the best possible for all $m > 2$ (and the first two are best for all m). If $m > 2$ and the minimal length of a path is $2m-2$, then this path must correspond to Jónsson terms.

Proof. The first two statements follow from the remarks above. To see the first enumerated statement, first note that, in a shortest path, there can be at most two elements with the same first coordinate and similarly for the third coordinate. Moreover, if the first link of the sequence has the form $(x,x,y) \longrightarrow (x,x,b)$ (corresponding to a *Jónsson path*) then none of the elements except the first has its third coordinate y. Similarly if the first link has the form $(x,x,y) \longrightarrow (a,x,y)$ (corresponding to an *alvin path*), then only the first element has first coordinate x. Thus a minimal ρ-path between (x,x,y) and (y,x,x) can have at most $2m-1$ elements and so has length at most $2m-2$.

In order to see the other statements we first need a claim.

Claim 7.3. *If the distributivity level of $\mathcal{V}$ is $2m-2$ and there is an alvin path witnessing this, then $\mathcal{V}$ is k–permutable, for some k.*

Proof. Let σ be the automorphism of $\mathbf{F}_{\mathcal{V}}(x,y)$ which interchanges x and y and let τ be the relation on T given by $(a,x,b)\ \tau\ (c,x,d)$ if $a = \sigma(d)$. If the terms giving rise to these triples are f and g, respectively, then this condition says $f(x,x,y) = g(x,y,y)$. It follows that if there is a τ-path in T going from (x,x,y) to (y,x,x), then $\mathcal{V}$ has Hagemann-Mitschke terms, as displayed in (8.1).

Now suppose there is a minimal ρ-path from (x,x,y) to (y,x,x) of length $2m-2$ and that the first link is ρ_3; that is, the first two elements are (x,x,y) and (a,x,y). Since the length is even, the last link must be ρ_1, so the last two elements are (y,x,b) and (y,x,x). The projection onto the first coordinate of path has one x (in the first prosition) and every other element of $\mathbf{F}_{\mathcal{V}}(x,y)$ occurs twice, consecutively with the first projection of the last two elements both y. Every element except x also occurs twice in the projection onto the third coordinate, which begins with two y's and ends with a single x.

To show there is a τ-path, we start by noting the first link of the ρ-path, $(x,x,y)\ \rho\ (a_1,x,y)$, is a τ-link. $\sigma(a_1)$ is the third projection of two consecutive triples of the ρ-path. Let $(a_2,x,\sigma(a_1))$ be the second of these. Note this triple is the first of the two consecutive triples with first projection a_2. Continuing is this way we get τ-related triples. This does not cycle so eventually we get to a triple of the form (y,x,e) which is then τ-related to (y,x,x), proving $\mathcal{V}$ is k-permutable. □

Assume the distributivity level of $\mathcal{V}$ is $2m-2$ and there is an alvin path witnessing this. By the claim $\mathcal{V}$ is k-permutable for some k. As is shown in the next section, $k \leq m$. Now a ρ-path in T is a $(\rho_1 \wedge \rho_2) \cup (\rho_3 \wedge \rho_2)$-path in $\mathbf{S}$, and since these are congruences, its length is at most m. This implies $2m-2 \leq m$, which implies $m \leq 2$. This proves the second and third enumerated statements and the last statement.

We present an example below which, for each m, constructs a variety whose 2-generated free algebra has size m with distributivity level and Jónsson level $2m-2$ and alvin level $2m-1$. □

The Example. Let $M_n = \{0,\dots,n\}$ and define σ on M_n by $\sigma(r) = n-r$. Define operations d_{2k+1}, $0 \leq 2k+1 \leq n$, on M_n by applying the

following rules in order:

$$\begin{aligned}
&d_{2k+1}(a,b,a) = a && \\
&d_{2k+1}(a,b,c) = \sigma(d_{2k+1}(\sigma(a),\sigma(b),\sigma(c))) && \text{if } a > c \\
&d_{2k+1}(a,b,c) = a && \text{if } k < a \\
&d_{2k+1}(a,b,c) = c && \text{if } k+1 > c \\
&d_{2k+1}(a,b,c) = k && \text{if } b \leq k \\
&d_{2k+1}(a,b,c) = k+1 && \text{otherwise}
\end{aligned}$$

The algebra $\mathbf{M}_n$ is the algebra on M_n with operations d_{2k+1}, $0 \leq 2k+1 \leq n$. One easily verifies that these operations are order preserving.

First we show that $\mathbf{M}_n$ is the 2-generated free algebra in $\boldsymbol{V}(\mathbf{M}_n)$ with free generators 0 and n. Clearly $\mathbf{M}_n$ is generated by 0 and n. More generally, if $v \leq u$ then the interval between v and u is a subuniverse generated by u and v. Let $\rho_{v,u}$ be the retraction map: $\rho_{v,u}(z) = v$ if $z \leq v$, $\rho_{v,u}(z) = u$ if $z \geq u$, and $\rho_{v,u}(z) = z$ otherwise. One can verify that σ and $\rho_{v,u}$ commute with each d_{2k+1} (for the case $a > c$, the identity $\sigma\rho_{v,u} = \rho_{\sigma(u),\sigma(v)}\sigma$ helps) and so σ is an automorphism and $\rho_{v,u}$ is an endomorphism of $\mathbf{M}_n$. It follows that, for each u and v, there is an endomorphism mapping 0 to v and n to v, which implies $\mathbf{M}_n$ is free.

Lemma 7.4. *Let* $\mathbf{S}$ *be the subalgebra of* $\mathbf{M}_n^3$ *generated by* $(0,0,n)$, $(0,n,0)$ *and* $(n,0,0)$. $\mathbf{S}$ *is invariant under* $\mathbf{S}_3$*, the group of all permutations of the three coordinates, since the generators are. The elements of* $\mathbf{S}$ *consist of all the images under* $\mathbf{S}_3$ *of the set*

$$\{(a,b,c) : a \leq b \leq c, \text{ and } b + c = n-1 \text{ or } n\}. \tag{7.3}$$

Proof. Let U be the set of all images under permutations in $\mathbf{S}_3$ of the set given in (7.3) so that U consists of all triples (a,b,c) whose two largest elements sum to either $n-1$ or n. We want to show that U is a subuniverse. This, of course, will imply $S \subseteq U$. So suppose $(a_i,b_i,c_i) \in U$, for $i = 0, 1, 2$. We want to show that

$$\begin{aligned}
&d_{2k+1}((a_0,b_0,c_0),(a_1,b_1,c_1),(a_2,b_2,c_2)) \\
&\qquad = (d_{2k+1}(a_0,a_1,a_2), d_{2k+1}(b_0,b_1,b_2), d_{2k+1}(c_0,c_1,c_2))
\end{aligned} \tag{7.4}$$

is also in U.

