PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 2, October 1981

EQUATIONAL THEORIES WITH A MINORITY POLYNOMIAL

R. PADMANABHAN AND B. WOLK[1]

ABSTRACT. It is known that every finitely based variety of algebras with distributive and permutable congruences is one-based and those admitting a majority polynomial are two-based. In this note we prove two results, one similar to the above and the other in a completely opposite direction: (i) every finitely based variety of algebras of type $\langle 3 \rangle$ satisfying the two-thirds minority condition is one-based and (ii) for every natural number n, there exists a variety of algebras admitting even a full minority polynomial which is $(n + 1)$-based but not n-based. An application to the strict consistency of defining relations for semigroups is given.

Ever since the appearance of Mal′cev's now classical theorem characterizing the permutability of congruences in a variety, the Mal′cev polynomials have played a steadily increasing role in studying the equational problems of group-like or lattice-like algebras (see, for example, [1], [4], [5] and the thorough survey article [8]). A ternary polynomial $p(x, y, z)$ satisfying the two Mal′cev identities

$$(1) \qquad p(x, x, y) = p(y, x, x) = y$$

is called a "two-thirds minority" polynomial and it is called a minority polynomial if it further satisfies the third minority condition $p(x, y, x) = y$ as well. In contrast to the minority, there is the concept of a "majority polynomial" satisfying some or all of the identities

$$(2) \qquad p(x, x, y) = p(x, y, x) = p(y, x, x) = x.$$

Ternary polynomials satisfying the identities (1) or (2) or certain of their combinations have nice universal algebraic significances; thus while (1) is equivalent to the permutability of congruences, (2) is equivalent to the strongest type of congruence distributivity [2]. A particular combination of (1) and (2), viz. two-thirds minority and one-third majority, due to A. F. Pixley [7], is the strongest possible: it gives both the distributive and permutable congruence properties. In [5] it was shown that any finitely based variety of algebras with distributive and permutable congruences is one-based, and those admitting a majority polynomial are two-based. In this note, we prove two results: Every finitely based subvariety of algebras of type $\langle 3 \rangle$ satisfying the two-thirds minority identities is one-based and a completely opposite result for finitely based varieties of algebras admitting even a full minority polynomial. Finally, a mixture of majority and minority laws is of interest. The full

Received by the editors June 4, 1980.
1980 *Mathematics Subject Classification*. Primary 08B05.
[1]The research of both the authors was supported by a grant from NSERC of Canada (#A8215).

majority polynomial ($p(x, x, y) = p(x, y, x) = p(y, x, x) = x$) and the (1, 2) combination polynomial ($p(x, x, y) = p(y, x, y) = p(y, x, x) = y$) were both considered in [5]. The last possibility is the (2, 1) combination polynomial ($p(x, x, y) = p(y, x, y) = p(y, x, x) = x$), but the trivial polynomial $p(x, y, z) = y$ satisfies these identities.

1. Let **M** be the variety of all algebras of type $\langle 3\rangle$ in the basic ternary operation satisfying the two-thirds minority condition

$$p(x, x, y) = p(y, z, z) = y. \tag{3}$$

LEMMA 1. *In* **M**, *the validity of any finite set of identities is equivalent to that of a single identity.*

PROOF. Let $f = g$ be any identity and let x be a variable not occurring in $f = g$. Then it is clear that **M** satisfies $f = g$ iff **M** satisfies $p(f, g, x) = x$. Let $a(x_1, x_2, \ldots, x_n) = x_1$ and $b(y_1, y_2, \ldots, y_m) = y_1$ now be two identities of type $\langle 3\rangle$. It is clear that these two identities together imply

$$a(b(y_{11}, y_{12}, \ldots, y_{1m}), b(y_{21}, y_{22}, \ldots, y_{2m}), \ldots, b(y_{n1}, y_{n2}, \ldots, y_{nm})) = y_{11}.$$

Conversely, if **M** satisfies the above identity, then putting $y_{11} = y_{12} = \cdots = y_{1m}, \ldots, y_{n1} = y_{n2} = \cdots = y_{nm}$ and using the idempotency of p we get $a(y_{11}, y_{21}, \ldots, y_{n1}) = y_{11}$ and hence $b(y_{11}, y_{12}, \ldots, y_{1m}) = y_{11}$. Thus, modulo (1), any two identities, and hence any finite number of identities, can be equivalently expressed by one identity of the form $f(x_0, \ldots, x_n, w) = w$ where w is a variable. In what follows, we call the variables x_i dummy variables of f.

