Bull. London Math. Soc. 46 (2014) 870–880
doi:10.1112/blms/bdu044

Idempotent n-permutable varieties

M. Valeriote and R. Willard

Abstract

One of the important classes of varieties identified in tame congruence theory is the class of varieties which are *n-permutable for some n*. In this paper, we prove two results: (1) for every $n > 1$, there is a polynomial-time algorithm that, given a finite idempotent algebra $\mathbf{A}$ in a finite language, determines whether the variety generated by $\mathbf{A}$ is n-permutable and (2) a variety is n-permutable for some n if and only if it interprets an idempotent variety that is not interpretable in the variety of distributive lattices.

1. *Introduction*

This paper is concerned with varieties (that is, equationally axiomatizable classes) of general algebraic structures, the interpretability quasi-order relating varieties, and polynomial-time algorithms for testing congruence properties of finite algebras. For general background, see, for example, [2].

By an *algebra*, we mean any structure $\mathbf{A} = \langle A, f_i(i \in I)\rangle$ consisting of a nonvoid set A, called the *universe* of $\mathbf{A}$, and a system of finitary operations f_i over the set A, called the *basic operations* of $\mathbf{A}$. The *signature* of $\mathbf{A}$ is the indexed family $\tau = (n_i : i \in I)$ stipulating the number of variables admitted by each operation f_i. A subset of A that is closed under the basic operations of $\mathbf{A}$ is called a *subuniverse* of $\mathbf{A}$, and if it is nonempty will form the universe of a *subalgebra* of $\mathbf{A}$. A *variety* is a class of algebras over a common signature that is closed under direct products, subalgebras, and homomorphic images.

If $\mathbf{A}$ is an algebra, then we say that a binary relation on A is *compatible* (with $\mathbf{A}$) if it is a subuniverse of $\mathbf{A}^2$. A *congruence* of an algebra $\mathbf{A}$ is an equivalence relation θ on A that is compatible with $\mathbf{A}$. If θ is a congruence of $\mathbf{A}$, then an algebra of the same signature as $\mathbf{A}$ can be defined in a natural way on the set A/θ of the θ equivalence classes. The collection of congruences of an algebra forms a lattice, denoted by $\operatorname{Con}\mathbf{A}$, with lattice operations $\alpha \wedge \beta = \alpha \cap \beta$ and $\alpha \vee \beta$ the transitive closure of $\alpha \cup \beta$. To a large degree, the congruence lattices of algebras in a given variety $\mathscr{V}$ determine the structure of the members of $\mathscr{V}$.

If $\mathbf{A}$ is an algebra and R, S are reflexive subuniverses of $\mathbf{A}^2$, then $R \circ S$ denotes the subuniverse $\{(a, b) : \exists x \in A$ with $(a, x) \in R$ and $(x, b) \in S\}$. The operation $\circ$ is associative on reflexive subuniverses of $\mathbf{A}^2$ and satisfies $R \cup S \subseteq R \circ S$. Define $R \circ_1 S = R$ and $R \circ_{k+1} S = R \circ (S \circ_k R)$ for $k > 1$. The utility and importance of the operation $\circ$ are partly explained by the fact that, for any congruences α, β of $\mathbf{A}$, their join in the congruence lattice of $\mathbf{A}$ is given by $\alpha \vee \beta = \bigcup_n \alpha \circ_n \beta$.

For $n \geqslant 2$, an algebra $\mathbf{A}$ is said to be (congruence) *n-permutable* if for all $\alpha, \beta \in \operatorname{Con}\mathbf{A}$ we have $\alpha \vee \beta = \alpha \circ_n \beta$. Hagemann and Mitschke [11], generalizing Mal'cev [18] and improving [9, 21] provided the following 'classical' characterization of n-permutable varieties.

Received 21 October 2013; revised 7 March 2014; published online 17 June 2014.

2010 *Mathematics Subject Classification* 08B05 (primary), 06F99, 68Q25 (secondary).

The authors were supported by the Natural Sciences and Engineering Research Council of Canada.

PROPOSITION 1.1 [**11**]. *Fix* $n \geqslant 1$. *A variety* $\mathscr{V}$ *is* $(n+1)$*-permutable if and only if it satisfies the following condition*:

There exist terms $p_1(x,y,z),\dots,p_n(x,y,z)$ in the language of $\mathscr{V}$ so that the following are identities of $\mathscr{V}$:

$$\begin{aligned} p_1(x,y,y) &\approx x, \\ p_i(x,x,y) &\approx p_{i+1}(x,y,y) \quad \text{for } 1 \leqslant i < n, \\ p_n(x,x,y) &\approx y. \end{aligned}$$

Recall that an algebra $\mathbf{A}$ is *idempotent* if each of its fundamental operations f satisfies the *idempotent law* $f(x,x,\dots,x) \approx x$ (equivalently, if each 1-element subset of A is a subalgebra of $\mathbf{A}$), and a variety is idempotent if each of its members is. Idempotent algebras and varieties are important for a number of reasons, not the least of which is the role of finite idempotent algebras in the algebraic approach to the Constraint Satisfaction Dichotomy Conjecture (see, for example, [**1**, **4**, **17**]).

For each $n > 1$, Proposition 1.1 suggests the following algorithm for determining whether an algebra $\mathbf{A}$ generates an n-permutable variety: generate all ternary term operations of $\mathbf{A}$ and search through them for operations satisfying the Hagemann–Mitschke identities. On finite algebras in finite signatures, this algorithm can be implemented in exponential time, and Horowitz has proved [**13**, **14**] that the problem of determining whether a finite algebra generates an n-permutable variety for fixed $n > 2$ is EXPTIME-complete. However, for finite *idempotent* algebras, Freese and the first author [**7**] proved that testing whether $\mathbf{V}(\mathbf{A})$ is 2-permutable, or whether $\mathbf{V}(\mathbf{A})$ is n-permutable for some n, can both be accomplished in polynomial time, and they asked [**7**, Problem 8.5] whether, for each fixed $n > 2$, there similarly exists a polynomial-time algorithm for n-permutability in the idempotent case. In Section 3, we answer this question affirmatively.

