An Application of Matrix Theory to a Problem in Universal Algebra*

N. S. MENDELSOHN
University of Manitoba
Winnipeg, Manitoba, Canada

Communicated by Alan J. Hoffman

1. INTRODUCTION

This paper gives an example of the application of matrix theory to a problem in universal algebra. It is motivated by some work of Trevor Evans [1] and D. E. Knuth (private communication and [2]).

To describe the most general algebra in which we are interested, we shall use prefix, bracket-free, notation. For readers unfamiliar with prefix bracket-free notation the following remarks will help clarify the idea. Traditionally, binary operators such as $+$, $\cdot$, etc. are in what is now called "infix" notation, e.g., $a \cdot b$, $a + b$ have the operators appear between the elements. In prefix notation an operator would appear to the left of the elements on which it operates. When all operators appear on the left it is unnecessary to use brackets provided only we know the degree of each operator (i.e., whether it is unary, binary, ternary, etc.). For example, if we write f_1ab instead of $a \cdot b$ and f_2ab instead of $a + b$, the associative law $a(bc) = (ab)c$ becomes $f_1af_1bc = f_1f_1abc$, while the distributive law $a(b + c) = ab + ac$ becomes $f_1af_2bc = f_2f_1abf_1ac$.

We define an algebra A as follows: $A = \langle S, f_1, f_2, \ldots, f_{n-1} \rangle$, where S is a finite set and $f_1, f_2, \ldots, f_{n-1}$ are binary operators on S (here we use prefix bracket-free notation, e.g., f_ixy) and satisfying the following $(n-1)^2$ identities,

$$f_if_jabf_jbc = \lambda_{i+j}, \qquad i, j = 1, 2, \ldots, n-1, \tag{1.1}$$

* Dedicated to Professor A. M. Ostrowski on his 75th birthday.

Linear Algebra and Its Applications 1, 471–478 (1968)

where

$$\lambda_{i,j} = \begin{cases} f_{i+j}ab & \text{if } i+j \leqslant n-1, \\ b & \text{if } i+j = n, \\ f_{i+j-n}bc & \text{if } i+j > n. \end{cases}$$

It can be shown that

(1) the cardinality of $S = k^n$ where k may be an arbitrary positive integer;

(2) the set $\{f_i ax \mid x \in S\}$ has cardinality k;

(3) each operator has the same idempotents and the number of such idempotents is k (here b is an idempotent of f_i if $f_i bb = b$).

These results can be proved by using standard results on eigenvalues of a certain matrix. The first two of them can easily be obtained by using simple algebraic arguments. However, the author knows of no way in which to obtain the third result without the use of matrix theory. In fact, if we do not insist on the finiteness of S, and instead examine the free algebra with the given identities, we can show that such a system has no idempotents. A proof of this fact will be sketched at the end. There is no apparent way, other than by the intervention of matrices, in which the finiteness of S can be exploited to yield the idempotents.

2. MOTIVATION

Trevor Evans was interested in universal algebras having a spectrum $\{1^n, 2^n, 3^n, 4^n, \ldots\}$. (The spectrum of a universal algebra is the set of integers $\{n_1, n_2, \ldots, n_i, \ldots\}$ for which there are models in which S contains n_i elements, $i = 1, 2, \ldots$.) A possible way of constructing such an algebra is the following. Let M be a set of k elements and let S be the cartesian product of n copies of M. Evans and his students then defined a single operator x on S by means of the definition

$$(a_1, a_2, \ldots, a_n) \times (b_1, b_2, \ldots, b_n) = (a_n, b_1, b_2, \ldots, b_{n-1}).$$

By finding the correct equational identities they were able to show that the only models were precisely this multiplication of n-tuples which solves

the spectrum problem. Here we make a slight change. We define $n-1$ operators $f_1, f_2, \ldots, f_{n-1}$ by

$$f_i(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_{i+1}, a_{i+2}, \ldots, a_n, b_1, b_2, \ldots, b_i).$$

It is easily verified that the $(n-1)^2$ identities (1.1) are satisfied by this model of n-tuples. However, our axioms (1.1) are satisfied by models other than the above defined products of n-tuples. In fact, it can be shown that the models of (1.1) are precisely the set of directed graphs in which between any two points there is precisely one directed path of length n. In the next section, for simplicity of exposition, we shall give the complete argument for the case $n = 3$.