First we show that $U' = \{(a,b,c) \in M_n^3 : a+b,\ a+c,\ b+c \leq n\}$ is a subuniverse of $\mathbf{M}_n^3$. Suppose that $(a_i,b_i,c_i) \in U'$. Then $b_i \leq n - c_i$, and so, since d_{2k+1} preserves order, $d_{2k+1}(b_0,b_1,b_2) \leq d_{2k+1}(n-c_0, n-$

$c_1, n - c_2)$. Thus

$$\begin{aligned} &d_{2k+1}(b_0, b_1, b_2) + d_{2k+1}(c_0, c_1, c_2) \\ &\quad = d_{2k+1}(b_0, b_1, b_2) + n - d_{2k+1}(n - c_0, n - c_1, n - c_2) \\ &\quad \leq d_{2k+1}(b_0, b_1, b_2) + n - d_{2k+1}(b_0, b_1, b_2) = n \end{aligned}$$

showing U' is a subuniverse.

Now assume $(a_i, b_i, c_i) \in U$. Since $U \subseteq U'$ it is enough to show that some two of the three components of (7.4) sum to at least $n - 1$.

There is a symmetry between a, b and c so we may assume $a_0 = \min(a_0, b_0, c_0)$, and thus $b_0 + c_0 = n - \varepsilon_0$, where $\varepsilon_0 = 0$ or 1. If $b_2 + c_2 = n - \varepsilon_2$, where $\varepsilon_2 = 0$ or 1, then the above calculation shows

$$\begin{aligned} &d_{2k+1}(b_0, b_1, b_2) + d_{2k+1}(c_0, c_1, c_2) \\ &\quad = d_{2k+1}(b_0, b_1, b_2) + n - d_{2k+1}(n - c_0, n - c_1, n - c_2) \\ &\quad = n - [d_{2k+1}(b_0 + \varepsilon_0, n - c_1, b_2 + \varepsilon_2) - d_{2k+1}(b_0, b_1, b_2)] \end{aligned}$$

One can show that $d_{2k+1}(b_0 + \varepsilon_0, u, b_2 + \varepsilon_2) - d_{2k+1}(b_0, v, b_2)$ is either 0 or 1 for ε_0, $\varepsilon_2 \in \{0, 1\}$ and any u and v with $u \geq v$. It follows that

$$(d_{2k+1}(a_0, a_1, a_2), d_{2k+1}(b_0, b_1, b_2), d_{2k+1}(c_0, c_1, c_2)) \in U$$

in this case.

So we may assume $b_2 + c_2 < n - 1$ and by symmetry we may assume a_2 and b_2 are the two largest of a_2, b_2, and c_2 and that $a_2 + b_2 = n - \varepsilon_2$. Now we have

$$\begin{aligned} &d_{2k+1}(b_0, b_1, b_2) + d_{2k+1}(c_0, c_1, c_2) \\ &\quad = d_{2k+1}(b_0, b_1, b_2) + n - d_{2k+1}(n - c_0, n - c_1, n - c_2) \\ &\quad = n + d_{2k+1}(b_0, b_1, b_2) - d_{2k+1}(b_0 + \varepsilon_0, n - c_1, n - c_2). \end{aligned}$$

If $b_0 \leq b_2$, then $b_0 + \varepsilon_0 \leq b_2 + \varepsilon_0 \leq n - c_2$. Whenever $a \leq c$, $d_{2k+1}(a, b, c) \in \{a, k, k + 1, c\}$ and if $k + 1 \leq c$, the value is one of $\{a, k, k + 1\}$. Using this and the fact that $b_1 \leq n - c_1$, one can show that if $k + 1 \leq b_2$, then $d_{2k+1}(b_0 + \varepsilon_0, n - c_1, n - c_2) - d_{2k+1}(b_0, b_1, b_2)$ is either 0 or 1 and so

$$d_{2k+1}(b_0, b_1, b_2) + d_{2k+1}(c_0, c_1, c_2)$$

is n or $n - 1$.

So we may assume $b_2 < k + 1$. Summarizing our assumptions at this point:

(1) b_0 and c_0 are the largest of (a_0, b_0, c_0)
(2) a_2 and b_2 are the largest of (a_2, b_2, c_2)
(3) $b_0 \leq b_2 \leq k$

Item (2) implies $c_2 \leq b_2$. So $c_2 \leq b_2 \leq k \leq (n-1)/2$ and thus $n - c_2 \geq (n+1)/2 > k$. Since $b_0 + c_0 \in \{n-1, n\}$, $c_0 \geq (n-1)/2 \geq c_2$. We claim that $d_{2k+1}(n - c_0, n - c_1, n - c_2) \in \{k, k+1\}$ and calculate

$$n - c_0 = b_0 + \varepsilon_0 \leq b_2 + \varepsilon_0 \leq k + \varepsilon_0.$$

If $n - c_0 = k+1$ then $d_{2k+1}(n-c_0, n-c_1, n-c_2) = k+1$. In all other cases $n - c_0 \leq k < n - c_2$, which implies $d_{2k+1}(n-c_0, n-c_1, n-c_2) \in \{k, k+1\}$, as claimed. Thus $d_{2k+1}(c_0, c_1, c_2) \in \{n-k, n-k-1\}$.

Similar arguments show $d_{2k+1}(a_0, a_1, a_2) \in \{k, k+1\}$. Indeed, $a_0 \leq b_0 \leq b_2 \leq k \leq (n-1)/2$ and so $a_2 \geq (n-1)/2$. Thus $a_0 \leq k \leq a_2$ and as before this implies $d_{2k+1}(a_0, a_1, a_2) \in \{k, k+1\}$.