The interpretability quasi-ordering between varieties can be defined as follows. If $\mathscr{V}$ is a variety and Σ is a set of identities in a signature τ, then we say that $\mathscr{V}$ *interprets* Σ if there is a function $f \mapsto t_f$ from τ to terms in the language of $\mathscr{V}$, so that $(A,(t_f^{\mathbf{A}} : f \in \tau))$ is a model of Σ for all $\mathbf{A} \in \mathscr{V}$. If $\mathscr{W}$ is another variety, then we write $\mathscr{W} \leqslant \mathscr{V}$ and say that $\mathscr{W}$ is *interpretable in* $\mathscr{V}$ if $\mathscr{V}$ interprets some (equivalently every) set of identities Σ axiomatizing $\mathscr{W}$. (In this definition, we have glossed over a fine point regarding nullary operations; for details, see [**2**, **8**, **19**].) Roughly speaking, $\mathscr{W} \leqslant \mathscr{V}$ means that every member of $\mathscr{V}$ carries the structure of a member of $\mathscr{W}$. The relation $\leqslant$ is a quasi-order on the class of all varieties; varieties that are 'higher' in this quasi-ordering can be considered as having 'more structure'.

The class $\mathscr{P}$ of varieties that are n-permutable for some n is one of four classes identified in the work of Hobby and McKenzie [**12**] in the locally finite case, and the work of Kearnes and Kiss [**16**] in general, as being particularly significant from a structural point of view. The other three classes are:

(1) $\mathscr{T}$, the class of varieties having a Taylor term;
(2) $\mathscr{HM}$, the class of all varieties having a Hobby–McKenzie term;
(3) $\mathscr{SD}(\wedge)$, the class of congruence meet-semidistributive varieties.

Each of $\mathscr{P}$, $\mathscr{T}$, $\mathscr{HM}$, and $\mathscr{SD}(\wedge)$ is an order-filter with respect to the interpretability quasi-order, and each has the property that a variety is in the class if and only if its idempotent reduct is. Each of these classes is definable by a linear idempotent Maltsev condition, has a characterization involving congruence properties, and (for locally finite varieties) has an omitting-types tame congruence-theoretic characterization.

For idempotent varieties, membership in each of $\mathscr{T}, \mathscr{HM}, \mathscr{SD}(\wedge)$ has a strikingly simple characterization in the interpretability quasi-order. Let *Sets* denote the variety of nonempty sets (that is, algebras with no operations), let *Semilattices* denote the variety of semilattices, and for each ring R with unit let ${}_R\mathscr{M}$ denote the variety of all unital left R-modules.

PROPOSITION 1.2. *Let $\mathscr{E}$ be an idempotent variety*:

(1) *$\mathscr{E} \in \mathscr{T}$ if and only if $\mathscr{E} \not\leqslant$ Sets*;
(2) *$\mathscr{E} \in \mathscr{HM}$ if and only if $\mathscr{E} \not\leqslant$ Semilattices*;
(3) *$\mathscr{E} \in \mathscr{SD}(\wedge)$ if and only if $\mathscr{E} \not\leqslant {}_R\mathscr{M}$ for every simple unital ring R.*

Proof. Statement (1) is due to Taylor [**20**, Corollary 5.3]; see [**12**, Lemma 9.4] for a detailed proof. Statement (2) is due to Hobby and McKenzie [**12**, Lemma 9.5]. Statement (3) is essentially due to Kearnes and Kiss as we now explain. The ($\Rightarrow$) implication is easy since nontrivial varieties of modules are never congruence meet-semidistributive. For the opposite implication, assume that $\mathscr{E} \notin \mathscr{SD}(\wedge)$. The proof of (10) $\Rightarrow$ (4) in [**16**, Theorem 8.1] gives a nontrivial module $\widehat{\mathbf{B}}$ over some ring S and an algebra $\mathbf{B} \in \mathscr{E}$ such that $\mathbf{B}$ is a term reduct of $\widehat{\mathbf{B}}$. We can assume that $\widehat{\mathbf{B}}$ is a faithful S-module and so $\mathbf{HSP}(\widehat{\mathbf{B}}) = {}_S\mathscr{M}$. Then $\mathbf{B} \in \mathscr{E}$ implies $\mathscr{E} \leqslant \mathbf{HSP}(\widehat{\mathbf{B}}) = {}_S\mathscr{M}$. Let R be a simple homomorphic image of S; then ${}_S\mathscr{M} \leqslant {}_R\mathscr{M}$, proving $\mathscr{E} \leqslant {}_R\mathscr{M}$. □

What is missing is a correspondingly simple result for the class $\mathscr{P}$. For locally finite varieties, one can easily deduce from [**12**, Theorem 9.14] that if $\mathscr{E}$ is locally finite and idempotent, then $\mathscr{E} \in \mathscr{P}$ if and only if $\mathscr{E} \not\leqslant$ *DistLat*, where *DistLat* denotes the variety of distributive lattices. Kearnes and Kiss [**16**, Problem P6] have asked whether this characterization is valid for all idempotent varieties. Freese [**6**, Theorem 8] has recently given a partial confirmation by verifying the equivalence for idempotent *linear* varieties. In Section 3, we answer the question of Kearnes and Kiss affirmatively. Equivalently, we prove that if an idempotent algebra $\mathbf{A}$ has a nontrivial compatible partial order, then the variety generated by $\mathbf{A}$ contains a two-element algebra having a compatible total order.