THEOREM 1. *Every finitely based subvariety of* **M** *is one-based.*

PROOF. If $f(x_0, x_1, \ldots, x_n, w) = w$ is the additional identity which defines the subvariety in question, then it is clear that it does satisfy the identity

$$fp(fp(x, x, y), fp(z, z, fw), w) = y \tag{3}$$

where fu is an abbreviation for $f(x_0, x_1, \ldots, x_n, u)$. Conversely, let us assume the validity of identity (3). We further assume that the set of dummy variables in the outermost f is disjoint from the remaining dummy variables in the inside f's.

Suppose x abbreviates $fp(a, a, fy)$. Then

$$fp(x, x, y) = fp(fp(a, a, fy), fp(a, a, fy), y) = fy \quad \text{by (3).}$$

Now, we see that substituting $fp(a, a, y)$ for x in (3) immediately yields

$$fp(fy, fp(z, z, fw), w) = y. \tag{4}$$

From the identities (3) and (4) we get

$$p(x, x, y) = y \tag{5}$$

and hence, in particular, p is idempotent. Also, by (4) and (5) we have

$$fp(fy, f^2w, w) = y. \tag{6}$$

Since p is idempotent and f is a p-polynomial, by identifying all the dummy variables in "fy" and "f^2w" and also y to say w, and using the idempotency of p several times we get $fw = w$ and, hence (6) reduces to $p(y, w, w) = y$ and that p is a two-thirds minority polynomial and moreover we have the identity $f(x_0, x_1, \ldots, x_n, w) = w$. This completes the proof of the theorem.

COROLLARY 1. *The property of a ternary polynomial $p(x, y, z)$ satisfying all the three minority identities*

$$p(x, x, y) = p(y, x, x) = p(x, y, x) = y \tag{7}$$

can be expressed by a single identity.

The above result follows, of course, from Theorem 1 by simply taking $p(x_0, w, x_1)$ for fw in the main identity (3) of that theorem. However, the following simple identity will do:

$$p(p(x, x, y), p(z, w, z), w) = y. \tag{8}$$

The minority polynomial is conceptually as nice and simple as, say, the majority polynomial. Both are expressible by a single identity (see Lemma 3 of [5]), and also, in presence of a majority polynomial, there is available a general method of reducing the validity of two identities to that of one (this result is due to K. A. Baker [1], see also Lemma 1 of [5]). But such a general method of reducing a set of n identities to $n - 1$ identities in general algebras does not exist in the presence of even a full minority polynomial.

For $n > 1$, let K_n be the variety of all algebras of type $\tau = \langle 3, 1, \ldots, 1\rangle$ with the fundamental operations $p(x, y, z), h_1(x), \ldots, h_n(x)$ satisfying the identities

$$p(x, x, y) = p(x, y, x) = p(y, x, x) = y, \tag{7}$$

$$h_1(x) = h_2(x) = \cdots = h_n(x) = x. \tag{9}$$

THEOREM 2. *This variety K_n is $(n + 1)$-based but not n-based.*

To show K_n is not n-based, we use 2^{n+1} algebras of type τ. Let $\langle F; +, *, 0, 1\rangle$ be the two-element field, and let $V = F^{n+1}$ be an $(n + 1)$-dimensional vector space over F. For each $v \in V$, $v = \langle v_0, v_1, \ldots, v_n\rangle$, define an algebra A_v of type τ over F by interpreting the operations of τ on F as follows:

$$\begin{aligned} p|_{A_v}(x, y, z) &= x + y + z + v_0, \\ h_i|_{A_v}(x) &= x + v_i \quad \text{for } i = 1, 2, \ldots, n. \end{aligned} \tag{10}$$

Then $A_v \in K_n$ iff $v = \langle 0, 0, \ldots, 0\rangle = 0$.

LEMMA 2. *Let $r = s$ be an identity of K_n. Then $\{v | r = s$ holds in $A_v\}$ is a subspace of V of dimension n.*

PROOF. (For example, $p(x, h_2(y), y) = x$ holds in A_v iff $v_0 + v_2 = 0$.) Note r and s are polynomials in the operations of τ, and the identity $r = s$ holds in A_0. Let r_v be the polynomial over F produced by the interpretation (10) of τ in A_v, and define s_v similarly. Then the various r_v's differ only in their constant terms. To describe this variation, define $h_0 = p$, and let $\mathbf{r} = \langle \mathbf{r}_0, \mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_n\rangle$ be a vector of length $n + 1$, where $\mathbf{r}_i$ = the number of occurrences of the operation h_i in the polynomial r. Let $\mathbf{r}'$ be the modulo 2 reduction of $\mathbf{r}$. So $\mathbf{r}'$ is a vector in V. Then it is easy to see that $r_v = r_0 + (\mathbf{r}' \cdot v)$, where $\cdot$ denotes the usual dot product of vectors in V. Similarly, $s_v = s_0 + (s' \cdot v)$.