Hence $d_{2k+1}(a_0, a_1, a_2) + d_{2k+1}(c_0, c_1, c_2)$ is at least $n-1$, showing

$$(d_{2k+1}(a_0, a_1, a_2), d_{2k+1}(b_0, b_1, b_2), d_{2k+1}(c_0, c_1, c_2)) \in U$$

in this case.

In the remaining case we have

(1) b_0 and c_0 are the largest of (a_0, b_0, c_0)
(2) a_2 and b_2 are the largest of (a_2, b_2, c_2)
(3) $b_2 < b_0$

Using an argument similar to the one showing $b_2 + c_2 < n - 1$, we may assume $a_0 + b_0 < n - 1$. Thus

$$a_0 < n - b_0 \leq n - b_2 = a_2 + \varepsilon_2, \tag{7.5}$$

which implies $a_0 \leq a_2$.

We want to show that

$$\begin{aligned} &d_{2k+1}(n - b_0, n - b_1, n - b_2) - d_{2k+1}(a_0, a_1, a_2) \\ &\quad = d_{2k+1}(n - b_0, n - b_1, a_2 + \varepsilon_2) - d_{2k+1}(a_0, a_1, a_2) \end{aligned}$$

is at most 1. This will be the case if $n - b_0 \leq k$, so we assume $k < n - b_0$. This implies $d_{2k+1}(n-b_0, n-b_1, n-b_2) = n - b_0$ and so $d_{2k+1}(b_0, b_1, b_2) = b_0$. Also $k < n - b_0 = c_0 + \varepsilon_0$ and so $k \leq c_0$. So, if $c_0 \leq c_2$, then $d_{2k+1}(c_0, c_1, c_2) = c_0$, which gives $d_{2k+1}(b_0, b_1, b_2) + d_{2k+1}(c_0, c_1, c_2) = b_0 + c_0 = n - \varepsilon_0$, as desired.

So we may assume $n - c_0 \leq n - c_2$. If $k \leq n - c_0$, then $d_{2k+1}(c_0, c_1, c_2) = c_0$ and we are done. So $n - c_0 \leq k$ and, since $n - b_2 < n - c_2$, $k < n - c_2$. Hence $d_{2k+1}(n - c_0, n - c_1, n - c_2)$ is k or $k+1$ and so $d_{2k+1}(c_0, c_1, c_2)$ is $n - k$ or $n - k - 1$.

Since $a_0 \leq n - c_0 \leq k$ and also $k < n - b_0$ and (7.5) imply $k \leq a_2$. Hence $a_0 \leq k \leq a_2$ which implies $d_{2k+1}(a_0, a_1, a_2)$ is either k or $k+1$. It follows that $d_{2k+1}(a_0, a_1, a_2) + d_{2k+1}(c_0, c_1, c_2)$ is n or $n-1$ (since we know it is at most n). This completes the proof that U is a subuniverse.

Showing that the subalgebra generated by $(0,0,n)$, $(0,n,0)$ and $(n,0,0)$ contains U is straightforword and left to the reader. □

The lemma implies that the subset T of Theorem 7.2 is $\{(a,0,c) : a+c \text{ is } n-1 \text{ or } n\}$; and so the shortest ρ-path connecting $(0,0,n)$ to $(n,0,0)$ has length $2n$ (and uses all the elements of T). Since $m = |\mathbf{A}| = n+1$, $2n = 2m-2$, proving that $\mathbf{M}_n$ achieves the bound of Theorem 7.2. The lemma also implies that the first link of a shortest ρ-path must begin with ρ_1, and hence the alvin level is $2m-1$.

We note that Howard Lee in his thesis work has independently produced a class of examples with properties similar to our $\mathbf{M}_n$'s and that in particular have arbitrarily large Jónsson levels [20].

8. Gumm Terms and other Maltsev Conditions

3-ary terms $d_0, \dots, d_{k-1}$, p are called *Gumm terms* if the equations of (7.1) hold except the last equation is replaced by the two equations

$$d_{k-1}(x,y,y) \approx p(x,y,y)$$
$$p(x,x,y) \approx y$$

By Gumm's result [8], a variety has modular congruence lattices if and only if it has Gumm terms for some k. We say a variety has *Gumm level* k if Gumm terms exist for this k but for no smaller k. (Under this counting, a variety having Jónsson level 1 satisfies $x \approx y$, while a variety having Gumm level 1 is a variety having a Maltsev term.)

We can determine the Gumm level and find Gumm terms for (the variety $\mathcal{V}$ generated by) a finite algebra using a method similar to the one for Jónsson terms. As before we let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x,y)$ generated by (x,x,y), (x,y,x) and (y,x,x), and we let T be the subset of S of triples whose middle coordinate is x. Looking at (7.2) when f is the p of Gumm's condition, we see the first coordinate is y and the third coordinate will equal the third coordinate of the triple obtained in (7.2) using $f = d_{k-1}$.

Theorem 8.1. *Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^3_{\mathcal{V}}(x,y)$ generated by (x,x,y), (x,y,x) and (y,x,x). Let T be the subset of S consisting of triples whose middle coordinate is x. $\mathcal{V}$ is congruence modular if and only if there is a sequence $\mathbf{u}^0, \mathbf{u}^1, \dots, \mathbf{u}^{k-1}, \mathbf{v}$ of elements in S such that*

(1) $\mathbf{u}^0 = (x,x,y)$,
(2) $\mathbf{u}^j \in T$, $j = 0, \dots, k-1$,
(3) $\mathbf{u}^j \ \rho \ \mathbf{u}^{j+1}$, $j = 0, \dots, k-2$,
(4) $v_0 = y$ *and* $v_2 = u_2^{k-1}$.

If $\mathcal{V}$ is congruence modular then the Gumm level of $\mathcal{V}$ is the least k for which such elements exist. Moreover, if $\mathcal{V}$ is congruence modular then the Gumm level is at most $2m-2$, where $m = |\mathbf{F}_{\mathcal{V}}(x,y)|$ and this is the best possible bound in terms of m.

