COLLOQUIUM MATHEMATICUM

VOL. XXII 1971 FASC. 2

A NOTE ON VARIETIES OF UNARY ALGEBRAS

BY

STANLEY BURRIS (WATERLOO, CANADA)

If G and G^* are two non-isomorphic (congruence) simple finite groups, then they generate distinct varieties (see [6], p. 166).

B. Jónsson has proved in [5] that the same result is valid for lattices. The following construction will show that this property fails to hold for unary algebras (for terminology see [3]).

Let $\langle G, \cdot \rangle$ be a multiplicative group and consider the left translation algebra $\mathfrak{A}(G) = \langle G, \mathfrak{F} \rangle$, where $\mathfrak{F} = \{f_a: a \in G, f_a(x) = ax\}$.

LEMMA 1. *A basis for the identities of* $\mathfrak{A}(G)$ *is given by* $\{f_a f_b = f_{ab}: a, b \in G\}$.

Proof. An immediate consequence of the observation that $f_{a_1} \dots f_{a_n} = f_{b_1} \dots f_{b_m}$ iff $a_1 \dots a_n = b_1 \dots b_m$.

An equivalence relation θ on G is *left compatible* if $\langle x, y \rangle \in \theta \Rightarrow \langle zx, zy \rangle \in \theta$ for all z in G (see [1]). It is easy to see that θ is left compatible iff θ [1] is a subgroup of G and the equivalence classes are precisely the left cosets of θ [1].

LEMMA 2. *θ is a congruence for $\mathfrak{A}(G)$ iff θ is left compatible with G.*

Proof. Straightforward.

For convenience of notation, if H is a subgroup of G, let $\mathfrak{A}(G)/H$ denote the algebra with the carrier G/H and with $f_a(bH) = abH$ $(b \in G)$ as fundamental operations (G/H denotes the set of left cosets). Also, define $N(G, H) = \bigcap \{\lambda H \lambda^{-1}: \lambda \in G\}$.

THEOREM. *A basis for the laws of $\mathfrak{A}(G)/H$ (where $H \neq G$) is given by*

$$\{f_a f_b = f_{ab}: a, b \in G\} \cup \{f_a = f_1: a \in N(G, H)\}.$$

Proof. In view of Lemma 1 we only need to determine the a, b in G such that $f_a = f_b$ in $\mathfrak{A}(G)/H$; but this is equivalent to $f_{b^{-1}a} = f_1$. If $f_a = f_1$ in $\mathfrak{A}(G)/H$, then $f_a(\lambda H) = \lambda H$ for all $\lambda \in G$, i.e. $a \in \bigcap \{\lambda H \lambda^{-1}: \lambda \in G\} = N(G, H)$, and conversely.

EXAMPLE. Let G be the alternating group on 5 elements, and let H and K be two maximal subgroups of different orders. Then $\mathfrak{A}(G)/H$

and $\mathfrak{A}(G)/K$ are simple and non-isomorphic, and since $N(G, H) = N(G, K) = \{1\}$, it follows from the Theorem that they generate the same variety.

PROBLEM 1. Does there exist a variety of semi-groups generated by each of two non-isomorphic simple finite semi-groups? (**P 704**).

Following a suggestion of Djokovic the author was able to conclude the existence of any given finite number of non-isomorphic simple finite unary algebras which generate the same variety (1) by examining the maximal subgroups of $PSL(2, 2^f)$ for suitable f (cf. [4], p. 213). However, it is easy to show that we cannot increase this to an infinite number for the following reasons. Let $\mathscr{V}$ be a variety of unary algebras generated by a finite algebra. Since congruence simple (and cardinality greater than two) implies at most one subalgebra, it follows that every congruence simple algebra in $\mathscr{V}$ would be a homomorphic image of the free algebra on one generator, or a two element algebra, and thus there could only be a finite number of congruence simple algebras in $\mathscr{V}$.

On the other hand, Comer has exhibited in [2] a variety of semi-groups which can be generated by any one of an infinite number of non-isomorphic subdirectly irreducible finite semi-groups.

PROBLEM 2. Does there exist an infinite number of non-isomorphic simple finite algebras which generate the same variety? (**P 705**).

The author would like to thank H. Crapo and D. Higgs for valuable comments on the topic of this paper.

Added in proof. T. Karnofsky (Berkeley) has announced positive result for the two problems; see Notices of the American Mathematical Society 17 (1970), p. 939.

---

(1) This generalizes Wille [7].

REFERENCES

[1] A. Clifford and G. Preston, *Algebraic theory of semi-groups*, Vol. 1, AMS, 1961.

[2] S. Comer, *Concerning a problem of B. Jónsson*, Notices of the American Mathematical Society 15 (1968), p. 788.

[3] G. Grätzer, *Universal algebra*, Princeton 1968.

[4] B. Huppert, *Endliche Gruppen I*, Berlin 1967.

[5] B. Jónsson, *Algebras whose congruence lattices are distributive*, Mathematica Scandinavica 21 (1967), p. 110–121.

[6] H. Neumann, *Varieties of groups*, Berlin 1967.

