UNARY ALGEBRAS

JOHN G. MARICA AND STEVEN J. BRYANT

This paper is concerned with algebraic systems composed of a nonempty set A and a single unary operation on A; i.e., a function on A into A, usually denoted by $'$. Such a system is called a unary algebra.

Our main objective is to give a proof of the following theorem: If A and B are two finite unary algebras and A^2 is isomorphic to B^2, then A is isomorphic to B.[1] In this statement, A^2 means the Cartesian product of the algebra A with itself. In addition to this result, we prove some basic structure theorems for unary algebras, and cancellation theorems for some classes of unary algebras. In § 7 we list some counter examples which indicate limitations on the generalization of these results to infinite algebras.

Most of the definitions and theorems were suggested by the graphs of unary algebras and should be easily understood in this context. The graphs are obtained by joining each element to its "prime" or "successor" by a directed line segment. Theorems, equations, definitions, etc. are numbered consecutively in each section.

1. Notation and general theorems.

We shall not distinguish notationally between an algebra and the set of elements of the algebra, and unless it is essential to do otherwise, we shall use $'$ to denote the operation in all of the algebras discussed. In general, upper case letters will denote algebras, lower case letters will denote elements. Brackets and parentheses are used in several senses, but for p, q integers (p, q) and $[p, q]$ will always denote the g.c.d. and l.c.m., respectively, of p and q.

1.1. DEFINITION. If $A \subset B, A \neq 0, B$ a unary algebra, and A is closed under $'$, i.e., $A' \subset A$, then A will be called a subalgebra of B.

1.2. LEMMA. *If F is a family of subalgebras of A, then $\bigcup F$ is a subalgebra of A, and if $\bigcap F \neq \phi$, then $\bigcap F$ is a subalgebra of A.*

The proof is immediate.

1.3. DEFINITION. If A and B are unary algebras and $A \cap B = \phi$ then $A \cup B$ is the algebra formed from $A \cup B$ by applying the operation of A to elements of A and the operation in B to elements of B.

Received April 7, 1959, in revised form February 2, 1960. To be presented before the Amer. Math. Soc., Monterey, California, April 18, 1959

[1] This problem was mentioned by Tarski in a course taken by one of the authors during 1951.

1.4. DEFINITION. $A \times B$ is the Cartesian product of A and B, i.e., the algebra formed from the Cartesian product of the sets A and B by defining the operation componentwise.

1.5. THEOREM. $A \times (B \cup C) \sim A \times B \cup A \times C$.

The proof is immediate.

1.6. DEFINITION. If $x \in A$ we define $x^0 = x$, and for $n > 0, x^n = (x^{n-1})'$. Thus, $x^1 = x', x^2 = (x')'$, etc.

1.7. DEFINITION. x is called a cyclic element of A if $x^a = x$ for some $n > 0$.

1.8. DEFINITION. $A/k = \{x : x \in A$ and x^k is cyclic$\}$. In particular, $A/0$ is the set of all cyclic elements of A.

It is easily seen that unless A/k is empty it is a subalgebra of A.

1.9. DEFINITION. If x, y are in A then we say x is connected to y if and only if for some n, m $x^n = y^m$.

This relation is an equivalence relation (in fact, a congruence relation) and we have:

1.10. DEFINITION. The equivalence classes with respect to the relation of 1.9 are called the components of A, the class to which x belongs being written $C(x)$.

If an algebra has only one component we call it connected. The components are disjoint subalgebras and an algebra is completely characterized by the set of its components. Formally, we have

1.11. THEOREM. *If A, B are unary algebras then $A \sim B$ if and only if the components of A are pairwise isomorphic to the components of B.*

The proof is obtained by defining the isomorphism $f: A \sim B$ as the union of the isomorphisms on the components; and conversely, given f, f restricted to each of the components of A yields an isomorphism onto a component of B. In general, if a sequence of algebras is pairwise isomorphic with another sequence, in some order, we shall write $\{A_i\} \sim \{B_j\}$.