Proof. All statements except for the last should be clear. The algebras $\mathbf{M}_n$ given above show the bound here is the best possible. Indeed, Lemma 7.4 shows that the only member of S, whose first coordinate is y, is (y,x,x). So $\mathbf{v}$ must be (y,x,x) and thus the sequence $\mathbf{u}^0, \mathbf{u}^1, \dots, \mathbf{u}^{k-1}, \mathbf{v}$ is a sequence which actually gives Jónsson terms so the proof above shows that the bound of this theorem is achieved. □

Remarks on speed. Theorem 8.1 leads to an algorithm to test if a variety $\mathcal{V}$ is congruence modular using a certain 3-generated subalgebra $\mathbf{S}$ of $\mathbf{F}^3_{\mathcal{V}}(x,y)$. By Proposition 6.1 $\mathbf{S}$ can be found in time a constant times $r||\mathbf{S}||$, where r is the highest arity of the basic operations. Since the rest of the test in Theorem 8.1 can be done in less time, we see that we can test for modularity in this time.

Using Day's Theorem 3.5 we obtain the next result which gives an algorithm with running time a constant times $r||\mathbf{S}'||$, where here $\mathbf{S}'$ is a particular 4-generated subalgebra of $\mathbf{F}^2_{\mathcal{V}}(x,y)$.

Theorem 8.2. *Let $\mathbf{S}'$ be the subalgebra of $\mathbf{F}^2_{\mathcal{V}}(x,y)$ generated by $a = (x,x)$, $b = (x,y)$, $c = (y,x)$ and $d = (y,y)$. Then $\mathcal{V}$ is congruence modular if and only if $(a,b) \in \mathrm{Cg}^{\mathbf{S}'}(c,d)$.*

Proof. Let a', b', c' and d' be free generators of $\mathbf{F}_4 = \mathbf{F}_{\mathcal{V}}(a',b',c',d')$ and let

$$\rho_1 = \mathrm{Cg}^{\mathbf{F_4}}((a',b'),(c',d')), \quad \rho_2 = \mathrm{Cg}^{\mathbf{F_4}}((a',c'),(b',d')), \quad \rho = \rho_1 \wedge \rho_2.$$

Since $\mathbf{F}_4/\rho_1$ and $\mathbf{F}_4/\rho_2$ are both isomorphic to $\mathbf{F}_{\mathcal{V}}(x,y)$, $\mathbf{F}_4/\rho$ is a subdirect product of two copies of $\mathbf{F}_{\mathcal{V}}(x,y)$, and $a = a'/\rho$, etc., has the form of the theorem. Now (a',b',c',d') is a Day quadruple in $\mathbf{F}_{\mathcal{V}}(a',b',c',d')$ if and only if (a,b,c,d) is one in F_4/ρ. The result follows easily from this. □

To summarize, we can determine if $\mathcal{V}$ is congruence modular by calculating a certain 3-generated subalgebra, $\mathbf{S}$, of $\mathbf{F}^3_{\mathcal{V}}(x,y)$, *or* by calculating a certain 4-generated subalgebra, $\mathbf{S}'$, of $\mathbf{F}^2_{\mathcal{V}}(x,y)$.

Since $\mathbf{S}'$ is 4-generated, unary polynomials can be represented with five-place terms and so the theorem leads to the following Maltsev condition. We have permuted the variables so that the pattern of the three inside variables looks much like Jónsson's condition for distributivity.

Theorem 8.3. *A variety $\mathcal{V}$ has modular congruence lattices if and only if there are 5-ary terms $f_0, \dots, f_k$ such that $\mathcal{V}$ satisfies*

$$\begin{aligned}
&f_0(u,x,y,z,v) \approx x \\
&f_i(y,x,y,x,y) \approx x && \text{for } 0 \le i \le k \\
&f_i(x,x,x,y,y) \approx f_{i+1}(x,x,x,y,y) && \text{for all even } i < k \\
&f_i(x,x,y,y,y) \approx f_{i+1}(x,x,y,y,y) && \text{for all odd } i < k \\
&f_k(u,x,y,z,v) \approx z.
\end{aligned}$$

This Maltsev condition is not new: it was discovered by Nation [23], who derived it in a more conventional manner as the Maltsev condition associated with a certain lattice equation. He noted that this condition shows modularity can be defined using two-variable equations (Day's Maltsev condition has three-variable equations; of course Gumm's condition also only involves two variables, but was proved later).

Hagemann-Mitschke terms for k-permutability. In [9] it was shown that a variety has k-permutable congruences if and only if it has ternary terms $p_0, p_1, \dots, p_k$ such that

$$\begin{aligned}
&p_0(x,y,z) \approx x \\
&p_i(x,x,y) \approx p_{i+1}(x,y,y), \quad \text{for } i = 0, \dots, k-1 \\
&p_k(x,y,z) \approx z
\end{aligned} \tag{8.1}$$

Theorem 8.4. *Let $\mathcal{V}$ be a variety and let $\mathbf{S}$ be the subalgebra of $\mathbf{F}^2_{\mathcal{V}}(x,y)$ generated by (x,x), (x,y) and (y,y). Let τ be the relation on S defined by $(a,b)\ \tau\ (c,d)$ if $a = d$. $\mathcal{V}$ has k-permutable congruences if and only if there is a τ-path in S from (x,x) to (y,y) of length at most k.*

If $\mathcal{V}$ is k-permutable then $k \le m$, where $m = |\mathbf{F}_{\mathcal{V}}(x,y)|$ and this is the best possible.

Proof. For an example showing the bound is the best possible we use a reduct of an algebra constructed by Kearnes [14]. Let $\mathbf{K}_n$ be the algebra with universe $\{0, 1, \dots, n-1\}$ and operations

$$h_i(x,y,z) = (x \wedge z) \vee (x \wedge p_{n-i}(y)) \vee (z \wedge p_i(y))$$

$i = 1, \dots, n-1$, where $\vee$ and $\wedge$ are just the lattice operations on K_n, and

$$p_i(x) = \begin{cases} i & \text{if } x < i \\ i-1 & \text{otherwise} \end{cases}$$

Then $\mathbf{K}_n$ is freely generated by 0 and $n-1$ and the subalgebra generated by $(0,0)$, $(0,n-1)$ and $(n-1,n-1)$ is $\{(a,b) \in K_n^2 : b \ge a-1\}$. It follows that $\mathbf{K}_n$ is n but not $n-1$ permutable.

