MINIMAL VARIETIES AND QUASIVARIETIES

CLIFFORD BERGMAN and RALPH MCKENZIE

Communicated by T. E. Hall

Abstract

We prove that every locally finite, congruence modular, minimal variety is minimal as a quasi-variety. We also construct all finite, strictly simple algebras generating a congruence distributive variety, such that the set of unary term operations forms a group. Lastly, these results are applied to a problem in algebraic logic to give a sufficient condition for a deductive system to be structurally complete.

A variety is called equationally complete if it contains no proper, non-trivial subvarieties. In other words, if it is a minimal (non-trivial) variety. As every variety is also a quasivariety, it seems natural to ask whether a minimal variety is also minimal as a quasivariety. Surely one's initial impulse is to respond "of course not", but upon reflection, one discovers that most of the familiar minimal varieties are indeed minimal quasivarieties.

In this paper we try to bring the situation into focus. We give a simple condition for a locally finite variety to be minimal as a quasivariety and prove that every locally finite, congruence modular, minimal variety is minimal as a quasivariety. We discuss examples that show that neither "local finiteness" nor "congruence modularity" can be dropped.

In the last section, we present an application of these results to algebraic logic. To every so-called algebraizable deductive system, there corresponds a quasivariety of algebras. This quasivariety is minimal if and only if the deductive system is maximal. That is, the addition of a new rule of inference will yield a logic in which every formula is provable. Similarly, the quasivariety generates a minimal variety if the logic is maximal with respect to the addition of new logical axioms. Thus our main theorem implies that these two notions of maximality coincide on those deductive systems whose associated quasivarieties are locally finite and congruence modular.

1. Preliminaries

The variety generated by an algebra A, denoted $V(A)$, is equal to the class $HSP(A)$ of all homomorphic images of subalgebras of direct powers of A. Similarly, the quasivariety generated by A, $Q(A)$, is equal to $SPP_U(A)$, the class of algebras isomorphic to subalgebras of products of ultrapowers of A. If A is finite, this latter class reduces to $SP(A)$.

An algebra A is called *strictly simple* if it is simple (implying $|A| > 1$) and has no proper non-trivial subalgebras. It is obvious that every non-trivial, locally finite variety contains a strictly simple member, (namely a non-trivial algebra of minimal cardinality) thus every minimal, locally finite variety is generated by a strictly simple algebra.

LEMMA 1. *Let A be a finite subdirectly irreducible algebra. Then $V(A)$ is a minimal quasivariety if and only if $V(A) = SP(A)$ and for every non-trivial $B \in V(A)$, we have $A \in S(B)$.*

PROOF. Suppose that $V(A)$ is a minimal quasivariety. Then of course $V(A) = SP(A)$. Also, if $B \in V(A)$ is non-trivial, then $SP(B) = V(A)$, implying that $A \in SP(B)$ and thus $A \in S(B)$ since A is subdirectly irreducible. Conversely, if $\mathscr{C}$ is a non-trivial subquasivariety of $V(A)$, then the condition implies that $A \in S(\mathscr{C}) = \mathscr{C}$, so $V(A) = SP(A) = Q(A) \subseteq \mathscr{C}$.

COROLLARY 2. *Let $\mathscr{V}$ be a locally finite variety. Then $\mathscr{V}$ is a minimal quasivariety if and only if $\mathscr{V}$ has a unique subdirectly irreducible algebra A, and A is embeddable into every non-trivial member of $\mathscr{V}$. The algebra A, if it exists, is finite and strictly simple.*

THEOREM 3. *Let A be a finite, strictly simple algebra. The variety generated by A is a minimal quasivariety if and only if $V(A) = SP(A)$ and A embeds into every non-trivial subalgebra of $A \times A$.*

PROOF. Let $\mathscr{V} = V(\mathbf{A})$. Suppose $\mathscr{V}$ is a minimal quasivariety. Then by Lemma 1, $\mathscr{V} = SP(\mathbf{A})$ and $\mathbf{A}$ embeds into every non-trivial member of $\mathscr{V}$, so in particular into every non-trivial subalgebra of $\mathbf{A} \times \mathbf{A}$. So we consider the converse.

Assume $\mathscr{V} = SP(\mathbf{A})$ and $\mathbf{A} \in S(\mathbf{D})$ for every $\mathbf{D} \leq \mathbf{A} \times \mathbf{A}$ with $|D| > 1$. Let $\mathbf{B}$ be a non-trivial member of $\mathscr{V}$. To apply Lemma 1 we need to show that $\mathbf{B}$ extends $\mathbf{A}$. $\mathscr{V}$ is generated by a finite algebra, so it is locally finite. Therefore, we may assume that $\mathbf{B}$ is finite, so $\mathbf{B} \leq \mathbf{A}^n$ for some $n > 0$. We prove by induction on n that $\mathbf{B}$ extends $\mathbf{A}$. The cases $n = 1$ and $n = 2$ are included among the assumptions.

So suppose that the required result is true for all $n < k$ for a certain integer $k > 2$. Let $\mathbf{B} \leq \mathbf{A}^k$, $|B| > 1$. Let $\mathbf{B}_0$ and $\mathbf{B}_1$ be the projections of $\mathbf{B}$ into the product of the first $k - 1$ copies of $\mathbf{A}$, and into the last copy of $\mathbf{A}$, respectively. If $\mathbf{B}_0$ is trivial, then $\mathbf{B} \cong \mathbf{B}_1$ and the desired conclusion follows. Assume that $\mathbf{B}_0$ is non-trivial. Then by the induction assumption, there exists an algebra $\mathbf{C} \leq \mathbf{B}_0$, $\mathbf{C} \cong \mathbf{A}$. Letting $\mathbf{D}$ be the subalgebra of $\mathbf{B}$ consisting of all elements whose projection into $\mathbf{A}^{k-1}$ belongs to $\mathbf{C}$, we have that $\mathbf{D} \leq \mathbf{B}$, $\mathbf{D}$ projects onto $\mathbf{C}$, and $\mathbf{D} \in S(\mathbf{A}^2)$. Thus by induction ($n = 2$) $\mathbf{D}$ embeds $\mathbf{A}$ and we are done.