Suppose that A and B are unary algebras, $x \in A$ and $y \in B$, $f: A \sim B$, (that is, f is an isomorphism of A onto B) and $f(x) = y$. If x^r is cyclic, and hence for some p $x^{r+p} = x^r$, then y satisfies the same equation. It follows from this that the image of A/k under f must be B/k, the result holding for all k.

If C and D are unary algebras, $z \in C, w \in D, z^{r+p} = z^r$, and $w^{r+t} = w^r$, then in $C \times D$, with $q = [p, t]$ we have $(z, w)^{r+q} = (z, w)^r$. We collect these results in

1.12. THEOREM. *If $f\colon A \sim B$ then $f\colon A/k \sim B/k$. Moreover, for any C, D $C/k \times D/k \sim (C \times D)/k$.*

In particular, this shows that isomorphisms send the cyclic part of one algebra onto the cyclic part of the image. This fact will be used frequently in the remainder of the paper

2. The cyclic case.

Let us now restrict our attention to finite algebras and, in fact, to those finite algebras in which every element is cyclic. We call these cyclic algebras, and a component of a cyclic algebra, a cycle.

It is evident that a cyclic is characterized by the number of its elements, one with p elements being called a p-cycle. It is also clear that a cyclic algebra is determined up to isomorphism by the number of p-cycles for $p = 1, 2, \cdots$. We now want to show directly that for cyclic algebras $A^2 \sim B^2$ implies $A \sim B$.

If x is cyclic then by Definition 1.7 $x^n = x$ for some n, let us write $o(x)$ for the smallest such n and call this the order of x. With A and B cyclic let a_i, b_i, c_i, and d_i be the number of elements of order i in A, B, A^2 and B^2 respectively. Then Lemma 2.1, which follows, is evident, and Lemma 2.2 is quickly obtained by counting, using the fact that $o(x) = r$ and $o(y) = s$ implies $o(x, y) = [r, s]$.

2.1. LEMMA. *$A \sim B$ if and only if for each i $a_i = b_i$.*

2.2. LEMMA. *$c_n = 2 \sum a_i a_j + a_n^2$, in which the sum is extended over all pairs (i, j) with $i < j$ and $[i, j] = n$.*

Suppose now that $A^2 \sim B^2$ and hence for each i, $c_i = d_i$. If A is not isomorphic to B then there is a smallest n for which $a_n \neq b_n$. We have always:

$$c_n = 2 \sum_{\substack{i<j\\ [i,j]=n}} a_i a_j + a_n^2 = 2 \sum_{\substack{i<j<k\\ [i,j]=n}} a_i a_j + 2 \sum_{\substack{i\mid n\\ i\neq n}} a_i a_n + a_n^2$$

and similarly for d_n, since $j = n$ and $[i, j] = n$ implies $i \mid n$. From this we obtain

$$2 \sum_{\substack{i\mid n\\ i=n}} a_i a_n + a_n^2 = 2 \sum_{\substack{i\mid n\\ i\neq n}} b_i b_n + b_n^2$$

since $a_i = b_i$ for any $i < n$. Hence

$$a_n[2 \sum_{\substack{i\mid n\\ 1\neq n}} a_i] + a_n^2 = b_n[2 \sum_{\substack{i\mid n\\ i\neq n}} b_i] + b_n^2 \,.$$

But the expressions in brackets are the same since $i < n$ and from this it follows readily that $a_n = b_n$ which is a contradiction. We have shown

2.3. THEOREM. *If A and B are finite cyclic algebras and $A^2 \sim B^2$ then $A \sim B$.*

We do not have cancellation even for finite cyclic algebras (see § 7).

3. Ordering.

In § 2 we have seen that the cyclic part of an algebra is well behaved, with respect to the square root problem, and we now turn to the noncyclic part. Consider the class of unary algebras defined by:

3.1. DEFINITION. A unary algebra A will be called basic if it is connected, has exactly one cyclic element, and for each $k \geqq 0$ A/k is finite. $\boldsymbol{B}$ denotes the class of basic algebra.