We leave the details, as well as the rest of the proof, to the reader. □

Examples of finite k-permutable but not $k-1$-permutable algebras were first given by E. T. Schmidt [24].

It is interesting to note that the variety generated by $\mathbf{K}_n$ is also congruence distributive with Jónsson level n, which is of course the maximum for an n-permutable variety. So it is in $\mathrm{CD}(n) \setminus \mathrm{CD}(n-1)$. It is also in $\mathrm{CD}'(n) \setminus \mathrm{CD}'(n-1)$ (this refers to the ALVIN variant of Jónsson's condition). When n is even, terms showing $\boldsymbol{V}(\mathbf{K}_n) \in \mathrm{CD}'(n)$ are $f_i(x,y,z)$, $i = 0, \dots, n$, where $f_i(x,y,z) = h_i(x,y,z)$ when i is odd, and

$$f_i(x,y,z) = h_i(x, h_i(x,y,z), z)$$

for i even.

If we take the reduct of $\mathbf{K}_n$ to the f_i's, the resulting algebra $\mathbf{K}'_n$ is still in $\mathrm{CD}'(n)$, of course, but it is not in $\mathrm{CD}(n)$. $\mathbf{K}'_n$ is also the free algebra on two generators, $x = 0$ and $y = n-1$, in its variety. Using arguments similar to those used in Lemma 7.4, one can show that the subalgebra $\mathbf{S}$ generated by (x,x,y), (x,y,x) and (y,x,x) consists of all triples in $\{0, \dots, n-1\}^3$ whose two larger coordinates sum to $n-2$, $n-1$, or n, *except* that when this sum is n, the summands are not allowed to be even numbers. Using this it follows that $\mathbf{K}'_n$ is $\mathrm{CD}'(n)$ but not $\mathrm{CD}(n)$. This example finishes the proof of Proposition 7.1.

In Section 6 polynomial time algorithms were presented to determine if a given finite idempotent algebra generates a congruence modular, congruence distributive, or congruence k-permutable variety for some k. We close this section with a problem that deals with possible specializations of these results.

Problem 8.5. For a fixed k, are there polynomial time algorithms to determine if a given finite idempotent algebra has: Gumm level k, or Jónsson level k, or is k-permutable?

We note that Theorem 6.2 settles this problem for Jónsson level 2 and 2-permutability, since an algebra has a majority term if and only if it has Jónsson level 2.

9. Some Hardness Results

In this section we will see that the results from Sections 3, 5 and 6 for finite idempotent algebras do not carry over to the non-idempotent case. Example 4.6 from Kiss-Prohle [18] provides, for each n, an algebra $\mathbf{A}_n$ of size n such that $\boldsymbol{H}\,\boldsymbol{S}(\mathbf{A}_n^{n-1})$ is congruence distributive and permutable, has type set $\{\mathbf{3}\}$, no non-majority triples, and no tails.

Nevertheless, $\mathbf{A}^n$ has a two element quotient that is essentially unary and so $\boldsymbol{HSP}(\mathbf{A}_n)$ satisfies no non-trivial idempotent Maltsev condition. Note that as presented, the clone of $\mathbf{A}_n$ does not appear to be finitely generated, but in any case, we only need to use the 3-ary term operations of $\mathbf{A}_n$ to obtain the desired properties. These examples demonstrate that many of the results from Sections 3 and 5 breakdown in the absence of idempotency.

We now turn our attention to the polynomial time algorithms presented in Section 6. The main result of this section is that without the idempotency hypothesis, a number of problems not only fail to be polynomial-time solvable, but are in fact exponential-time complete. Consider the following problems:

GEN-CLO: Given a finite set A, a finite set of operations $\mathcal{F}$ on A and an operation h on A, is h in the clone on A generated by $\mathcal{F}$?

GEN-CLO$_1$: Given a finite set A, a finite set of unary operations $\mathcal{F}$ on A and a unary operation h on A, is h in the clone on A generated by $\mathcal{F}$?

GEN-CLO$'$: Given a finite set A, a finite set of operations $\mathcal{F}$ on A and a **unary** operation h on A, is h in the clone on A generated by $\mathcal{F}$?

In each of these problems, the size of an instance is measured by the size of the set A and the sizes of the operation tables of the input operations.

Kozen [19] has shown that GEN-CLO$_1$ is PSPACE complete and in [1], Bergman, Juedes, and Slutzki prove that GEN-CLO is EXPTIME complete. Note that they claim that H. Friedman had earlier proved this result. By examining the proof presented by Bergman et al., it can be seen that in fact GEN-CLO$'$ is EXPTIME complete.

We now describe a procedure that takes as input an instance $\Gamma = \langle A, \mathcal{F}, h\rangle$ of GEN-CLO$'$ and produces a finite algebra $\mathbf{B}_\Gamma$ with certain properties.

Let 0, 1 be two elements not in A and let $B = A \cup \{0, 1\}$. For an operation $g(x_1, \ldots, x_n)$ on A, let $g'(x_1, \ldots, x_n)$ denote the operation on B that extends g and is such that $g'(b_1, \ldots, b_n) = 0$ if $b_i = 0$ or 1 for some i. For $\mathcal{G}$ a set of operations on A, $\mathcal{G}'$ will denote the set of all g' for $g \in \mathcal{G}$.

Let $x \wedge y$ denote the operation on B such that

$$x \wedge y = \begin{cases} x & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}$$

Note that $\wedge$ defines a flat meet semilattice operation on B and induces the partial order $x \leq y$ if and only if $x = x \wedge y$. For x, $y \in B$ we define $x \vee y$ to be the least upper bound of $\{x, y\}$ with respect to this partial order, if it exists. So, the join of two elements will exist if and only if they are comparable with respect to $\leq$.