2. *Polynomial-time algorithm*

In this section, we show that for any integer $n \geqslant 1$, there is a polynomial-time algorithm to determine if a given finite idempotent algebra generates a congruence $(n+1)$-permutable variety. This generalizes results for congruence 2-permutability from [**7**, **13**] that were also observed by McKenzie. Our result is in contrast to the general, nonidempotent case, where this problem is exponential time complete for $n > 1$ (see [**13**]). Throughout this section, fix n to be a positive integer and let $\mathbf{A}$ be a finite algebra.

DEFINITION 2.1. Let $\vec{p} = (p_1(x,y,z), p_2(x,y,z), \dots, p_n(x,y,z))$ be a sequence of idempotent ternary operations on A. For such sequences, we set $p_0(x,y,z)$ and $p_{n+1}(x,y,z)$ to be the first and third projection functions, respectively, in the following.

(1) For a, $b \in A$ and $0 \leqslant i \leqslant n$, we call (a,b,i) an $\mathbf{A}$-triple of sort i and we say that $\vec{p}$ is a local Hagemann–Mitschke sequence of operations for the triple (a,b,i) if the equality $p_i(a,a,b) = p_{i+1}(a,b,b)$ holds.

(2) For S a collection of $\mathbf{A}$-triples, we say that $\vec{p}$ is a local Hagemann–Mitschke sequence of operations for S if it is a local Hagemann–Mitschke sequence for each triple in S.

THEOREM 2.2. *For $n \geqslant 1$, a finite algebra $\mathbf{A}$ generates an $(n+1)$-permutable variety if and only if for each set S of $\mathbf{A}$-triples of size $n+1$ there is a local Hagemann–Mitschke sequence of term operations of $\mathbf{A}$ for S.*

Proof. One direction follows from Proposition 1.1. For the other direction, we show by induction on $|S|$ that for every collection S of $\mathbf{A}$-triples there is a local Hagemann–Mitschke sequence of term operations of $\mathbf{A}$ for S. For S the set of all $\mathbf{A}$-triples, the corresponding sequence of term operations is a sequence of Hagemann–Mitschke terms for $\mathbf{A}$.

The base of the induction, when $|S| \leqslant n+1$, is given, and so suppose that S is a set of $\mathbf{A}$-triples with $|S| > n+1$ and that for every strictly smaller set of $\mathbf{A}$-triples, there is a local Hagemann–Mitschke sequence of term operations for it. Since $|S| > n+1$, there is some i such that there is more than one $\mathbf{A}$-triple of sort i in S. Let (a,b,i) be one such triple and let $U = S \setminus \{(a,b,i)\}$. Since $|U| < |S|$, it follows that there is a local Hagemann–Mitschke sequence of term operations $\vec{u}$ for U.

We now define V to be the following set of $\mathbf{A}$-triples:

$$\begin{aligned} V = \{&(u_j(c,c,d),d,j) :\ 0 \leqslant j < i \text{ and } (c,d,j) \in S\} \\ \cup\{&(u_i(a,a,b),u_{i+1}(a,b,b),i)\} \\ \cup\{&(c,u_j(c,c,d),j) :\ i < j \leqslant n \text{ and } (c,d,j) \in S\}. \end{aligned}$$

Since S contains more than one $\mathbf{A}$-triple of sort i, it follows that $|V| < |S|$ and so there is a local Hagemann–Mitschke sequence of term operations $\vec{v}$ for V. Let $\vec{s}$ be the following sequence of ternary term operations of $\mathbf{A}$:

$$\begin{aligned} s_j(x,y,z) &= v_j(u_j(x,y,z),u_j(y,y,z),z) \quad \text{for } 1 \leqslant j < i, \\ s_i(x,y,z) &= v_i(u_i(x,y,z),u_i(y,y,z),u_{i+1}(y,z,z)), \\ s_{i+1}(x,y,z) &= v_{i+1}(u_i(x,x,y),u_{i+1}(x,y,y),u_{i+1}(x,y,z)), \end{aligned}$$

and

$$s_j(x,y,z) = v_j(x,u_j(x,y,y),u_j(x,y,z)) \quad \text{for } i+1 < j \leqslant n.$$

We claim that $\vec{s}$ is a local Hagemann–Mitschke sequence of term operations for S. First note that since $\vec{u}$ and $\vec{v}$ are local Hagemann–Mitschke sequences of term operations, it follows that, by definition, the term operations in these two sequences are idempotent. It follows that the term operations in the sequence $\vec{s}$ are also idempotent. The following calculations establish the rest of our claim.

(1) Let $(c,d,j) \in S$ with $0 \leqslant j < i-1$. Then

$$\begin{aligned} s_j(c,c,d) &= v_j(u_j(c,c,d),u_j(c,c,d),d) \\ &= v_{j+1}(u_j(c,c,d),d,d) \\ &= v_{j+1}(u_{j+1}(c,d,d),d,d) \\ &= s_{j+1}(c,d,d). \end{aligned}$$

(2) Let $(c,d,i-1) \in S$ (assuming that $i \neq 0$). Then

$$\begin{aligned} s_{i-1}(c,c,d) &= v_{i-1}(u_{i-1}(c,c,d),u_{i-1}(c,c,d),d) \\ &= v_i(u_{i-1}(c,c,d),d,d) \\ &= v_i(u_i(c,d,d),d,d) \\ &= v_i(u_i(c,d,d),u_i(d,d,d),u_{i+1}(d,d,d)) \\ &= s_i(c,d,d). \end{aligned}$$