Now $r_0 = s_0$, since $r = s$ holds in A_0. So $r_v - s_v = (\mathbf{r}' - \mathbf{s}') \cdot v$, using obvious meanings for "subtraction". This shows that $r = s$ holds in A_v iff $r_v = s_v$ iff v is orthogonal to the vector $\mathbf{r}' - \mathbf{s}'$. Since the set of all such vectors v forms a subspace of codimension 1, the lemma is proved.

PROOF OF THEOREM 2. Corollary 1 shows that K_n can be defined by the $n + 1$ identities of (8) and (9). So K_n is at most $(n + 1)$-based. If $\{r_i = s_i | i = 1, 2, \ldots, n\}$ are any n identities of K_n, let $V_i = \{v \in V | r_i = s_i \text{ holds in } A_v\}$. By Lemma 2, each V_i is a subspace of codimension 1. The intersection of n such subspaces has codimension at most n, and is therefore a nonzero subspace. This means that all n identities are true in some A_v, with $v \neq 0$. Since this A_v is not in K_n, these n identities do not define K_n. So K_n is not n-based.

2. An application to semigroups. Let $X = \{x_0, x_1, \ldots, x_n\}$ be an alphabet and let R be a set of defining relations over X. R is said to be *strictly consistent* if there is at least one nontrivial semigroup generated by X and satisfying the defining relations in R.

COROLLARY 2. *Let $X = \{x_0, x_1, \ldots, x_n\}$ and R any set of defining relations over X. If $|R| < n + 1$ then R is always strictly consistent.*

PROOF. Let $R = \{r_i(x_0, \ldots, x_n) = s_i(x_0, \ldots, x_n) | i = 1, \ldots, k,\ k < n + 1\}$ be not strictly consistent. Let us formally represent the generators x_i as mappings of F, the two-element field, thus

$$x_i \colon F \to F \quad \text{where } x_i(y) = h_i(y).$$

Now each semigroup word $r(x_0, x_1, \ldots, x_n)$ corresponds to a mapping $r(h_0, h_1, \ldots, h_n) \colon F \to F$ computed as per the composition of the word r. For each $i \in \{1, 2, \ldots, k\}$, define

$$S_i = \{v | A_v \vDash r_i = s_i\}$$

where now $r_i(h_0, h_1, \ldots, h_n) = s_i(h_0, h_1, \ldots, h_n)$ is an identity in the language of τ. By the lemma, each S_i is a subspace of V of dimension n. Hence,

$$\bigcap_{i=1}^{k} S_i = \{v | A_v \vDash r_i = s_i \text{ for all } i \in \{1, 2, \ldots, k\}\}$$

is a subspace of dimension $n + 1 - k$ and the collection of defining relations $R = \{r_i = s_i | i = 1, 2, \ldots, k\}$ will be strong enough not to be strictly consistent iff $\bigcap_{i=1}^{k} S_i = \{0\}$, the null space. This can happen iff $n + 1 - k = 0$ or $k = n + 1$ but we are given that $k < n + 1$. Hence, for any R with $|R| < n + 1$, there exists a nontrivial semigroup generated by n elements and satisfying all the k defining relations in R. Actually, this semigroup–represented as mappings–can easily be computed by noting that $A_v \vDash r = s$ iff $v \cdot (\mathbf{r} - \mathbf{s}) = 0$. This number $|X| - |R|$, known as the deficiency number, has been widely studied in group theory (see p. 93 of [3]).

References

1. K. A. Baker, *Finite equational bases for finite algebras in a congruence-distributive equational class*, Adv. in Math. **24** (1977), 207–243.

2. B. Jonsson, *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.

3. R. C. Lyndon and P. E. Schupp, *Combinational group theory*, Springer-Verlag, New York, 1977.

4. R. N. McKenzie, *On spectra and the negative solution of the decision problem for identities having a finite nontrivial model*, J. Symbolic Logic **40** (1975), 186–196.

5. R. Padmanabhan and R. Quackenbush, *Equational theories of algebras with distributive congruences*, Proc. Amer. Math. Soc. **41** (1973), 373–377.

6. R. Padmanabhan, *Equational theory of algebras with a majority polynomial*, Algebra Universalis **7** (1977), 273–275.

7. A. F. Pixley, *Distributivity and permutability of congruence relations in equational classes of algebras*, Proc. Amer. Math. Soc. **14** (1963), 105–109.

8. W. Taylor, *Equational logic*, Appendix 4 in G. Grätzer, *Universal algebra*, 2nd ed., Springer-Verlag, New York, 1979.

Department of Mathematics, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2