With $\wedge$ and $\vee$ defined as in the previous paragraph, it is not hard to see that the ternary operation $(x \wedge y) \vee (x \wedge z)$ is defined for all x, y, $z \in B$. Also note that on B, $(x \wedge y) \vee (x \wedge z) \in \{x, 0\}$. With more effort, or by consulting Section 6 of [21], it can be seen that any algebra having $(x \wedge y) \vee (x \wedge z)$ as a term operation belongs to CD(4).

Let $\mathbf{B}_\Gamma$ be the algebra with universe B and with basic operations $\mathcal{F}' \cup \{t_h(x', x, y, z)\}$, where t_h is defined as follows:

$$t_h(x', x, y, z) = \begin{cases} (x \wedge y) \vee (x \wedge z) & \text{if } h'(x) = x' \\ 0 & \text{otherwise.} \end{cases}$$

Note that $t_h(0, x, y, z) = 0$ for all x, y, $z \in A$ and $t_h(1, x, y, z) = 0$ for all x, y, $z \in B$. Also note that $t_h(x', x, y, z) \in \{x, 0\}$. Without loss of generality, we may assume that the identity map, $\mathrm{id}_A \in \mathcal{F}$ and so id'_A is in $\mathcal{F}'$. Note that the operation id'_A is the identity on A and maps 0 and 1 to 0.

Lemma 9.1. *Let $u(x)$ be a term operation of $\mathbf{B}_\Gamma$. If $u(A) \subseteq A$ then there is some term operation $v(x)$ of the algebra $\langle A, \mathcal{F} \rangle$ such that $u(a) = v(a)$ for all $a \in A$.*

Conversely, if $v(x)$ is a term operation of $\langle A, \mathcal{F} \rangle$ then $v'(x)$ is a term operation $\mathbf{B}_\Gamma$.

Proof. We prove the first part by induction on the length of a term that defines u and leave the proof of the second part to the reader. If u is defined by a term of length 1 then $u(x) = x$ for all $x \in B$ and so setting $v(x) = x$ works. If u is defined by a term of length greater than 1 then for all $x \in B$, $u(x) = f'(s_1(x), \ldots, s_n(x))$ or $u(x) = t_h(s_1(x), s_2(x), s_3(x), s_4(x))$ for some $f \in \mathcal{F}$ and some unary term operations $s_i(x)$ of $\mathbf{B}_\Gamma$ that have shorter lengths.

In the former case, since $u(A) \subseteq A$ it follows that $s_i(A) \subseteq A$ for all i. By induction we conclude that for each i there is a term operation $v_i(x)$ of $\langle A, \mathcal{F} \rangle$ such that $s_i(a) = v_i(a)$ for all $a \in A$. It follows that by setting $v(x)$ to be the term operation $f(v_1(x), \ldots, v_n(x))$ that $u(a) = v(a)$ for all $a \in A$. In the latter case, $u(A) \subseteq A$ implies, by the remark above, that $s_2(a) \in A$, for $a \in A$, and that $u(a) = t_h(s_1(a), s_2(a), s_3(a), s_4(a)) = s_2(a)$. By induction $s_2(a) = v_2(a)$, for some term operation v_2 of $\langle A, \mathcal{F} \rangle$, and thus $u(a) = v_2(a)$, for all $a \in A$, as required. $\square$

Theorem 9.2. *Let $\Gamma = \langle A, \mathcal{F}, h\rangle$ be an instance of* GEN-CLO′. *If h is in the clone on A generated by $\mathcal{F}$ then $(x \wedge y) \vee (x \wedge z)$ is in the clone of $\mathbf{B}_\Gamma$. Conversely, if $\mathbf{B}_\Gamma$ has any idempotent term that depends on more than one variable then h is in the clone on A generated by $\mathcal{F}$.*

Proof. If h is in the clone on A generated by $\mathcal{F}$ then by the previous lemma $h'(x)$ is a term operation of $\mathbf{B}_\Gamma$. Then $(x \wedge y) \vee (x \wedge z) = t_h(h'(x), x, y, z)$ is a term operation of $\mathbf{B}_\Gamma$.

Conversely, suppose that $n > 1$ and $u(x_1, \ldots, x_n)$ is an idempotent term operation of $\mathbf{B}_\Gamma$ that depends on all n variables. Since u is surjective and $t_h(x', x, y, z)$ is the only basic operation of $\mathbf{B}_\Gamma$ that is surjective then it follows that

$$u(x_1, \ldots, x_n) = t_h(s_1(\bar{x}), s_2(\bar{x}), s_3(\bar{x}), s_4(\bar{x}))$$

for some n-ary term operations s_i of $\mathbf{B}_\Gamma$. Since $u(x, x, \ldots, x) = x$ for all $x \in B$ then

$$x = t_h(u_1(x), u_2(x), u_3(x), u_4(x))$$

for all $x \in B$, where $u_i(x) = s_i(x, x, \ldots, x)$. When $x \in A$ we conclude that $u_2(x) = x$ and $u_1(x) = h'(x)$. Then, by the previous lemma there is a term operation $v(x)$ of $\langle A, \mathcal{F}\rangle$ such that $h(x) = u_1(x) = v(x)$ for all $x \in A$. This establishes that h is in the clone on A generated by $\mathcal{F}$. □

We would like to thank Ross Willard for his comments on an earlier version of the construction used in this section. With his input we were able to strengthen the following corollary considerably. We would also like to mention that there are some similarities between our construction and one introduced by Hobby in [10] to establish a related hardness result.

Corollary 9.3. *The following problems are all EXPTIME complete: Given a finite algebra $\mathbf{A}$,*

- $(1)_n$ *for a fixed $n > 1$, does $\mathbf{A}$ have an idempotent term operation that depends on n variables?*
- $(2)_n$ *for a fixed $n > 1$, does $\mathbf{A}$ have an idempotent term operation that depends on k variables for some k between 2 and n variables?*
- (3) *does $\mathbf{A}$ have a semilattice term operation?*
- $(4)_T$ *does $\mathbf{A}$ generate a variety that omits all of the types in the set T, where T is one of:*
  - (a) $\{\mathbf{1}\}$,
  - (b) $\{\mathbf{1}, \mathbf{2}\}$,
  - (c) $\{\mathbf{1}, \mathbf{5}\}$,
  - (d) $\{\mathbf{1}, \mathbf{2}, \mathbf{5}\}$.