We now focus our attention on congruence modular varieties. For an extensive development of the structure theory of these varieties, we direct the reader to [3]. For our purposes we require only the notion of an Abelian algebra. An algebra $\mathbf{A}$ (generating a congruence modular variety) is *Abelian* if there is a congruence on $\mathbf{A}^2$ which has the diagonal of A (*i.e.*, the set $\{(x, x) : x \in A\}$) as a congruence class. An Abelian algebra can be shown to be polynomially equivalent to a module over a ring.

LEMMA 4. *Let $\mathscr{V}$ be a locally finite, congruence modular, minimal variety, and let $\mathbf{A}$ be a strictly simple member of $\mathscr{V}$.*

(1) *If $\mathbf{A}$ is Abelian, then $\mathscr{V}$ is a minimal quasivariety.*

(2) *If $\mathbf{A}$ is not Abelian, then $\mathscr{V}$ is congruence distributive and $\mathscr{V}$ is a minimal quasivariety if and only if $\mathbf{A}$ can be embedded into every subalgebra of $\mathbf{A}^2$.*

PROOF. By minimality, $\mathscr{V}$ is finitely generated, and by [3, 10.15], $\mathbf{A}$ is finite; moreover, $\mathscr{V} = V(\mathbf{A})$. Suppose that $\mathbf{A}$ is Abelian. Then by [3, Theorem 12.4], every algebra in $\mathscr{V}$ is a Boolean power of $\mathbf{A}$, so $\mathscr{V} = SP(\mathbf{A})$. Furthermore, every subalgebra of $\mathbf{A} \times \mathbf{A}$ will be isomorphic to either $\mathbf{A}$ or $\mathbf{A} \times \mathbf{A}$. Therefore, by Theorem 3, $\mathscr{V}$ is a minimal quasivariety.

Now assume that $\mathbf{A}$ is non-Abelian. Then by [3, Theorem 12.1] $\mathscr{V}$ is congruence distributive. By Jónsson's version of the Birkhoff subdirect product

theorem [5], A is, up to isomorphism, the only subdirectly irreducible member of $\mathscr{V}$. The result now follows from Theorem 3.

By Lemma 4, our analysis of minimal, congruence modular varieties reduces to the congruence distributive case. For this, we will need the well-known Jónsson terms.

LEMMA 5 [5]. *Let* A *be an algebra.* V(A) *is congruence distributive if and only if there are ternary terms* $t_1(x, y, z), \dots, t_n(x, y, z)$ *for some* $n \geq 1$ *in the language of* A *such that these equations are true in* A:
(i) $t_1(x, y, z) \approx x$;
(ii) $t_i(x, y, x) \approx x$ *for* $1 \leq i \leq n$;
(iii) $t_i(x, y, y) \approx t_{i+1}(x, y, y)$ *for all odd* $i < n$;
(iv) $t_i(x, x, y) \approx t_{i+1}(x, x, y)$ *for all even* $i < n$;
(v) $t_n(x, y, z) \approx z$.

2. The monoid of unary terms

SOME DEFINITIONS. Let A be an algebra. $\mathrm{Clo}(A)$ denotes the set of term operations of A, and $\mathrm{Pol}(A)$ the set of polynomial operations of A (that is, operations built up from the basic and constant operations on A). For a natural number n, $\mathrm{Clo}_n(A)$ and $\mathrm{Pol}_n(A)$ denote the sets of n-ary members of $\mathrm{Clo}(A)$ and $\mathrm{Pol}(A)$ respectively. An element e of A is *idempotent* if $\{e\}$ is a subuniverse of A.

Observe that $\mathrm{Clo}_1(A)$ is a monoid acting on the set A. We say that the action of a monoid M on a set is *regular* if no non-identity element of M has a fixed point. When no confusion will result, we simply call the monoid regular. Our immediate goal is to characterize those A (strictly simple and generating a congruence distributive variety) such that $\mathrm{Clo}_1(A)$ is a group.

The next lemma is well-known.

LEMMA 6. *Let* A *be an algebra and* θ *be an equivalence relation on A. Then* θ *is a congruence of* A *if and only if*
$$\forall f \in \mathrm{Pol}_1(A) \quad (a, b) \in \theta \Rightarrow (fa, fb) \in \theta.$$

LEMMA 7. *Let* S *be a finite semigroup and* $a \in S$. *Then for some integer* $n > 0$, $a^n = a^{2n}$.

PROOF. Since S is finite, there is an integer k such that $a^k = a^{k+n} = a^{k+2n} = \cdots$ for some $n > 0$. Thus we may assume that $a^k = a^{k+n}$ and $n \geq k$. Then $a^n = a^k \cdot a^{n-k} = a^{k+n} \cdot a^{n-k} = a^{2n}$.

THEOREM 8. *Let* A *be a finite strictly simple algebra generating a congruence distributive variety, and let* M *be the monoid* $\text{Clo}_1(A)$. *Then* M *is a group if and only if it is regular.*

PROOF. Suppose that M fails to be a group. Then M contains an operation α which is not a permutation of A. By Lemma 7, there exists an n such that $\alpha^n = \alpha^{2n}$. Then for any $a \in A$, $\alpha^n(a)$ is a fixed point of α^n, but α^n is a non-identity element of M.

Now assume that M is a group. If M is a trivial group, then there is nothing to prove, so assume M is non-trivial. Therefore there is an element $a \in A$ which is not idempotent. Choose any $b \in A$. Since A is strictly simple, b lies in the subalgebra generated by a, so for some $\alpha \in M$, $b = \alpha(a)$, whence $a = \alpha^{-1}(b)$. Since M is a group, $\alpha^{-1} \in M$. Therefore b is not idempotent either, and we conclude that A contains no idempotent elements. Furthermore, M acts transitively on A.