[7] R. Wille, *On a problem of B. Jónsson*, Notices of the American Mathematical Society, 1968, p. 647.

Reçu par la Rédaction le 29. 10. 1969

COLLOQUIUM MATHEMATICUM

VOL. XXII 1971 FASC. 2

REMARKS ON ALGEBRAS HAVING TWO BASES OF DIFFERENT CARDINALITIES

BY

J. DUDEK (WROCŁAW)

Let $\mathfrak{A} = (X; F)$ be an abstract algebra and let $S(\mathfrak{A})$ denote the set of all n such that in $\mathfrak{A}$ there exists an essentially n-ary algebraic operation, i.e, an operation depending on all its variables.

E. Marczewski has raised the following conjecture (see [1]): if $\mathfrak{A}$ contains two bases of different cardinalities, then $S(\mathfrak{A})$ contains all positive n (for the definition of bases see [1]). Observe that because of the existence of the trivial unary operation $e_1^1(x) = x$ there is $1 \in S(\mathfrak{A})$ for arbitrary $\mathfrak{A}$.

Narkiewicz [2] obtained some partial results connected with the conjecture. In particular, he proved that

(i) if $\mathfrak{A}$ contains two bases of different cardinalities, then $2 \in S(\mathfrak{A})$.

In this paper we prove some further results (Theorems 1, 2 and 3).

If $\mathfrak{A} = (X; F)$ is an abstract algebra, then by $I(\mathfrak{A})$ we denote an algebra $(X;\ I(F))$, where $I(F)$ is the set of all idempotent algebraic operations $f(x_1, \ldots, x_n)$, i.e., of all operations satisfying equality $f(x, x, \ldots, x) = x$. The algebra $I(\mathfrak{A})$ is called the *maximal idempotent reduct* of $\mathfrak{A}$.

Let $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_m\}$ be two bases of $\mathfrak{A}$ such that $m < n < \aleph_0$. It is easy to check that

$$\text{(ii)} \qquad \begin{aligned} f_i(g_1, g_2, \ldots, g_n)(x_1, x_2, \ldots, x_m) &= x_i \qquad (i = 1, 2, \ldots, m), \\ g_j(f_1, f_2, \ldots, f_m)(y_1, y_2, \ldots, y_n) &= y_j \qquad (j = 1, 2, \ldots, n), \end{aligned}$$

where f_i and g_j are some algebraic operations in $\mathfrak{A}$.

THEOREM 1. *If $\mathfrak{A}$ contains two bases of different cardinalities, then the set $S(I(\mathfrak{A}))$ is infinite.*

Proof. Consider the operations

$$\begin{aligned} F_i &= F_i(x_1^1, x_2^1, \ldots, x_m^1, x_1^2, x_2^2, \ldots, x_m^2, \ldots, x_1^n, x_2^n, \ldots, x_m^n) \\ &= f_i\big(g_1(x_1^1, x_2^1, \ldots, x_m^1),\ g_2(x_1^2, x_2^2, \ldots, x_m^2),\ \ldots,\ g_n(x_1^n, x_2^n, \ldots, x_m^n)\big), \end{aligned}$$

where f_i and g_j satisfy (ii). Obviously, all F_i are idempotent. Observe that for every $k = 1, 2, \ldots, n$ there exists an operation F_i depending on some variable $x^k_{i_0}$, where $1 \leqslant i_0 \leqslant m$, for otherwise there would exist k_0 such that no operation F_i would depend on $x_1^{k_0}, x_2^{k_0}, \ldots, x_m^{k_0}$, and hence the operation

$$g_{k_0}(x_1^{k_0}, x_2^{k_0}, \ldots, x_m^{k_0})$$
$$= g_{k_0}(F_1, F_2, \ldots, F_m)(x_1^1, \ldots, x_m^1, x_1^2, \ldots, x_m^2, \ldots, x_1^{k_0}, \ldots, x_m^{k_0}, \ldots, x_1^n, \ldots, x_m^n)$$

would be an algebraic constant, a contradiction with (ii).

Now we shall prove that among operations F_i there exists one depending on p variables, where $p \geqslant n/m$. In fact, if each F_i depends on less than n/m variables, then the set of variables on which the operations F_i depend will be of the cardinality less than $m(n/m) = n$ which gives a contradiction with the first part of the proof. Without loss of generality we may assume that m is the minimal cardinality of bases in $\mathfrak{A}$ and n is the next one. By a theorem of Marczewski (see [1]) numbers of elements of bases in $\mathfrak{A}$ form arithmetical progress $l_s = m + sr$, where $s = 0, 1, \ldots$, $r = n - m$. Let q be a natural number. Then there exists a base B_s such that $|B_s| = l_s$ and $l_s/m \geqslant q$, and among the operations F_i defined for the bases A and B_s there exists an operation depending on at least q' variables, where $l_s \cdot m \geqslant q' \geqslant l_s/m$. Because q was arbitrary, we get the thesis of Theorem 1.