(5) *does* $\mathbf{A}$ *generate a congruence modular variety?*
(6) *does* $\mathbf{A}$ *generate a congruence distributive variety?*
$(7)_n$ *For a fixed* $n > 3$*, is* $\mathbf{A}$ *in* $\mathrm{CD}(n)$*?*

Proof. From the theorem it follows that if the instance $\Gamma = (A, \mathcal{F}, h)$ of GEN-CLO′ is such that h is not in the clone on A generated by $\mathcal{F}$ then $\mathbf{B}_\Gamma$ does not have any idempotent term operation that depends on more than one variable. It then follows that for each of the listed problems, the answer is negative for the algebra $\mathbf{B}_\Gamma$.

On the other hand, if h is in the clone on A generated by $\mathcal{F}$ then $(x \wedge y) \vee (x \wedge z)$ is a term operation of $\mathbf{B}_\Gamma$ and so the answer to each of the listed problems is positive for $\mathbf{B}_\Gamma$.

Since the construction of the algebra $\mathbf{B}_\Gamma$ from Γ can be carried out in polynomial time we conclude that the EXPTIME complete problem GEN-CLO′ can be reduced to each of the listed problems. It is not hard to see that each of the first three problems is in EXPTIME; for the remaining problems, membership in EXPTIME follows from the observations and remarks found in Sections 7 and 8. So each of the list problems is EXPTIME complete. □

The previous corollary does not settle the issue of the complexity of determining if a finite algebra has a majority term (or equivalently has Jónsson level 2) and so we pose the following problem. Note that for idempotent algebras, Theorem 6.2 establishes that this question can be solved by a polynomial time algorithm.

Problem 9.4. Is the problem of determining if a finite algebra has a majority (or Maltsev) term EXPTIME-complete?

Corollary 9.5. *The following problems are EXPTIME hard and belong to 2-EXPTIME: Given a finite algebra* $\mathbf{A}$*,*

(1) *Does* $\mathbf{A}$ *have an idempotent term operation that depends on more than one variable?*
(2) *Does* $\mathbf{A}$ *have idempotent term operations that depend on arbitrarily large numbers of variables?*

Proof. Our encoding of instances of GEN-CLO′ as finite algebras can be used to establish the hardness of both problems. To place the problems in the complexity class 2-EXPTIME, we make use of a result of Urbanik [26]. In his Lemma 20, he shows that a finite algebra $\mathbf{A}$ has an idempotent term operation that depends on more than 1 variable if and only if it has one that depends on at most $\max\{|A|, 3\}$ variables. The problem of determining if a given algebra has this property

is a member of 2-EXPTIME, since checking this condition just involves constructing all term operations of $\mathbf{A}$ of arity at most $\max\{|A|, 3\}$.

Using Theorems 1 and 2 from [26] it follows that $\mathbf{A}$ has idempotent term operations that depend on arbitrarily large numbers of variables if and only if $\mathbf{A}$ has an idempotent term operation that depends on more than $\log_2 |A|$ variables (for then the idempotent reduct of $\mathbf{A}$ is not a diagonal algebra). From this we conclude that the second of our problems lies in 2-EXPTIME. □

We speculate that both problems are actually in EXPTIME and pose the following problem.

Problem 9.6. Determine if either problem from the previous corollary is in EXPTIME.

Let $\mathsf{ID\text{-}MEM}_n$ be the problem that takes as input a finite algebra $\mathbf{A}$, a subset S of A of size at most n and an element $a \in A$ and asks whether a is in the subalgebra of the idempotent reduct of $\mathbf{A}$ generated by S.

Corollary 9.7. *For every $n > 1$ the problem $\mathsf{ID\text{-}MEM}_n$ is EXPTIME complete.*

Proof. Given an instance $\langle \mathbf{A}, S, a \rangle$ of $\mathsf{ID\text{-}MEM}_n$, to determine if a is in the subalgebra of the idempotent reduct of $\mathbf{A}$ generated by S, we need only construct the n-ary idempotent term operations of $\mathbf{A}$ and then apply them to the elements of S until the element a appears. This process can be carried out in time bounded by an exponential function of the size of $\mathbf{A}$ and so $\mathsf{ID\text{-}MEM}_n$ is in EXPTIME. To establish EXPTIME hardness of $\mathsf{ID\text{-}MEM}_n$, we reduce the EXPTIME complete problem of determining if a finite algebra has an idempotent term operation that depends on between 2 and n variables to $\mathsf{ID\text{-}MEM}_n$.

For $\mathbf{A}$ an algebra, let $\mathbf{A}^\diamond$ denote the idempotent reduct of $\mathbf{A}$. Note that for any algebra, $(\mathbf{A}^\diamond)^n = (\mathbf{A}^n)^\diamond$. A key observation is that if a finite algebra $\mathbf{A}$ has an idempotent term that depends on m variables then there are tuples $\vec{b}_i$, $i \leq m$, and $\vec{a}$ in A^m such that $\vec{a}$ is in the subalgebra of $(\mathbf{A}^m)^\diamond$ generated by the $\vec{b}_i$'s and is not equal to any of the $\vec{b}_i$'s.

To see this, suppose that $t(\bar{x})$ is an m-ary idempotent term of $\mathbf{A}$ that depends on all of its variables. Then for each $i \leq m$, there are b_i^j, for $j \leq m$ of A such that $t(b_i^1, \ldots, b_i^m) = a_i \neq b_i^i$. Then in $(\mathbf{A}^m)^\diamond$,

$$t(\vec{b}_1, \ldots, \vec{b}_m) = \vec{a} = (a_1, a_2, \ldots, a_m)$$

where $\vec{b}_i = (b^i_1, b^i_2, \ldots, b^i_m)$ and so $\vec{a}$ is in the subalgebra of the idempotent reduct of $\mathbf{A}^m$ generated by the $\vec{b}_i$'s but is not equal to any of them.