Now, for any subset X of A, we put

$$\text{Fix}\, X = \{ \alpha \in M : \alpha(x) = x \text{ for all } x \in X \}.$$

Let Σ be the collection of all sets $X \subseteq A$ such that $|\text{Fix}\, X| > 1$, and let $U_1, \ldots, U_k$ be a list of the distinct maximal members of Σ. Then define

$$G_i = \text{Fix}\, U_i \quad \text{for } 1 \le i \le k.$$

Observe that each G_i is a subgroup of M and, for any $\alpha \in M$ and $1 \le i \le k$, there is $j \le k$ such that $\alpha \circ G_i \circ \alpha^{-1} = G_j$ and $\alpha(U_i) = U_j$. Finally, define T to be the subgroup of M generated by $\bigcup_{i=1}^{k} G_i$.

CLAIM. *For every* $\gamma \in T$, $\gamma(U_i) = U_i$, *for* $i = 1, \ldots, k$.

PROOF. Clearly it suffices to check the claim for the generators of T. If $\gamma \in G_i$ then $\gamma(U_i) = U_i$ since $\gamma \in \text{Fix}\, U_i$. So assume $\gamma \in G_j$, $j \ne i$. Pick any $a \in U_j - U_i$. Then $\gamma(a) = a$. Suppose $\gamma(U_i) \ne U_i$. Then there is $c \in U_i$ such that $b = \gamma^{-1}(c) \notin U_i$. Let $\delta \in G_i - \{\text{id}\}$. Then from the maximality of U_i it follows that $b \ne \delta(b) = d$ and $d \notin U_i$ as δ permutes U_i.

Let $t_1, \ldots, t_n$ be Jónsson terms for A. We proceed to show that for every $1 \le i < n$ we have $t_i(b, c, d) = t_{i+1}(b, c, d)$. Then from Lemma 5 it will follow that $b = d$. This is the contradiction that will establish the claim. First assume that i is odd, so that we have

$$t_i(x, y, y) = t_{i+1}(x, y, y)$$

for all $x, y \in A$. Then define

$$\alpha(x) = t_i\big(x, \delta\gamma(x), \delta(x)\big) \quad \text{and}$$
$$\beta(x) = t_{i+1}\big(x, \delta\gamma(x), \delta(x)\big).$$

Notice that $\alpha(x) = \beta(x) = x$ for all $x \in U_i$ by Lemma 5(ii). Also, $\alpha(a) = \beta(a)$ by 5(iii). Thus the function $\beta^{-1} \circ \alpha \in M$ fixes all points of $U_i \cup \{a\}$. Since U_i is maximal in Σ, it follows that $\alpha = \beta$. In particular we have

$$t_i(b,c,d) = \alpha(b) = \beta(b) = t_{i+1}(b,c,d).$$

Now assume that i is even. In this case put

$$\alpha(x) = t_i\big(x, \gamma(x), \delta(x)\big) \quad \text{and}$$
$$\beta(x) = t_{i+1}\big(x, \gamma(x), \delta(x)\big).$$

It follows from Lemma 5 (ii) and (iv) that α and β agree on the set $U_i \cup \{a\}$. Thus, just as above, we conclude that $\alpha = \beta$ and

$$t_i(b,c,d) = \alpha(b) = \beta(b) = t_{i+1}(b,c,d).$$

This concludes the proof of the claim.

Let θ be the equivalence relation on A whose classes are the orbits under the action of T. Then θ is a congruence on $\mathbf{A}$. To show this, by Lemma 6, it is enough to prove that if $(a,b) \in \theta$ and $f \in \mathrm{Pol}_1(\mathbf{A})$ then $(f(a), f(b)) \in \theta$. Furthermore, by the definition of T, we may assume that $b = \gamma(a)$ for some $\gamma \in G_i$ and $1 \leq i \leq k$.

There is a term $s \in \mathrm{Clo}\,(\mathbf{A})$ and $c_1, c_2, \ldots, c_n \in A$ such that $f(x) = s(x, c_1, \ldots, c_n)$. Then by the transitivity of $\mathbf{M}$, $f(x) = h(x,a)$ for some binary term h. We define two members of M:

$$\alpha(x) = h(x,x) \quad \text{and} \quad \beta(x) = h(\gamma(x), x).$$

Thus we need to show that $\big(\alpha(a), \beta(a)\big) \in \theta$.

Since $\gamma \in G_i$, α and β agree on U_i. Thus $\beta \circ \alpha^{-1} \in G_j$, some $j \leq k$. Since $(\beta \circ \alpha^{-1})(\alpha(a)) = \beta(a)$, it follows that $\big(\alpha(a), \beta(a)\big) \in \theta$ as desired.

Now the group T is in all events a group of more than one element, since there is at least one set U_i (which may, conceivably, be the empty set). Thus $\theta \neq 0_A$. Therefore by the simplicity of $\mathbf{A}$, $\theta = 1_A$, equivalently, T acts transitively. Then by the Claim, each set U_i must be either empty or identical to A. As the definition of U_i precludes its equality with A, we must have $k = 1$ and $U_1 = \varnothing$. That is, $\mathbf{M}$ is regular.

The referee has offered an alternate proof of Theorem 8. As it is equally interesting, (and markedly different) we sketch the argument. Assume that $\mathbf{M}$ is a group and $\mathbf{A}$ has no idempotent elements. M is a subuniverse of $\mathbf{A}^4$. Let $\mathbf{F}$ denote the subalgebra of $\mathbf{A}$ with universe M. For any subset Z of A, let η_Z be the projection congruence on $\mathbf{F}$ corresponding to Z. Observe that $(\alpha, \beta) \in \eta_Z \Leftrightarrow \alpha^{-1} \circ \beta \in \mathrm{Fix}\,Z$, and $\eta_Z = \bigcap_{z \in Z} \eta_z$.