(3) Let $(c, d, i) \in S \setminus \{(a, b, i)\} = U$. Then

$$\begin{aligned} s_i(c, c, d) &= v_i(u_i(c, c, d), u_i(c, c, d), u_{i+1}(c, d, d)) \\ &= u_{i+1}(c, d, d) \\ &= v_{i+1}(u_i(c, c, d), u_{i+1}(c, d, d), u_{i+1}(c, d, d)) \\ &= s_{i+1}(c, d, d). \end{aligned}$$

(4) Since $(u_i(a, a, b), u_{i+1}(a, b, b), i) \in V$, it follows that

$$\begin{aligned} s_i(a, a, b) &= v_i(u_i(a, a, b), u_i(a, a, b), u_{i+1}(a, b, b)) \\ &= v_{i+1}(u_i(a, a, b), u_{i+1}(a, b, b), u_{i+1}(a, b, b)) \\ &= s_{i+1}(a, b, b). \end{aligned}$$

(5) Let $(c, d, i+1) \in S$. Then

$$\begin{aligned} s_{i+1}(c, c, d) &= v_{i+1}(u_i(c, c, c), u_{i+1}(c, c, c), u_{i+1}(c, c, d)) \\ &= v_{i+1}(c, c, u_{i+1}(c, c, d)) \\ &= v_{i+2}(c, u_{i+1}(c, c, d), u_{i+1}(c, c, d)) \\ &= v_{i+2}(c, u_{i+2}(c, d, d), u_{i+2}(c, d, d)) \\ &= s_{i+2}(c, d, d). \end{aligned}$$

(6) Let $(c, d, j) \in S$ with $i + 1 < j < n$. Then

$$\begin{aligned} s_j(c, c, d) &= v_j(c, u_j(c, c, c), u_j(c, c, d)) \\ &= v_j(c, c, u_j(c, c, d)) \\ &= v_{j+1}(c, u_j(c, c, d), u_j(c, c, d)) \\ &= v_{j+1}(c, u_{j+1}(c, d, d), u_{j+1}(c, d, d)) \\ &= s_{j+1}(c, d, d). \end{aligned}$$

(7) Let $(c, d, n) \in S$ (assuming that $i \neq n$). Then

$$\begin{aligned} s_n(c, c, d) &= v_n(c, u_n(c, c, c), u_n(c, c, d)) \\ &= v_n(c, c, u_n(c, c, d)) \\ &= v_n(c, c, d) = d. \end{aligned}$$

□

COROLLARY 2.3. *A finite idempotent algebra* $\mathbf{A}$ *generates a congruence* $(n+1)$*-permutable variety if and only if for every pair of* $(n+1)$*-tuples* $(a_0, a_1, \dots, a_n)$, $(b_0, b_1, \dots, b_n)$ *of elements from* A, *the pair* (a_0, b_n) *is in the relational product* $R_1 \circ R_2 \circ \cdots \circ R_n$, *where* R_i *is the subuniverse of* $\mathbf{A}^2$ *generated by the pairs* (a_{i-1}, a_i), (b_{i-1}, a_i), *and* (b_{i-1}, b_i).

Proof. By the theorem, we need to ensure that for every set of $n + 1$ $\mathbf{A}$-triples, the algebra $\mathbf{A}$ has a local Hagemann–Mitschke sequence of term operations for that set. If any two of the $\mathbf{A}$-triples in the set have the same sort, then the projection operations onto the first or third variable can be used to construct a local Hagemann–Mitschke sequence of term operations for the $n + 1$ $\mathbf{A}$-triples. So, the only type of sets of $n + 1$ $\mathbf{A}$-triples that need to be considered are of the form $\{(a_0, b_0, 0), (a_1, b_1, 1), \dots, (a_n, b_n, n)\}$ for some pair of $(n+1)$-tuples $(a_0, a_1, \dots, a_n)$, $(b_0, b_1, \dots, b_n)$ over A. It is not hard to see that there will be a local Hagemann–Mitschke sequence of term operations for such a set if and only if the condition stated in the corollary holds. □

COROLLARY 2.4. *For a fixed $n \geqslant 1$, there is a polynomial-time algorithm to determine if a given finite idempotent algebra $\mathbf{A}$ generates a congruence $(n+1)$-permutable variety.*

Proof. The condition from the previous corollary can be tested in polynomial time (as a function of the size of the algebra $\mathbf{A}$). We use the fact that the 3-generated subalgebras R_i of $\mathbf{A}^2$ from the corollary can be efficiently generated.[†] $\square$

COROLLARY 2.5. *For $n \geqslant 1$, a finite idempotent algebra $\mathbf{A}$ generates a congruence $(n+1)$-permutable variety if and only if every $(n+2)$-generated subalgebra of $\mathbf{A}^{(n+1)}$ is congruence $(n+1)$-permutable.*

Proof. We show that the condition of Corollary 2.3 can be met under the assumption that every $(n+2)$-generated subalgebra of $\mathbf{A}^{(n+1)}$ is congruence $(n+1)$-permutable. Let $\bar{a} = (a_0, a_1, \ldots, a_n)$ and $\bar{b} = (b_0, b_1, \ldots, b_n)$ be a pair of $(n+1)$-tuples of elements from A and let the R_i be the subalgebras of $\mathbf{A}^2$ from the corollary.