3. THE CASE $n = 3$

We now use the more usual "infix" notation. Let $A = \langle S, \cdot\ , * \rangle$ where S in a finite set and $x \cdot y$, $x * y$ are two binary operators on S, which satisfy the four identities

$$(a \cdot b) \cdot (b \cdot c) = a * b, \tag{3.1}$$

$$(a \cdot b) * (b \cdot c) = b, \tag{3.2}$$

$$(a * b) \cdot (b * c) = b, \tag{3.3}$$

$$(a * b) * (b * c) = b \cdot c. \tag{3.4}$$

A model of these identities can be obtained as follows. Let G be a directed graph with a set V of vertices, such that between any two of the vertices u and v there is a unique directed path

$$u \to x \to y \to v$$

of length 3. Since x and y are uniquely determined by u and v we may define the two products $u \cdot v = x$ and $u * v = y$. Let a, b, c be any three (not necessarily distinct) vertices. Consider the paths

$$a \to a \cdot b \to a * b \to b \to b \cdot c \to b * c \to c.$$

Using the fact that the paths from $a \cdot b$ to $b \cdot c$ and $a * b$ to $b * c$ are of length 3 it follows immediately that the identities (3.1), (3.2), (3.3), (3.4) all hold.

We now show that the converse holds, namely, that if $A = \langle S, \cdot * \rangle$ satisfies (3.1), (3.2), (3.3), (3.4) then we can construct a directed graph with the vertices being the elements of the set S, and such that there is a unique directed path of length 3 between any two vertices of S.

In fact, if $x, y \in S$ introduce an edge from x to y $(x \to y)$ iff there is an element $z \in S$ such that $y = x \cdot z$.

With this definition we now prove the following lemmas.

LEMMA 1. $x \cdot k \to x * k$.

Proof. Consider the expression

$$\{(a * x) * (x * k)\} \cdot \{(x * k) * b\}.$$

This can be reduced by (3.3) and by (3.4). Equating these reductions we obtain

$$(x \cdot k) \cdot \{(x * k) * b\} = x * k. \tag{3.5}$$

Hence $x \cdot k \to x * k$.

LEMMA 2. $x * k \to k$.

Proof. $\{(x \cdot k) \cdot (k \cdot a)\} \cdot \{(k \cdot a) \cdot b\} = (x * k) \cdot \{(k \cdot a) \cdot b\}$ by (3.1). Also $\{(x \cdot k) \cdot (k \cdot a)\} \cdot \{(k \cdot a) \cdot b\} = (x \cdot k) * (k \cdot a) = k$ by (3.1) and (3.2). Hence

$$(x * k) \cdot \{(k \cdot a) \cdot b\} = k. \tag{3.6}$$

Hence $(x * k) \to k$.

LEMMA 3. *If $y = x \cdot k$ there exists an element l such that $x = l * y$.*

Proof. $\{(a * (d * x)\} * \{(d * x) * (x * k)\} = \{a * (d * x)\} * (x \cdot k)$ by (3.4). Again $\{a * (d * x)\} * \{(d * x) * (x * k)\} = (d * x) \cdot (x * k) = x$. Hence

$$\{a * (d * x)\} * (x \cdot k) = x. \tag{3.7}$$

Putting $l = a * (d * x)$ we have $(l * y) = x$.

LEMMA 4. $a \cdot [\{(a \cdot b) \cdot c\} \cdot d] = a \cdot b.$ (3.8)

Proof. Reduce the expression

$$\{(x \cdot a) * (a \cdot b)\} \cdot \{[(a \cdot b) \cdot c] \cdot d\}$$

in two ways by the use of (3.2) and by the use of (3.6), obtaining

$$a \cdot [\{(a \cdot b) \cdot c\} \cdot d] = a \cdot b.$$

COROLLARY. *Using a dual argument we obtain*

$$[a * \{b * (c * d)\}] * d = c * d. \tag{3.9}$$

THEOREM. *Given a, b any two elements in S, there is exactly one directed path of length 3 from a to b.*

Proof. By definition and by Lemmas 1 and 2 $a \to a \cdot b \to a * b \to b$. Hence there is at least one path. Suppose that there were a second path $a \to l \to f \to b$. Here $l = a \cdot x$, $f = (a \cdot x) \cdot y$, and $b = \{(a \cdot x) \cdot y\} \cdot z$. Hence $a \cdot b = a \cdot [\{(a \cdot x) \cdot y\} \cdot z] = a \cdot x$ by (3.8). Hence $l = a \cdot b$. Dually, $f = a * b$.