For $a, b \in A$, write $a \sim b$ iff $\eta_a = \eta_b$. This is clearly an equivalence relation on A, and as $\mathbf{A}$ is strictly simple and has no idempotents, $a \not\sim b \Leftrightarrow$

$\eta_a \vee \eta_b = 1_F$. Let X be any subset of A which is a union of $\sim$-classes and $Y = A - X$. We claim that X is a subuniverse of $\mathbf{A}$. By the distributivity of Con $\mathbf{F}$, $\eta_X \vee \eta_Y = 1_F$. Hence, by taking a Maltsev chain, we see that the group $\mathbf{M}$ is generated by the subset Fix $X \cup$ Fix Y. Since the elements of Fix Y preserve X, (and the elements of Fix X certainly preserve X) X is a subuniverse of $\mathbf{A}$.

Finally, since $\mathbf{A}$ has no proper subalgebras, we conclude that either $|A| = 2$, or any two elements of A are equivalent modulo $\sim$. In either case, $\mathbf{M}$ is regular.

It is possible to construct all of the algebras satisfying the conditions of Theorem 8. In [7], [8] and [9], A. Szendrei analyzes the clones of strictly simple algebras. We can apply those results to characterize, up to term equivalence, all finite, strictly simple algebras $\mathbf{A}$ generating a congruence distributive variety, and whose clone of unary terms forms a group.

Let A be a non-empty set. An n-ary operation f on A is called *idempotent* if

$$f(a, a, \ldots, a) = a \quad \text{for all } a \in A.$$

An algebra $\mathbf{A}$ is idempotent if every term function of $\mathbf{A}$ is idempotent.

Now, for any $a \in A$ define

$$X_n^a = \bigcup_{i=1}^{n} (A \times A \times \cdots \times \overset{i\text{th}}{\{a\}} \times A \times \cdots \times A), \quad n \geq 2,$$

(each summand contains n factors) and let $\mathscr{F}_k^a$ denote the clone of idempotent operations on A preserving X_k^a. Put $\mathscr{F}_\omega^a = \bigcap_{k=2}^{\omega} \mathscr{F}_k^a$. If $\mathbf{G}$ is a group acting on the set A, let $\mathscr{R}_A(\mathbf{G})$ denote the clone of operations f on A such that

$$f(x_1, x_2, \ldots, x_n)g = f(x_1 g, x_2 g, \ldots, x_n g) \quad \text{for every } g \in G, \text{ and } x_i \in A$$

and let $\mathscr{I}_A(\mathbf{G})$ denote the idempotent members of $\mathscr{R}_A(\mathbf{G})$.

THEOREM 9 (Szendrei). *Let $\mathbf{A}$ be a finite, strictly simple algebra with $|A| > 2$. If $\mathbf{A}$ is idempotent, then $\mathbf{A}$ is term equivalent to one of the following algebras:*

(1) *$\langle A, \mathscr{I}_A(\mathbf{G}) \rangle$ for a group $\mathbf{G}$ acting on A such that every non-identity member of $\mathbf{G}$ has at most one fixed point;*

(2) *the full idempotent reduct of the module $\langle A, +, \mathrm{End}_K \mathbf{B} \rangle$ for some vector space $\mathbf{B} = \langle A, +, K \rangle$ over a field K;*

(3) *$\langle A, \mathscr{I}_A(\mathbf{G}) \cap \mathscr{F}_k^0 \rangle$ for some k $(2 \leq k \leq \omega)$, some element $0 \in A$, and a group $\mathbf{G}$ acting on A such that 0 is the unique fixed point of every non-identity member of $\mathbf{G}$.*

If A *has no idempotent elements, and if* Aut(A) *acts transitively on A, then* A *is term equivalent to one of the following*:

(4) $\langle A, \mathscr{R}_A(\mathbf{G}) \rangle$, *for a transitive and regular group* **G** *of permutations of A*;

(5) *an algebra as in* (2), *above*

(6) $\langle A, \mathbf{G} \rangle$, *where* $|A|$ *is prime and* **G** *is a regular, transitive (hence cyclic) permutation group on A.*

The proof of [8, Theorem 1] shows that the algebras of type (1), (3) and (4) generate congruence distributive varieties. In fact, those of type (1) and (4) are quasi-primal. The algebras of type (2) (and (5)) all generate congruence modular, abelian varieties. Those of type (6) are essentially unary, and do not generate a congruence modular variety.

COROLLARY 10. *Let* A *be a finite, strictly simple algebra generating a congruence distributive variety and such that* $\mathrm{Clo}_1(\mathbf{A})$ *is a group.*

(1) *If* A *has an idempotent, then* A *is an idempotent algebra and, if* $|A| > 2$ *then* A *is term-equivalent to an algebra as described in Theorem* 9(1) *or* (3) *above.*

(2) *If* A *has no idempotents, then* A *is term equivalent to the algebra* $\langle A, \mathscr{R}_A(\mathbf{G}) \rangle$, *where* **G** *is the automorphism group of* A.

PROOF. Suppose first that **A** has an idempotent. Then that element is a fixed point of every member of $\mathrm{Clo}_1(\mathbf{A})$. By Theorem 8, $\mathrm{Clo}_1(\mathbf{A})$ is regular, so must be trivial. Therefore every member of **A** is idempotent. If $|A| > 2$, then we can apply Theorem 9. Case 9(2) cannot occur here, since it implies that **A** is Abelian.

Assume now that **A** has no idempotent elements. For any element (a, b) of A^2, the subalgebra of $\mathbf{A}^2$ generated by (a, b) is equal to

$$\{(\alpha(a), \alpha(b)) : \alpha \in \mathrm{Clo}_1(\mathbf{A})\},$$

which by Theorem 8 is isomorphic to **A** under each of the coordinate projections. Thus it is the graph of an automorphism of **A**. It follows that Aut(**A**) acts transitively on A. Furthermore, the set of fixed points of an automorphism is a subalgebra of **A**. Therefore, the action is regular as well.