On the other hand, if a finite algebra $\mathbf{A}$ has a subset S of size m and an element a such that a is not in S but is in the subalgebra of $\mathbf{A}^\diamond$ generated by S then $\mathbf{A}$ has an m-ary idempotent term that depends on at least 2 variables, since there must be some idempotent term that when applied to the elements of S yields a.

So, given a finite algebra $\mathbf{A}$ and $n > 1$, to determine if $\mathbf{A}$ has an idempotent term that depends on between 2 and n variables we need only check to see if there is some $1 < m \leq n$, a subset S of A^m of size at least 2 and at most m, and an element $\vec{a}$ in A^m that is not in S such that $\vec{a}$ is in the subalgebra of the idempotent reduct of $\mathbf{A}^m$ generated by S. This in turn is equivalent to testing $\mathsf{ID\text{-}MEM}_n$ with the algebra $\mathbf{A}^n$ on all subsets S of $\mathbf{A}^n$ of size at least 2 and at most n and all elements $\vec{a} \in A^n \setminus S$. From this we conclude that $\mathsf{ID\text{-}MEM}_n$ is EXPTIME hard and hence EXPTIME complete. □

References

[1] Clifford Bergman, David Juedes, and Giora Slutzki. Computational complexity of term-equivalence. *Internat. J. Algebra Comput.*, 9(1):113–128, 1999.

[2] Stanley Burris and H. P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1981.

[3] Matthias Clasen and Matthew Valeriote. Tame congruence theory. In *Lectures on algebraic model theory*, volume 15 of *Fields Inst. Monogr.*, pages 67–111. Amer. Math. Soc., Providence, RI, 2002.

[4] Alan Day. A characterization of modularity for congruence lattices of algebras. *Canad. Math. Bull.*, 12:167–173, 1969.

[5] Alan Day and Ralph Freese. A characterization of identities implying congruence modularity, I. *Canad. J. Math.*, 32:1140–1167, 1980.

[6] Ralph Freese. Computing congruences efficiently. *Algebra Universalis*, to appear.

[7] Ralph Freese and Ralph McKenzie. *Commutator theory for congruence modular varieties*, volume 125 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1987. Online version available at: `http://www.math.hawaii.edu/~ralph/papers.html`.

[8] H. P. Gumm. Congruence modularity is permutability composed with distributiveity. *Arhc. Math. (Basel)*, 36:569–576, 1981.

[9] J. Hagemann and A. Mitschke. On n-permutable congruences. *Algebra Universalis*, 3:8–12, 1973.

[10] David Hobby. Finding type sets is NP-hard. *Internat. J. Algebra Comput.*, 1(4):437–444, 1991.

[11] David Hobby and Ralph McKenzie. *The structure of finite algebras*, volume 76 of *Contemporary Mathematics*. American Mathematical Society, Providence, RI, 1988. Revised edition: 1996.

[12] B. Jónsson. Algebras whose congruence lattices are distributive. *Math. Scand.*, 21:110–121, 1967.
[13] K. A. Kearnes and M. Valeriote. A modification of Polin's variety. *Algebra Universalis*, 41(3):229–231, 1999.
[14] Keith A. Kearnes. Congruence permutable and congruence 3-permutable locally finite varieties. *J. Algebra*, 156(1):36–49, 1993.
[15] Keith A. Kearnes and Emil W. Kiss. *The shape of congruence lattices*. Preprint: online manuscript available at: `http://spot.colorado.edu/~kearnes/research.html`.
[16] Keith A. Kearnes and Emil W. Kiss. Modularity prevents tails. *Proc. Amer. Math. Soc.*, 127(1):11–19, 1999.
[17] Keith A. Kearnes and Ágnes Szendrei. The relationship between two commutators. *Internat. J. Algebra Comput.*, 8(4):497–531, 1998.
[18] Emil W. Kiss and Péter Pröhle. Problems and results in tame congruence theory. A survey of the '88 Budapest Workshop. *Algebra Universalis*, 29(2):151–171, 1992.
[19] Dexter Kozen. Lower bounds for natural proof systems. In *18th Annual Symposium on Foundations of Computer Science (Providence, R.I., 1977)*, pages 254–266. IEEE Comput. Sci., Long Beach, Calif., 1977.
[20] Howard Lee. Finite algebras that generate congruence distributive varieties. presentation at the American Mathematical Society Annual Meeting, San Antonio, Texas, 2006.
[21] Ralph McKenzie. Tarski's finite basis problem is undecidable. *Internat. J. Algebra Comput.*, 6(1):49–104, 1996.
[22] Ralph McKenzie, George McNulty, and Walter Taylor. *Algebras, Lattices, Varieties, Volume I*. Wadsworth and Brooks/Cole, Monterey, California, 1987.
[23] J. B. Nation. Varieties whose congruences satisfy certain lattice identities. *Algebra Universalis*, 4:78–88, 1974.
[24] E. T. Schmidt. On n-permutable equational classes. *Acta Sci. Math. (Szeged)*, 33:29–30, 1972.
[25] Ágnes Szendrei. A survey on strictly simple algebras and minimal varieties. In *Universal algebra and quasigroup theory (Jadwisin, 1989)*, volume 19 of *Res. Exp. Math.*, pages 209–239. Heldermann, Berlin, 1992.
[26] K. Urbanik. On algebraic operations in idempotent algebras. *Colloq. Math.*, 13:129–157, 1964/1965.
[27] Matthew Valeriote. A subalgebra intersection property for congruence distributive varieties. *Canadian Journal of Mathematics*, accepted for publication, 2006.
[28] Matthew A. Valeriote and Ross Willard. A characterization of congruence permutable locally finite varieties. *J. Algebra*, 140(2):362–369, 1991.

(Ralph Freese) Department of Mathematics, University of Hawaii, Honolulu, Hawaii, 96822 USA

(Matthew A. Valeriote) Department of Mathematics & Statistics, McMaster University, Hamilton, Ontario, L8S 4K1, Canada

E-mail address, Ralph Freese: `ralph@math.hawaii.edu`

E-mail address, Matthew A. Valeriote: `matt@math.mcmaster.ca`