Having established the correspondence between the algebraic systems satisfying (3.1), (3.2), (3.3), (3.4) and directed graphs with exactly one path of length 3 between any two of its vertices we are able to use matrix theory to obtain important information about our algebraic system.

Let $A = \langle S, \cdot\, * \rangle$ together with axioms (3.1), (3.2), (3.3), (3.4) and let G be the corresponding graph whose vertices are the elements of S and let B be the adjacency matrix of this graph. Here, B is a matrix whose rows and columns are indexed by the elements of S and whose entries are exclusively 0 and 1, the entry in the xth row and yth column being 1, iff $x \to y$. Then $B^3 = J$ where J is the matrix all of whose entries are 1. Let S contain m elements. Then B and J are square matrices of order m. The matrix J has eigenvalues m with multiplicity 1, and 0 with multiplicity $m - 1$. Now from $BJ = JB(= B^4)$ it follows that each row sum and each column sum of B has the same value. Let each row and each column of B contain k 1's. Then B has eigenvalues $k, 0, 0, 0, 0, \ldots, 0$. Hence $k = m^{1/3}$. This implies that S has k^3 elements. It also implies that the sets

$$R(a) = \{a \cdot x | x \in S\} \qquad \text{and} \qquad R^*(a) = \{y * a | y \in S\}$$

all have cardinality k.

Furthermore, tr $B = k$ since it is the sum of the characteristic roots. This means that B has exactly k 1's along its main diagonal. A place along the main diagonal of B where an entry 1 occurs corresponds to an element $b \in S$ such that $b = b \cdot x = y * b$ for some x and y.

We now show that $b = b \cdot x$ for some x iff $b = b \cdot b$. It is only necessary to prove $b = b \cdot x$ implies $b = b \cdot b$. From (3.8), $b \cdot x = b \cdot [\{(b \cdot x) \cdot x\} \cdot x]$, from which it follows $b = b \cdot \{(b \cdot x) \cdot x\} = b \cdot (b \cdot x) = b \cdot b$. It is also trivial that $b = b \cdot b$ iff $b = b * b$. This follows from (3.2) and (3.3) with a and c both replaced by b. Hence the system $A = \langle S, \cdot, * \rangle$ has exactly k idempotents, the same elements being idempotent under both operations.

It is clear that this type of argument could be extended in several ways. We could use each of the three concepts, graph, algebraic system, adjacency matrix to obtain information relevant to the other two. In a private communication D. E. Knuth has shown the author several results concerning the matrix equation $B^2 = J$ by exploiting similar ideas.

4. THE WORD PROBLEM

If we remove the finiteness condition on S, the resultant free algebra has a solvable word problem. This word problem has been solved for the author by machine computation by D. E. Knuth using the method described in [2]. The interest in the solution of the word problem is twofold. First, it is relatively complicated in form and hence illustrates the usefulness of a machine solution. Second, it yields a trivial proof of the fact that a free algebra with our given identities has no idempotents and, as a result, shows the value of the matrix formulation for the finite case which yields the existence and the number of the idempotents.

We sketch the idea of the proof here. First, a number of identities are established. Second, each of these identities will be considered as one-way replacements. For instance, the identity $(a \cdot b) \cdot (b \cdot c) = a * b$ will be written as $(a \cdot b) \cdot (b \cdot c) \rightarrow a * b$. A replacement in a word using this identity will mean that if a word has a subword of the form $(a \cdot b) \cdot (b \cdot c)$ then this subword will be replaced by $a * b$. We now list a set of 30 replacements.