Applying Theorem 9, **A** is term equivalent to one of the algebras in categories (4)–(6). However as noted above, only those of type (4) generate a congruence distributive variety. Thus **A** is term equivalent to $\langle A, \mathscr{R}_A(\mathbf{G}) \rangle$ for some group **G** acting on A in a transitive, regular manner.

By transitivity and regularity, we have $|G| = |A| = |\mathrm{Aut}(\mathbf{A})|$. Furthermore, since the action of **G** preserves every operation of **A**, there is a natural group

embedding of **G** into Aut(**A**). It follows that we may take **G** equal to Aut(**A**) in the Corollary.

3. The main theorem

LEMMA 11 (Folklore). *Let* **A** *be a finite, strictly simple algebra, and let* **B** *be a subalgebra of* A^2. *Then* $B \cong A$ *if and only if either* **B** *is the graph of an automorphism of* **A**, *or* $B = \{e\} \times A$ *or* $B = A \times \{e\}$ *for some idempotent element e of* **A**.

PROOF. Let $B \cong A$, where $B \leq A^2$. Let B_i $(i = 0, 1)$ be the projections of **B** into A at the two coordinates. Since B_i is a subalgebra of **A**, we have $B_i = A$ or $B_i = \{e\}$, a 1-element subuniverse. Our claim is clearly true if $|B_i| = 1$ for $i = 0$ or $i = 1$. Assume that $B_0 = A = B_1$. Then cardinality considerations imply that for every $x \in A$ there are unique elements $y, z \in A$ such that $(x, y) \in B$ and $(z, x) \in B$; *i.e.*, B is the graph of a permutation of A. Since B is a subuniverse of A^2, the permutation is an automorphism of **A**.

THEOREM 12. *Let* $\mathscr{V}$ *be a minimal, locally finite, congruence distributive variety. Then* $\mathscr{V}$ *is a minimal quasivariety.*

PROOF. Let **A** be a strictly simple algebra generating the variety $\mathscr{V}$. By Lemma 4(2), we must show that **A** can be embedded into every non-trivial subalgebra of A^2. Let us assume that this is false and derive a contradiction. Without loss of generality, we may assume that **A** is a counterexample of minimal cardinality. That is

(∗)   **A** is a strictly simple algebra generating a congruence distributive variety; there is a minimal, non-trivial subalgebra **R** of A^2 such that $A \notin S(R)$; and for every strictly simple algebra **B** generating a congruence distributive variety (of any type), if $|B| < |A|$ then every non-trivial subalgebra of B^2 extends **B**.

Observe that R is non-trivial and is not of the form $\{e\} \times A$ or $A \times \{e\}$ (since $R \not\cong A$), so **R** must be a subdirect square of **A**. Furthermore, it can not be the graph of a function, since then it would be an automorphism of **A**, and we would have $R \cong A$ again. Therefore

(†)   there are pairs $(a, b), (a, c) \in R$ with $b \neq c$.

Let $E = \{e \in A : e$ is an idempotent of **A**$\}$. Then

$$\forall (x, y) \in R \quad x \in E \Leftrightarrow y \in E;$$

for if, say $x \in E$ and $y \notin E$, then $\mathrm{Sg}^{\mathbf{A}^2}(\{(x,y)\})$ (the subuniverse of $\mathbf{A}^2$ generated by (x,y)) must be identical with $\{x\} \times A$ which is impossible. Let $T = R^{-1} \circ R$, the relation product of R with its inverse relation. Then T is a diagonal subuniverse of $\mathbf{A}^2$, *i.e.*, T contains the identity relation. Hence the equivalence relation θ generated by T is a congruence of $\mathbf{A}$. Now since $\mathbf{A}$ is simple we have either $\theta = 0_A$ (the identity relation) or $\theta = 1_A$ $(= A \times A)$.

If $\theta = 0_A$, then $T = 0_A$, which is false since $(c,b) \in T$ and $c \neq b$. Therefore $\theta = 1_A$. Now using the fact that $\theta = T \cup (T \circ T) \cup (T \circ T \circ T) \cup \cdots$ and the remarks above, for any $x, y \in A$, $x \in E \Leftrightarrow y \in E$. In other words, $E = \varnothing$ or $E = A$. But by (†), if a were idempotent, then $\{a\} \times A = \mathrm{Sg}^{\mathbf{A}^2}(\{(a,b),(a,c)\}) \subseteq R$, contradicting $\mathbf{A} \notin S(\mathbf{R})$. Thus $E = \varnothing$, *i.e.*, $\mathbf{A}$ has no idempotents.

Let $\mathbf{M} = \mathrm{Clo}_1(\mathbf{A})$. Since $\mathbf{A}$ has no idempotents and $\mathbf{R}$ is a minimal subalgebra, $\mathbf{R}$ is generated by any one of its elements. Therefore, $\mathbf{M}$ acts transitively on R, and of course, on A. Furthermore, R is irreflexive, since $(x,x) \in R$ implies $\mathbf{A} \cong \mathrm{Sg}^{\mathbf{R}}(\{(x,x)\}) = \mathbf{R}$, a contradiction.

Suppose that $\mathbf{M}$ were a group. Then by Theorem 8, the action of $\mathbf{M}$ would be regular. Since $\mathbf{M}$ acts transitively on R, there is $\alpha \in M$ with $(\alpha a, \alpha b) = (a, c)$ by (†). But then by regularity, α must be the identity map, contradicting the fact that $b \neq c$.

Since $\mathbf{M}$ is not a group, there is $\alpha \in M$ such that $\alpha(A) \neq A$. By Lemma 7, we can assume that $\alpha = \alpha \circ \alpha$. Let $B = \alpha(A)$. Observe that $B = \{x \in A : \alpha x = x\}$. We define an algebra $\mathbf{B} = \langle B, F \rangle$ by taking F to be the set of all operations $(\alpha \circ g)\restriction_B$ where $g \in \mathrm{Clo}(\mathbf{A})$. We define $S = R \cap B^2$; then it is clear that S is a subuniverse of the algebra $\mathbf{B}^2$. We shall finish the proof of the theorem by showing that $\mathbf{B}$ is a strictly simple algebra, that $V(\mathbf{B})$ is congruence distributive, and that $\mathbf{S}$ is a non-trivial subalgebra of $\mathbf{B}^2$ which does not embed $\mathbf{B}$—thus we will have contradicted our assumption (∗).