For $0 \leqslant i \leqslant n+1$, let $\bar{c}_i = (b_0, b_1, \ldots, b_{i-1}, a_i, a_{i+1}, \ldots)$ and let $\mathbf{C}$ be the subalgebra of $\mathbf{A}^{(n+1)}$ generated by the $\bar{c}_i$. In $\mathbf{C}$, let α and β be the congruences generated by the sets of pairs $\{(c_i, c_{i+1}) : i \text{ even}\}$ and $\{(c_i, c_{i+1}) : i \text{ odd}\}$, respectively. By construction, we have that $(\bar{a}, \bar{b}) \in \alpha \circ_{n+1} \beta$ and so by assumption, $(\bar{a}, \bar{b}) \in \beta \circ_{n+1} \alpha$.

For $0 \leqslant i \leqslant n+1$, let $\bar{d}_i = (d_0^i, d_1^i, \ldots, d_n^i)$ be elements of C such that

(1) $\bar{d}_0 = \bar{a}$;
(2) $(\bar{d}_i, \bar{d}_{i+1}) \in \beta$, for i even;
(3) $(\bar{d}_i, \bar{d}_{i+1}) \in \alpha$, for i odd;
(4) $\bar{d}_{n+1} = \bar{b}$;

and for $1 \leqslant i \leqslant n$, let $t_i(x_0, \ldots, x_{n+1})$ be a term such that

$$t_i^{\mathbf{C}}(\bar{c}_0, \ldots, \bar{c}_{n+1}) = \bar{d}_i.$$

By examining this equality in the coordinates $i-1$ and i, we see that the pair (d_{i-1}^i, d_i^i) belongs to R_i. Since for i even β is contained in the kernel of the projection of C onto its ith coordinate and for i odd α is contained in the kernel of the projection of C onto its ith coordinate, it follows that $d_i^i = d_i^{i+1}$ for $0 \leqslant i \leqslant n$. These elements witness that the pair (a_0, b_n) is in the relational product $R_1 \circ R_2 \circ \cdots \circ R_n$, as required. $\square$

The exponent $(n+1)$ in the previous corollary is tight, since the two-element distributive lattice $\mathbf{2}$ generates a variety that is not n-permutable for any n. Yet we have the following proposition.

PROPOSITION 2.6. *For every $n \geqslant 1$, every sublattice of $\mathbf{2}^n$ is congruence $(n+1)$-permutable.*

Proof. Suppose $\mathbf{L} \leqslant \mathbf{2}^n$, $\alpha, \beta \in \operatorname{Con} \mathbf{L}$, $a_0, a_1, \ldots, a_{n+1} \in L$, $(a_i, a_{i+1}) \in \alpha$ for even i, and $(a_i, a_{i+1}) \in \beta$ for odd i. It suffices to show $(a_0, a_{n+1}) \in \beta \circ_{n+1} \alpha$.

[†]More generally, for each fixed k, the problem that takes as input a finite algebra $\mathbf{A}$ in a finite signature, a subset $X \subseteq A^k$, and an element $\bar{a} \in A^k$ and decides whether $\bar{a}$ is in the subalgebra of $\mathbf{A}^k$ generated by X, is solvable in polynomial time. This fact is an easy generalization of an observation of [**15**]; see also [**3**].

Define the binary polynomial operation $\sqcap$ on $\mathbf{L}$ by $x \sqcap y = m(x, y, a_{n+1})$ where $m(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$. Also define the binary relation $\sqsubseteq$ on L by $x \sqsubseteq y$ if and only if $x \sqcap y = x$. Then $\sqcap$ is a (meet) semilattice operation on L and $\sqsubseteq$ is its corresponding partial order with least element a_{n+1}. Define $b_0 = a_0$ and $b_{i+1} = b_i \sqcap a_{i+1}$ for $i \leqslant n$. Then $a_0 = b_0 \sqsupseteq b_1 \sqsupseteq \cdots \sqsupseteq b_{n+1} = a_{n+1}$, $(b_i, b_{i+1}) \in \alpha$ for even i, and $(b_i, b_{i+1}) \in \beta$ for odd i.

Because $\sqsubseteq$ has a coordinate-wise definition in $L \subseteq \{0,1\}^n$, the poset $(L, \sqsubseteq)$ has height at most $n+1$. Hence, there exists $i \leqslant n$ such that $b_i = b_{i+1}$, which implies $(a_0, a_{n+1}) \in (\alpha \circ_n \beta) \cup (\beta \circ_n \alpha) \subseteq \beta \circ_{n+1} \alpha$, as required. $\square$

3. *Interpretability characterization*

In this section, we prove that an idempotent variety is n-permutable for some $n > 1$ if and only if it is not interpretable in the variety of distributive lattices. Our proof depends on the following lemma connecting the failure of n-permutability to the existence of algebras with a compatible partial order. The lemma follows easily from an unpublished result of Hagemann, that a variety is n-permutable for some n if and only if every compatible quasi-order in any member of the variety is an equivalence relation [**10**, Corollary 4], and is proved explicitly in [**6**, Theorem 3].

LEMMA 3.1. *The following are equivalent for an idempotent variety $\mathscr{E}$:*

(1) *$\mathscr{E}$ is not n-permutable for any $n > 1$;*
(2) *$\mathscr{E}$ contains a nontrivial member having a compatible bounded partial order.*

The heart of our argument is contained in the following claim.

PROPOSITION 3.2. *Suppose that $\mathbf{P}$ is an idempotent algebra having a compatible bounded partial order. Then the variety generated by $\mathbf{P}$ contains a two-element algebra having a compatible total order.*

Proof. Let $\leqslant$ be a compatible bounded partial order of $\mathbf{P}$ with least element 0 and greatest element 1.

DEFINITION 3.3. (1) Let $P_0 = P \setminus \{0\}$.
(2) For any $A \subseteq P$, define:

(a) $A{\uparrow} = \{x \in P : a \leqslant x \text{ for some a } \in A\}$;
(b) $A{\downarrow} = \{x \in P : x \leqslant a \text{ for some } a \in A\}$;
(c) $N_A = A{\uparrow} \setminus A{\downarrow}$.