From Theorem 1 and results of K. Urbanik (see [3]) we get

COROLLARY. *If $\mathfrak{A}$ is an algebra with two bases of different cardinalities, then $S(I(\mathfrak{A}))$ is of one of the following forms*: $\{1, 3, 5, \ldots\}$, $\{m, m+1, \ldots\}$, $\{1, 2, 3, \ldots, n\} \cup \{m, m+1, \ldots\}$, $\{1, 3, 5, \ldots\} \cup \{m, m+1, \ldots\}$.

THEOREM 2. *If $\mathfrak{A}$ contains two bases of different cardinalities, then there exists n_0 such that $2 \in S(\mathfrak{A})$ and $n \in S(\mathfrak{A})$ for all $n \geqslant n_0$.*

Proof. $2 \in S(\mathfrak{A})$ by (i). Consider $S(I(\mathfrak{A}))$. In view of the Corollary it remains to check the case $S(I(\mathfrak{A})) = \{1, 3, 5, \ldots\}$. But from [3] (Theorem 2, part 3, p. 139) it follows that $I(\mathfrak{A})$ is then a maximal idempotent reduct of a Boolean group, i.e., of a group satisfying $2x = 0$. This reduct can be considered as the algebra $(X; x_1 + x_2 + x_3)$, where $+$ is the group operation. Let $x \cdot y$ be an essentially binary operation which exists by (i). Then the operation $(x_1 + x_2 + \ldots + x_{2n-1}) \cdot x_{2n}$ is essentially $2n$-ary. In fact, because $+$ is commutative, it depends on all variables $x_1, x_2, \ldots, x_{2n-1}$ or on none of them. If it does not depend on x_{2n} or if it depends on none of the remaining variables, then the identification $x_1 = x_2 = \ldots = x_{2n-1} = x$ gives a contradiction with the assumption that the operation $x \cdot x_{2n}$ is essentially binary. Hence $S(\mathfrak{A}) = \{1, 2, 3, \ldots\}$.

THEOREM 3. *If $\mathfrak{A}$ contains two bases of different cardinalities and does not contain any algebraic constant, then*

$$S(I(\mathfrak{A})) \supseteq \{1, 2, \ldots, k\} \cup \{l, l+1, \ldots\}$$

for some k, l $(2 \leqslant k \leqslant l)$.

Proof. Consider the operations

$$H_i = H_i(x_1, x_2, \ldots, x_n) = f_i\big(\hat{g}_1(x_1), \hat{g}_2(x_2), \ldots, \hat{g}_n(x_n)\big),$$

where $\hat{g}(x) = g(x, x, \ldots, x)$.

Take the substitution

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}, \qquad 1 \leqslant i_k \leqslant 2, \; k = 1, 2, \ldots, n,$$

and put

$$H_i(\sigma)(x_1, x_2) = H_i(x_{i_1}, x_{i_2}, \ldots, x_{i_n}), \qquad \text{where } i = 1, 2, \ldots, m.$$

We shall prove that among operations $H_i(\sigma)$ there exists an essentially binary one. The operations H_i are idempotent by (ii).

Suppose to the contrary that all $H_i(\sigma)$ are trivial. This means that $H_i(\sigma) = H_i(\sigma)(x_1, x_2) = x_{\varepsilon(\sigma, i)}$, where $\varepsilon(\sigma, i) \in \{1, 2\}$. Define the mapping

$$\varphi(\sigma) = \big(\varepsilon(\sigma, 1), \varepsilon(\sigma, 2), \ldots, \varepsilon(\sigma, m)\big).$$

Let $\varphi(\sigma_1) = \varphi(\sigma_2)$. Then $\varepsilon(\sigma_1, k) = \varepsilon(\sigma_2, k)$ for $k = 1, 2, \ldots, m$. Putting

$$\sigma_1 = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \quad \text{and} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix},$$

we have

$$H_k(\sigma_1)(x_1, x_2) = H_k(\sigma_2)(x_1, x_2)$$

and

$$\begin{aligned}\hat{g}_k(x_{i_k}) &= g_k\big(H_1(\sigma_1)(x_1, x_2), \ldots, H_m(\sigma_1)(x_1, x_2)\big) \\ &= g_k\big(H_1(\sigma_2)(x_1, x_2), \ldots, H_m(\sigma_2)(x_1, x_2)\big) = \hat{g}_k(x_{j_k}).\end{aligned}$$

Hence $i_k = j_k$ for $k = 1, 2, \ldots, n$, because $\mathfrak{A}$ does not contain any algebraic constant. Thus we see that φ is one-to-one but it is impossible, because there does not exist a one-to-one mapping of the 2^n-element set into 2^m-element set. Thus we infer that in $I(\mathfrak{A})$ there exists an essentially binary operation and our theorem easily follows from the corollary.

Remark. The idea of the proof of Theorem 3 is similar to that of the proof of Theorem 1 in [2].

REFERENCES

[1] E. Marczewski, *Independence in abstract algebras. Results and problems*, Colloquium Mathematicum 14 (1969), p. 169–188.

[2] W. Narkiewicz, *Remarks on abstract algebras having bases with different number of elements*, ibidem 15 (1966), p. 11–17.

[3] K. Urbanik, *On algebraic operations in idempotent algebras*, ibidem 13 (1965), p. 129–157.

Reçu par la Rédaction le 24. 11. 1969