First, note that $\mathbf{B}$ is non-trivial; if $B = \{x\}$ for some $x \in A$, then choosing any $(u,v) \in R$ we have that $(x,x) = (\alpha u, \alpha v) \in R$, contradicting the irreflexivity of R. Moreover, $V(\mathbf{B})$ is congruence distributive by Lemma 5: if $t_1, \ldots, t_n$ are Jónsson terms for $\mathbf{A}$, and if we choose a term $s(x)$ so that $\alpha = s^{\mathbf{A}}$, then $s(t_1(x,y,z)), \ldots, s(t_n(x,y,z))$ are Jónsson terms for $\mathbf{B}$. Next, B is the only non-void subuniverse of $\mathbf{B}$: for if $x, y \in B$, there exists $\beta \in \mathrm{Clo}_1(\mathbf{A})$ with $\beta x = y$ and then $\alpha \circ \beta \restriction_B = g \in F$ and $g(x) = y$.

To see that $\mathbf{B}$ is simple, suppose that θ is a congruence of $\mathbf{B}$. Define

$$\psi = \left\{ (x,y) \in A^2 : (\forall f \in \mathrm{Pol}_1(\mathbf{A}))\ (\alpha f(x), \alpha f(y)) \in \theta \right\}.$$

By Lemma 6, ψ is a congruence on $\mathbf{A}$. We claim that $\theta = \psi \cap B^2$.

Clearly $\psi \cap B^2 \subseteq \theta$. To see the converse, let $(u,v) \in \theta$, and let $f \in \mathrm{Pol}_1(\mathbf{A})$. We need $(\alpha f(u), \alpha f(v)) \in \theta$. Using the same argument we employed in

Theorem 8, there is $h \in \mathrm{Clo}_2(\mathbf{A})$ such that $f(x) = h(x, u)$, for all $x \in A$. Since $(\alpha \circ h){\restriction}_B \in F$, $(\alpha \circ f){\restriction}_B$ is a polynomial operation of $\mathbf{B}$, so we indeed have $\alpha f(u) \equiv \alpha f(v) \pmod{\theta}$. Now the simplicity of $\mathbf{A}$ implies that $\psi \in \{0_A, 1_A\}$, so $\theta \in \{0_B, 1_B\}$. We conclude that $\mathbf{B}$ is strictly simple.

Finally we consider the relation S. Clearly S is non-empty. Since $\mathbf{B}$ is non-trivial and has no idempotents, S must have more than one element. Let (x, y) and (u, v) be elements of S. Then by the transitivity of $\mathbf{M}$, $(u, v) = (\beta x, \beta y) = (\alpha \beta x, \alpha \beta y) \in \mathrm{Sg}^{\mathbf{B}^2}(\{(x, y)\})$ for some $\beta \in M$, thus S is a minimal, non-trivial subuniverse of $\mathbf{B}^2$. Suppose $\mathbf{S} \cong \mathbf{B}$. Since $\mathbf{B}$ has no idempotents, S must be, by Lemma 11, the graph of an automorphism of $\mathbf{B}$. Now if $(x, y), (x, z) \in R$ then $(\alpha x, \alpha y), (\alpha x, \alpha z) \in S$, and so $\alpha y = \alpha z$. Thus $R^{-1} \circ R \subseteq \ker(\alpha)$. But as we saw earlier, the equivalence relation on A generated by $R^{-1} \circ R$ is a congruence on $\mathbf{A}$, and must be 1_A. Thus $\ker(\alpha) = 1_A$. But then $|B| = 1$, which we have already established to be false. So we conclude that $\mathbf{S} \not\cong \mathbf{B}$. Thus we have a contradiction to $(*)$.

Combining the theorem with Lemma 4, we have

COROLLARY 13. *Every locally finite, congruence modular, minimal variety is a minimal quasivariety.*

4. Examples

EXAMPLE 14. *There is a finite algebra that generates a minimal variety that is not minimal as a quasivariety.*

PROOF. Let $\mathbf{A} = \langle \{0, 1, 2\}, \cdot, f, g, \underline{0}, \underline{1}, \underline{2} \rangle$ be the algebra of type $\langle 2, 1, 1, 0, 0, 0 \rangle$ in which

$$x \cdot y = \begin{cases} 0, & \text{if } x = 0, \\ y, & \text{if } x \neq 0, \end{cases}$$
$$f(0) = f(1) = 0, \quad f(2) = 2,$$
$$g(0) = g(2) = 0, \quad g(1) = 1,$$

and $\underline{0}, \underline{1}, \underline{2}$ are names for the corresponding elements of $\mathbf{A}$.

Let $\mathscr{V}$ be the variety generated by $\mathbf{A}$. To see that $\mathscr{V}$ is a minimal variety, let $\mathbf{C}$ be any non-trivial member of $\mathscr{V}$. It suffices to show that $\mathbf{A} \leq \mathbf{C}$. It is easy to check that $\mathbf{A}$ is simple. Since $\mathscr{V} = HSP(\mathbf{A})$, $\mathbf{C}$ is a homomorphic image of an algebra $\mathbf{B} \leq \mathbf{A}^I$ for some set I. The elements $\underline{0}^{\mathbf{B}}, \underline{1}^{\mathbf{B}}, \underline{2}^{\mathbf{B}}$ are the constant functions of A^I, and form a subuniverse of $\mathbf{B}$ isomorphic to $\mathbf{A}$. Thus

there is a homomorphism $s : \mathbf{A} \to \mathbf{C}$ taking $0, 1, 2$ to $\underline{0}^C, \underline{1}^C, \underline{2}^C$ respectively. If s is trivial, then $\underline{0}^C = \underline{1}^C$. But the equations $\underline{0} \cdot x \approx \underline{0}$ and $\underline{1} \cdot x \approx x$ are true in $\mathbf{A}$, hence in $\mathscr{V}$. Therefore, for every $c \in C$, $\underline{0}^C = \underline{0}^C \cdot c = \underline{1}^C \cdot c = c$, contradicting the non-triviality of $\mathbf{C}$. Thus s is an embedding, so $\mathscr{V}$ is equationally complete.