(3) Let $\mathscr{J} = \{N_A : A \subseteq P_0\} \cup \{\{0\}\}$.

LEMMA 3.4. *The set P is not the union of any finite subset of $\mathscr{J}$.*

Proof. Suppose $\mathscr{J}_0 \subseteq \mathscr{J}$ and $\bigcup \mathscr{J}_0 = P$. Set $b_0 = 1$. As $b_0 \neq 0$, there must exist $N_{A_0} \in \mathscr{J}_0$ with $b_0 \in A_0{\uparrow} \setminus A_0{\downarrow}$. Thus, there exists $b_1 \in A_0$ with $b_1 \leqslant b_0$, and since $b_0 \notin A_0{\downarrow}$, we in fact have $b_1 < b_0$. Finally, $0 < b_1$ because $b_1 \in A_0 \subseteq P_0$.

Repeat: as $b_1 \neq 0$ there exists $N_{A_1} \in \mathscr{J}_0$ with $b_1 \in A_1{\uparrow} \setminus A_1{\downarrow}$. Note that $b_1 \in A_0 \subseteq A_0{\downarrow}$ implies $A_1 \neq A_0$. As before, we obtain $b_2 \in A_1$ with $0 < b_2 < b_1$. Let us try it again: as $b_2 \neq 0$ there exists $N_{A_2} \in \mathscr{J}_0$ with $b_2 \in A_2{\uparrow} \setminus A_2{\downarrow}$. Note that $b_2 \in A_1 \subseteq A_1{\downarrow}$ implies $A_2 \neq A_1$, and $b_2 < b_1 \in A_0$ implies $b_2 \in A_0{\downarrow}$, implying $A_2 \neq A_0$. As before, we obtain $b_3 \in A_2$ with $0 < b_3 < b_2$. Clearly, this goes on forever, implying $\mathscr{J}_0$ must be infinite. □

Hence, we can fix an ultrafilter $\mathscr{U}$ on P with the property that $\mathscr{U} \cap \mathscr{J} = \emptyset$.

Lemma 3.5. *For every $Z \in \mathscr{U}$, there exists $x \in Z$ such that $x \neq 0$ and $Z \cap \{x\}{\downarrow}$ is downward-dense above* 0; *that is, for all $u \in P$ satisfying $0 < u \leqslant x$ there exists $y \in Z$ satisfying $0 < y \leqslant u$.*

Proof. Suppose that there is no such $x \in Z$. Then for each $x \in Z \setminus \{0\}$, we can choose u_x satisfying $0 < u_x < x$ and $Z \cap \{u_x\}{\downarrow} \subseteq \{0\}$. Define $A = \{u_x : x \in Z \setminus \{0\}\}$. Then $Z \subseteq N_A \cup \{0\}$, contradicting the fact that $N_A \cup \{0\} \notin \mathscr{U}$. □

Definition 3.6. Let $\mathbf{U}$ denote the ultrapower $\mathbf{P}^P/\mathscr{U}$.

Note that the order relation $\leqslant$ is defined naturally in $\mathbf{U}$, and each operation of $\mathbf{U}$ is compatible with $\leqslant$. We will use the following notation (cf. [**5**, Definition V.2.4]): if $a, b, c, \ldots \in P^P$ and $f \in \mathrm{Clo}(\mathbf{P})$, then

$$\begin{aligned} a_{\mathscr{U}} &\text{ denotes the image of } a \text{ in } \mathbf{U}, \\ [\![a = b]\!] &\text{ denotes } \{x \in P : a(x) = b(x)\}, \\ [\![f(a, b, \ldots) < c]\!] &\text{ denotes } \{x \in P : f(a(x), b(x), \ldots) < c(x)\}, \end{aligned}$$

etc.

Let $\bar{0}$ denote the constant function $P \to P$ with value 0, let id denote the identity function $P \to P$, and let $\mathbf{0} = \bar{0}_{\mathscr{U}}$ and $\mathbf{1} = \mathrm{id}_{\mathscr{U}}$. If $f \in \mathrm{Clo}_2(\mathbf{P})$, then let $f^{[0]}$ denote the function $f(0, \_) : P \to P$. Finally, let $\mathbf{S}$ be the subalgebra of $\mathbf{U}$ generated by $\{\mathbf{0}, \mathbf{1}\}$.

Lemma 3.7. (1) *The set S satisfies: $S = \{f^{[0]}{}_{\mathscr{U}} : f \in \mathrm{Clo}_2(\mathbf{P})\}$.*
(2) *The set S satisfies: $|S| > 1$, and $\mathbf{0} \leqslant a \leqslant \mathbf{1}$ for all $a \in S$.*

Proof. Clearly $[\![\bar{0} = \mathrm{id}]\!] = \{0\} \notin \mathscr{U}$; hence $\mathbf{0} \neq \mathbf{1}$. The other claims are routine. □

Lemma 3.8. *For all $h \in \mathrm{Clo}_3(\mathbf{P})$ and all $a \in S$, if $a > \mathbf{0}$ and $h^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, a) = \mathbf{0}$, then $h^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, \mathbf{1}) = \mathbf{0}$.*

Proof. Assume instead that $h^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, \mathbf{1}) > \mathbf{0}$. Pick $f \in \mathrm{Clo}_2(\mathbf{P})$ with $f^{[0]}{}_{\mathscr{U}} = a$. Let $Z = [\![f^{[0]} > \bar{0} \text{ and } h(\bar{0}, \mathrm{id}, f^{[0]}) = \bar{0} \text{ and } h(\bar{0}, \mathrm{id}, \mathrm{id}) > \bar{0}]\!]$ and note that our assumptions imply $Z \in \mathscr{U}$. Clearly,

$$Z = \{x \in P : f(0, x) > 0 \text{ and } h(0, x, f(0, x)) = 0 \text{ and } h(0, x, x) > 0\}.$$