$(a \cdot b) \cdot (b \cdot c) \rightarrow a * b$ $\qquad$ $(c * b) * (b * a) \rightarrow b \cdot a$

$(a \cdot b) * (b \cdot c) \rightarrow b$ $\qquad$ $(c * b) \cdot (b * a) \rightarrow b$

$a \cdot ((a * b) \cdot c) \to a \cdot b$

$a * ((a * b) \cdot c) \to a * b$

$a \cdot ((a \cdot b) * c) \to a \cdot b$

$a * ((a \cdot b) * c) \to (a \cdot b) \cdot c$

$(a * b) \cdot ((b \cdot c) \cdot d) \to b$

$(a * b) * ((b \cdot c) \cdot d) \to b \cdot c$

$(a \cdot (b \cdot c)) \cdot (b * c) \to a * (b \cdot c)$

$(a \cdot (b \cdot c)) * (b * c) \to b \cdot c$

$a \cdot (((a \cdot b) \cdot c) \cdot d) \to a \cdot b$

$a * (((a \cdot b) \cdot c) \cdot d) \to (a \cdot b) \cdot c$

$(a \cdot b) \cdot (((a * b) \cdot c) \cdot d) \to a * b$

$(a \cdot b) * (((a * b) \cdot c) \cdot d) \to (a * b) \cdot c$

$(a * (b \cdot c)) \cdot ((b * c) \cdot d) \to b \cdot c$

$(c * (b \cdot a)) * a \to b * a$

$(c * (b \cdot a)) \cdot a \to b \cdot a$

$(c \cdot (b * a)) * a \to b * a$

$(c \cdot (b * a)) \cdot a \to c * (b * a)$

$(d * (c * b)) * (b \cdot a) \to b$

$(d * (c * b)) \cdot (b \cdot a) \to c * b$

$(c \cdot b) * ((c * b) * a) \to (c * b) \cdot a$

$(c \cdot b) \cdot ((c * b) * a) \to c * b$

$(d * (c * (b * a))) * a \to b * a$

$(d * (c * (b * a))) \cdot a \to c * (b * a)$

$(d * (c * (b \cdot a))) * (b * a) \to b \cdot a$

$(d * (c * (b \cdot a))) \cdot (b * a) \to c * (b \cdot a)$

$(d * (c \cdot b)) * ((c * b) \cdot a) \to c * b$

We shall say that a word W is irreducible if it contains no subword of any of the 30 forms which appear on the left-hand side of these replacements. Otherwise we say that W is reducible. If a word W is reducible we can form a sequence $W \to W_1 \to W_2 \to \cdots \to W_t$ where at each stage a subword having the form of the left side of one of our 30 replacements is replaced by the corresponding word on the right side. It is clear that after finitely many steps the word W_t is irreducible, since each replacement reduces the length of a word. Now the following properties can be established (we omit the proof but the reader can get the idea by reading [2]). Two irreducible words are equal if and only if they are identical. Hence, since any word can be transformed to an irreducible word, the word problem is solved.

With our solution of the word problem it is now easy to show that the free algebra on any number of generators satisfying identities (3.1), (3.2), (3.3), (3.4) has no idempotents. For if β is such an idempotent, we may assume without loss of generality that β is irreducible. Now $\beta \cdot \beta$ is irreducible unless $\beta = w_1 \cdot w_1$ or $\beta = w_1 * w_1$. This can easily

be checked by examination of the left side of each of the 30 replacements. We consider only the case where $\beta = w_1 \cdot w_1$ with $w_1 \cdot w_1$ irreducible (the argument for the case $\beta = w_1 * w_1$ is similar). Hence $\beta \cdot \beta = (w_1 \cdot w_1) \cdot (w_1 \cdot w_1) = w_1 * w_1$. Now $w_1 * w_1$ is irreducible unless $w_1 = w_2 \cdot w_2$ or $w_1 = w_2 * w_2$. But in either of these cases it follows that $w_1 \cdot w_1$ is irreducible, a contradiction. Hence if $\beta \cdot \beta = \beta$ we obtain $w_1 \cdot w_1 = w_1 * w_1$ with both sides irreducible. This contradicts the fact that two distinct irreducible words are unequal. Hence, there are no idempotents.

REFERENCES

1 T. Evans, Products of points—some simple algebras and their identities, *Amer. Math. Monthly* **74(1967)**, 362–372.

2 D. E. Knuth and P. B. Bendix, Simple word problems in universal algebras, to appear in *Proc. Conf. on Computational Problems in Abstract Algebra, Oxford, England, 1967.*

Received April 1, 1968