There is a congruence θ on $\mathbf{A} \times \mathbf{A}$ with one non-trivial equivalence class: $Z = \{(0,0), (0,1), (0,2), (1,0), (2,0)\}$. This follows because Z is an ideal of $\mathbf{A}^2$, i.e., for every $z \in Z$ and $a \in A^2$, $z \cdot a, a \cdot z, f(z)$ and $g(z)$ always lie in Z.

Now let $\mathbf{B} = \mathbf{A}^2/\theta$. Then $\mathbf{B}$ fails to satisfy the quasi-identity

$$(\forall x)\, (f(x) \approx g(x) \ \to \ x \approx \underline{0})$$

(since $f[(1,2)/\theta] = g[(1,2)/\theta] = (0,0)/\theta$) which holds in $\mathbf{A}$. Therefore, $\mathscr{V}$ is not a minimal quasivariety. (Alternately, show that $\mathbf{B}$ is subdirectly irreducible, and use Corollary 2.)

The variety $\mathscr{V}$ in this example is locally finite, since it is generated by a finite member. But of course it is not congruence modular. Our second example shows that the assumption of local finiteness is necessary in Corollary 13. In fact, the variety in this example will be arithmetical, that is, both congruence distributive and permutable. It was provided to us by H. Andréka and I. Németi, who have kindly allowed us to include it here. We only outline the proof.

EXAMPLE 15 (Andréka–Németi). *There is a minimal, arithmetical variety that is not minimal as a quasivariety.*

PROOF. Let $\mathbf{C}$ be the full ω-dimensional cylindric set algebra on a 3-element base. (See [4] for the relevant definitions.) Let $\mathscr{V} = V(\mathbf{C})$. Then $\mathscr{V}$ is the desired example. $\mathscr{V}$ is arithmetical, since every cylindric algebra is an expansion of a boolean algebra. The minimality of $\mathscr{V}$ as a variety is proved in [6, Corollary 3.15].

Let $\mathbf{M}$ be the subalgebra of $\mathbf{C}$ generated by $\varnothing$. $\mathbf{M}$ is a non-trivial algebra since $\mathbf{C}$ contains infinitely many distinct diagonal elements, each of which has a name in the language. Then it turns out that $\mathbf{M}$ satisfies the quasi-identity

$$(\forall x, y, z)\, (x \wedge y \approx x \wedge z \approx y \wedge z \approx 0 \ \& \ c_0 x \approx c_0 y \approx c_0 z \approx 1 \ \to \ 0 \approx 1)$$

while $\mathbf{C}$ does not. Therefore this quasi-identity defines a proper, non-trivial subquasivariety of $\mathscr{V}$.

5. An application to algebraic logic

In order to apply our results to algebraic logic, we need to outline some of the basic notions of that subject. We follow the treatment in [2]. We direct the reader to that monograph for additional references.

A *deductive system* is a pair $\mathscr{S} = \langle L, C \rangle$, in which L is a propositional language (*i.e.*, a set of propositional connectives) and C is an algebraic, structural closure operator on the set Fm of formulas of L in the propositional variables $p_0, p_1, p_2, \ldots$. That is, for all sets Γ, Δ of L-formulas:

$$\Gamma \subseteq C(\Gamma),$$

$$\Gamma \subseteq \Delta \Rightarrow C(\Gamma) \subseteq C(\Delta),$$

$$CC(\Gamma) \subseteq C(\Gamma),$$

$$C(\Gamma) \subseteq \bigcup \{ C(\Gamma') : \Gamma' \text{ is a finite subset of } \Gamma \},$$

$$\sigma(C(\Gamma)) \subseteq C(\sigma(\Gamma)) \quad \text{for all substitutions } \sigma.$$

(By a substitution, we mean a mapping $\sigma \colon \{p_0, p_1, \ldots\} \to Fm$. $\sigma(\Gamma)$ is the set of all formulas obtained by replacing p_i by $\sigma(p_i)$ in each $\gamma \in \Gamma$, for all $i \in \omega$.) C is called the *consequence operator* of $\mathscr{S}$, and $C(\Gamma)$ is the $\mathscr{S}$-theory generated by Γ.

Let $\mathscr{S} = \langle L, C \rangle$ and $\mathscr{S}' = \langle L, C' \rangle$ be two deductive systems in the same language L. We define

$$\mathscr{S} \leq \mathscr{S}' \Leftrightarrow (\forall \Gamma \subseteq Fm) \, C(\Gamma) \subseteq C'(\Gamma)$$

and call $\mathscr{S}'$ an *extension* of $\mathscr{S}$. Also, define

$$\mathscr{S} \equiv_0 \mathscr{S}' \Leftrightarrow C(\varnothing) = C'(\varnothing).$$

'$\equiv_0$' is an equivalence relation on the set of deductive systems over a fixed language. $C(\varnothing)$ can be thought of as the set of tautologies of $\mathscr{S}$.

The main results in [2] are directed towards developing the notion of an *algebraizable* deductive system. The definition is too involved to reproduce here. Intuitively, a deductive system $\mathscr{S}$ is algebraizable if and only if it can be associated with a quasivariety $\mathscr{S}^Q$ of algebras whose basic operation symbols are those of L. Under this association, the tautologies of $\mathscr{S}$ correspond to the identities of $\mathscr{S}^Q$, and the rules of inference to the quasi-identities. Furthermore, if both $\mathscr{S}$ and $\mathscr{S}'$ are algebraizable, then $\mathscr{S} \leq \mathscr{S}' \Leftrightarrow \mathscr{S}^Q \supseteq \mathscr{S}'^Q$. Not every deductive system is algebraizable. But from [2, Corollary 4.9] we have that every extension of an algebraizable deductive system is algebraizable.