Pick $x \in Z$ witnessing Lemma 3.5. Because $x \in Z$, we have

$$0 < f(0, x), \quad h(0, x, f(0, x)) = 0, \quad 0 < h(0, x, x).$$

Let $u = f(0, x)$. Because $f \in \mathrm{Clo}_2(\mathbf{P})$ and $0 < x$, we have $u \leqslant f(x, x) = x$. By our choice of x, there exists $y \in Z$ with $y \leqslant u$. As $y \in Z$, we have

$$0 < f(0, y), \quad h(0, y, f(0, y)) = 0, \quad 0 < h(0, y, y).$$

But $h \in \mathrm{Clo}_3(\mathbf{P})$, so h is order-preserving, so $0 < h(0, y, y) \leqslant h(0, x, u) = 0$, a contradiction. □

Define $E = \{(a, b) \in S^2 : a = \mathbf{0} \text{ or } b \neq \mathbf{0}\}$.

Lemma 3.9. *The set E satisfies $E \leqslant \mathbf{S}^2$.*

Proof. Suppose not. Then there exist $n \geqslant 1$, $h \in \mathrm{Clo}_n(\mathbf{P})$, and $(a_1, b_1), \ldots, (a_n, b_n) \in E$ such that $h^{\mathbf{S}}(a_1, \ldots, a_n) > \mathbf{0}$ while $h^{\mathbf{S}}(b_1, \ldots, b_n) = \mathbf{0}$. We can assume (by rearranging and possibly collapsing coordinates) that $(a_1, b_1) = (\mathbf{0}, \mathbf{0})$ and $b_j > \mathbf{0}$ for all $j \geqslant 2$. Because $h^{\mathbf{S}}$ is order-preserving, we can further assume that $a_2 = \cdots = a_n = \mathbf{1}$. Thus,

$$h^{\mathbf{S}}(\mathbf{0}, b_2, \ldots, b_n) = \mathbf{0} \quad \text{and} \quad h^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, \ldots, \mathbf{1}) > \mathbf{0}.$$

Thus, there must exist $1 \leqslant k < n$ such that

$$h^{\mathbf{S}}(\mathbf{0}, \underbrace{\mathbf{1}, \ldots, \mathbf{1}}_{k-1}, b_{k+1}, b_{k+2}, \ldots, b_n) = \mathbf{0}$$

and

$$h^{\mathbf{S}}(\mathbf{0}, \underbrace{\mathbf{1}, \ldots, \mathbf{1}, \mathbf{1}}_{k}, b_{k+2}, \ldots, b_n) > \mathbf{0}.$$

For $k < j \leqslant n$, choose $f_j \in \mathrm{Clo}_2(\mathbf{P})$ such that $b_j = (f_j^{[0]})_{\mathscr{U}}$ and define

$$\bar{h}(x, y, z) = h(x, \underbrace{y, \ldots, y}_{k-1}, z, f_{k+2}(x, y), \ldots, f_n(x, y)) \in \mathrm{Clo}_3(\mathbf{P}).$$

Also let $b = b_{k+1}$ and $f = f_{k+1}$. Then

$$[\![\bar{h}(\bar{0}, \mathrm{id}, f^{[0]}) = \bar{0}]\!] = [\![h(\bar{0}, \underbrace{\mathrm{id}, \ldots, \mathrm{id}}_{k-1}, f^{[0]}, f_{k+2}^{[0]}, \ldots, f_n^{[0]}) = \bar{0}]\!] \in \mathscr{U},$$

$$[\![\bar{h}(\bar{0}, \mathrm{id}, \mathrm{id}) > \bar{0}]\!] = [\![h(\bar{0}, \underbrace{\mathrm{id}, \ldots, \mathrm{id}}_{k-1}, \mathrm{id}, f_{k+2}^{[0]}, \ldots, f_n^{[0]}) > \bar{0}]\!] \in \mathscr{U}.$$

Hence, $b > \mathbf{0}$, $\bar{h}^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, b) = \mathbf{0}$, and $\bar{h}^{\mathbf{S}}(\mathbf{0}, \mathbf{1}, \mathbf{1}) > \mathbf{0}$, contradicting Lemma 3.8. □

Now let $\theta = E \cap E^{-1}$. It follows that $\theta \in \mathrm{Con}\,\mathbf{S}$, and that if $\mathbf{T} = \mathbf{S}/\theta$, then $|\mathbf{T}| = 2$ and E/θ is a compatible total ordering of $\mathbf{T}$. As $\mathbf{T}$ is in the variety generated by $\mathbf{P}$, we have proved Proposition 3.2. □

Corollary 3.10. *The following are equivalent for an idempotent variety $\mathscr{E}$:*

(1) *$\mathscr{E}$ is n-permutable for some $n > 1$;*
(2) *$\mathscr{E} \not\leqslant$ DistLat.*

Proof. The implication (1) $\Rightarrow$ (2) is well known and can be deduced from Proposition 1.1 by noting that the two-element distributive lattice does not support Hagemann–Mitschke terms.