For a fixed language L, let A denote the set of all algebraizable deductive systems over L, and write $\mathbf{A}$ for the poset $\langle A, \leq \rangle$. By a *maximal* (respectively,

0-*maximal*) element of $\mathbf{A}$, we mean a system $\mathscr{S} \in A$ such that, for every non-trivial $\mathscr{S}' \in A$, $\mathscr{S} \leq \mathscr{S}' \Rightarrow \mathscr{S} = \mathscr{S}'$ (respectively, $\mathscr{S} \leq \mathscr{S}' \Rightarrow \mathscr{S} \equiv_0 \mathscr{S}'$). ($\langle L, C \rangle$ is trivial if $C(\varnothing) = Fm$.) In other treatments of this subject, these two notions have been called "maximal" and "weakly maximal", respectively. See, for example [1].

Gathering all of this terminology together, we have the following corollary.

COROLLARY 16. *Let $\mathscr{S}$ be an algebraizable deductive system such that $\mathscr{S}^{\mathbf{Q}}$ is congruence modular and locally finite. If $\mathscr{S}$ is 0-maximal in $\mathbf{A}$, then $\mathscr{S}$ is maximal in $\mathbf{A}$.*

PROOF. Let $\mathscr{V} = \mathbf{H}(\mathscr{S}^{\mathbf{Q}})$ be the variety generated by $\mathscr{S}^{\mathbf{Q}}$. It is easy to see that $\mathscr{V}$ inherits both local finiteness and congruence modularity from $\mathscr{S}^{\mathbf{Q}}$.

We claim that $\mathscr{V}$ is a minimal variety. For suppose that $\mathscr{W}$ is a proper, non-trivial subvariety of $\mathscr{V}$. Define a deductive system $\mathscr{S}' = \langle L, C' \rangle$ by $C'(\Gamma) = C(\Gamma \cup \Theta(\mathscr{W}))$. Here, $\Theta(\mathscr{W})$ is the set of L-formulas corresponding to the identities of $\mathscr{W}$. $\mathscr{S}'$ is clearly an extension of $\mathscr{S}$, i.e., $\mathscr{S}' \geq \mathscr{S}$, so $\mathscr{S}' \in A$. But $\mathscr{S}' \not\equiv_0 \mathscr{S}$ since $C'(\varnothing) = C(\Theta(\mathscr{W})) \supseteq \Theta(\mathscr{W}) \supset \Theta(\mathscr{V}) = C(\varnothing)$. This contradicts the 0-maximality of $\mathscr{S}$.

Therefore, by Corollary 13, $\mathscr{V}$ is minimal as a quasivariety. Since $\mathscr{V} \supseteq \mathscr{S}^{\mathbf{Q}}$, we conclude that $\mathscr{V} = \mathscr{S}^{\mathbf{Q}}$. Suppose that $\mathscr{S}' \geq \mathscr{S}$. Then $\mathscr{S}'$ is algebraizable, and $\mathscr{S}'^{\mathbf{Q}} \subseteq \mathscr{S}^{\mathbf{Q}}$. Now it follows from the minimality of $\mathscr{S}^{\mathbf{Q}}$ that either $\mathscr{S}'^{\mathbf{Q}}$ is trivial, in which case $\mathscr{S}'$ is trivial, or else $\mathscr{S}' = \mathscr{S}$.

This last corollary may seem far less natural than our original problem. However, the fact of the matter is that our investigation of minimal varieties was motivated by a more general problem of algebraic logic (which happens to sound more natural than *its* universal algebraic equivalent). A deductive system $\mathscr{S}$ is *structurally complete* if, for every system $\mathscr{S}'$, $\mathscr{S} < \mathscr{S}' \Rightarrow \mathscr{S} \not\equiv_0 \mathscr{S}'$. (Intuitively: every new rule of inference yields new tautologies.) Seen in this light, Corollary 16 is a sufficient condition for structural completeness, and it was the study of the following algebraic equivalent that led us to the problem considered in this paper: we call a quasivariety $\mathscr{Q}$ *structurally complete* if and only if for every quasivariety $\mathscr{Q}'$, $\mathscr{Q}' \subset \mathscr{Q} \Rightarrow V(\mathscr{Q}') \subset V(\mathscr{Q})$.

References

[1] H. Andréka, I. Németi and I. Sain, 'Abstract Model Theoretic Approach to Algebraic Logic,' preprint, 1984.
[2] W. Blok and D. Pigozzi, *Algebraizable Logics*, Memoirs Amer. Math. Soc. **396**, 1989.

[3] R. Freese and R. McKenzie, *Commutator Theory for Congruence Modular Varieties*, London Mathematical Society Lecture Notes no. 125, Cambridge University Press, Cambridge, 1987.

[4] L. Henkin, D. Monk and A. Tarski, *Cylindric Algebras*, Part I, North-Holland, Amsterdam, 1971.

[5] B. Jónsson, 'Algebras whose congruence lattices are distributive,' *Math. Scand.* **21** (1967), 110–121.

[6] I. Németi, 'On varieties of cylindric algebras with applications to logic,' *Ann. Pure Appl. Logic* **36** (1987), 235–277.

[7] A. Szendrei, 'Idempotent algebras with restrictions on subalgebras,' *Acta Sci. Math.* **51** (1987), 251–268.

[8] A. Szendrei, 'Every idempotent plain algebra generates a minimal variety,' *Algebra Universalis* **25** (1988), 36–39.

[9] A. Szendrei, 'Demi-primal algebras,' *Algebra Universalis* **18** (1984), 117–128.

Iowa State University   University of California
Ames, Iowa 50011   Berkeley, California 94720
U.S.A.   U.S.A.