For the opposite implication, assume that $\mathscr{E}$ is not n-permutable for any $n > 1$. Then, by Lemma 3.1 and Proposition 3.2, $\mathscr{E}$ contains a two-element algebra $\mathbf{T}$ having a compatible total order. Thus, $\mathbf{T}$ is a term reduct of the two-element distributive lattice $\mathbf{2}$, which proves $\mathscr{E} \leqslant \mathbf{HSP}(\mathbf{2}) = \mathit{DistLat}$. □

We note that without the assumption of idempotence, Proposition 3.2 can fail badly. The following is an example of a variety $\mathscr{V}$ that is not n-permutable for any $n > 1$ but such that if $\mathbf{A}$ is a member of $\mathscr{V}$ having a nontrivial compatible partial order $\leqslant$, then $\leqslant$ has arbitrarily large finite chains.

Example 3.11. Let $\mathscr{V}$ be the variety defined by the identities for a pairing function. That is, the language of $\mathscr{V}$ consists of a binary operation p and two unary operations f, g, and $\mathscr{V}$ is defined by $p(f(x), g(x)) \approx x$, $f(p(x, y)) \approx x$, and $g(p(x, y)) \approx y$.

Consider the poset $(2^\omega, \leqslant)$ with the pointwise order. Define $f, g : 2^\omega \to 2^\omega$ and $p : 2^\omega \times 2^\omega \to 2^\omega$ by

$$\begin{aligned} f(a)(i) &= a(2i), \\ g(a)(i) &= a(2i+1), \\ p(a,b)(i) &= \begin{cases} a(i/2) & \text{if } i \text{ is even}, \\ b((i-1)/2) & \text{otherwise}. \end{cases} \end{aligned}$$

Define the algebra $\mathbf{P} = (2^\omega; f, g, p)$. Then $\mathbf{P} \in \mathscr{V}$ and $\leqslant$ is a compatible partial order for $\mathbf{P}$. As $\leqslant$ is a compatible quasi-order that is not an equivalence relation, $\mathscr{V}$ is not n-permutable for any n, by Hagemann's result.

Now suppose that $\mathbf{A}$ is any member of $\mathscr{V}$ having a nontrivial compatible partial order $\leqslant$. If $a_1 < a_2 < \cdots < a_k$ is a chain of length k in $\mathbf{A}$, then by the defining identities of $\mathscr{V}$ it follows that

$$p(a_1, a_1) < p(a_1, a_2) < \cdots < p(a_1, a_k) < p(a_2, a_k) < \cdots < p(a_k, a_k)$$

is a chain of length $2k - 1$.

References

1. L. Barto and M. Kozik, 'Constraint satisfaction problems solvable by local consistency methods', *J. ACM* 61 (2014) 3:1–3:19.
2. C. Bergman, 'Fundamentals and selected topics', *Universal algebra*, Pure and Applied Mathematics (Boca Raton) 301 (CRC Press, Boca Raton, FL, 2012).
3. C. Bergman, D. Juedes and G. Slutzki, 'Computational complexity of term-equivalence', *Internat. J. Algebra Comput.* 9 (1999) 113–128.
4. A. Bulatov, P. Jeavons and A. Krokhin, 'Classifying the complexity of constraints using finite algebras', *SIAM J. Comput.* 34 (2005) 720–742.
5. S. Burris and H. P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics 78 (Springer, New York, 1981).
6. R. Freese, 'Equations implying congruence n-permutability and semidistributivity', *Algebra Universalis* 70 (2013) 347–357.
7. R. Freese and M. A. Valeriote, 'On the complexity of some Maltsev conditions', *Internat. J. Algebra Comput.* 19 (2009) 41–77.
8. O. C. García and W. Taylor, 'The lattice of interpretability types of varieties', *Mem. Amer. Math. Soc.* 50 (1984) v+125.
9. G. Grätzer, 'Two Mal'cev-type theorems in universal algebra', *J. Combin. Theory* 8 (1970) 334–342.
10. J. Hagemann, 'Mal'cev-conditions for algebraic relations, and on regular and weakly regular congruences', Technical Report 75, Technische Hochschule Darmstadt, Fachbereich Mathematik, 1973.
11. J. Hagemann and A. Mitschke, 'On n-permutable congruences', *Algebra Universalis* 3 (1973) 8–12.
12. D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemporary Mathematics 76 (American Mathematical Society, Providence, RI, 1988).
13. J. Horowitz, 'Results on the computational complexity of linear idempotent Mal'cev conditions', PhD thesis, McMaster University, 2012.
14. J. Horowitz, 'Computational complexity of various Mal'cev conditions', *Internat. J. Algebra Comput.* 23 (2013) 1521–1531.

15. N. D. Jones and W. T. Laaser, 'Complete problems for deterministic polynomial time', *Theoret. Comput. Sci.* 3 (1976/77) 105–117.
16. K. A. Kearnes and E. W. Kiss, 'The shape of congruence lattices', *Mem. Amer. Math. Soc.* 222 (2013) viii+169.
17. B. Larose and P. Tesson, 'Universal algebra and hardness results for constraint satisfaction problems', *Theoret. Comput. Sci.* 410 (2009) 1629–1647.
18. A. I. Mal'cev, 'On the general theory of algebraic systems', *Mat. Sb. N.S.* 35 (1954) 3–20.
19. R. N. McKenzie, G. F. McNulty and W. F. Taylor, *Algebras, lattices, varieties*, The Wadsworth & Brooks/Cole Mathematics Series I (Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987).
20. W. Taylor, 'Varieties obeying homotopy laws', *Canad. J. Math.* 29 (1977) 498–527.
21. R. Wille, *Kongruenzklassengeometrien*, Lecture Notes in Mathematics 113 (Springer, Berlin, 1970).

M. Valeriote
Department of Mathematics and Statistics
McMaster University
1280 Main Street West
Hamilton, Ontario
Canada L8S 4L8

matt@math.mcmaster.ca

R. Willard
Department of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo, Ontario
Canada N2L 3G1

rdwillar@uwaterloo.ca