Notice that in a basic algebra there is an idempotent element, namely the single cyclic element. The rest of this section is devoted to the ordering of $\boldsymbol{B}$ in a useful way; the procedure is somewhat complicated and we have several preliminary definitions.

Suppose $A \in \boldsymbol{B}$ and $x \in A$, let $P(x)$ be the set of all elements of A which precede x; i.e.,

3.2. DEFINITION. $P(x) = \{y : y \in A \text{ and for some } n, y^n = x\}$.

This set of elements can be turned into a basic algebra by changing the definition of x', setting $x' = x$, and leaving everything else unchanged. The resulting algebra will also be called $P(x)$, and if x is the cyclic element of A, $P(x) = A$.

If $x \in A$, $A \in \boldsymbol{B}$, and a is the cyclic element of A then in view of the connectivity of A we may make

3.3 DEFINITION. $\deg(x) =$ the smallest integer n such that $x^n = a$.

Notice that for $A \in \boldsymbol{B}$, A/k is the subalgebra of A consisting of elements with degree less than or equal to k.

3.4. DEFINITION. If A is finite $h(A) = \max\{\deg(x) : x \in A\}$.

3.5. DEFINITION. For $A \in \boldsymbol{B}$, the width of $A = w(a) =$ the number of elements of degree 1.

3.6. DEFINITION. $[A] = \{P(x) : \deg(x) = 1 \text{ and } x \in A$.

$[A]$ is a collection of basic algebras and as mentioned after 1.11 we shall write $[A] \sim [B]$ when the elements of these sets are pairwise isomorphic.

3.7. THEOREM. *$A \sim B$ if and only if $[A] \sim [B]$.*

The proof of this should offer no difficulty since the members of $[A]$ are disjoint.

If A and B are in $\boldsymbol{B}$ then $A/0 \sim B/0$ since each has only a single element. The proof of the following theorem is included in § 8, but the theorem is probably not surprising.

3.8. THEOREM. *If A and B are in $\boldsymbol{B}$ and for each $k \geqq 0$ $A/k \sim B/k$ then $A \sim B$.*

In view of 3.7 we may make the following

3.9. DEFINITION. If A is not isomorphic to B, $e(A, B)$ is the largest integer for which $A/e \sim B/e$.

If A is not isomorphic to B and $e(A,B) = 0$ then $w(A) < w(B)$ or conversely; we order A, B accordingly. If $e(A, B) = 1$ then $w(A) = w(B)$ and $[A]$ and $[B]$ have the same length, but $[A/2] \not\sim [B/2]$. Each member of these sets is an algebra of height $\leqq 1$ and the collection of algebras of height $\leqq 1$ is ordered as above. We may then arrange the collections $[A/2]$, $[B/2]$ in nondecreasing order and compare them lexicographically. Continuing this process yields an ordering of $\boldsymbol{B}$.

The following lemma, together with 3.12 and 3.13 is devoted to a precise statement and proof of the preceding remarks. In the lemma, A and B are in $\boldsymbol{B}$ and the members of $[A]$ and $[B]$ will be assumed ordered by a relation R. We write $[A][R][B]$ to mean that $[A]$ is length-R-lexicographically less than $[B]$ in the following sense:

(i) $[A]$ is shorter than $[B]$, or

(ii) length $[A] =$ length $[B]$ and $[A]$ is lexicographically less that $[B]$ when both are regarded as nondecreasing sequences relative to R (i.e., the members of $[A]$ are indexed so that $A_i \sim A_{i+1}$ or $A_i R A_{i+1}$ for $A_i \in [A]$).

To simplify matters we write $=$ instead of $\sim$.

3.10. LEMMA. *Let R_k, $k \geqq 0$, be a relation satisfying:*

(i) *$(A, B) \in R_k$ implies $e(A, B) \leqq k$.*

(ii) *If $e(A, B) \leqq k$ then either $(A, B) \in R_k$ or $(B, A) \in R_k$ and not both.*

(iii) *$(A, B) \in R_k$ and $(B, C) \in R_k$ implies $(A, C) \in R_k$.*

(iv) *If $e(A, B) \leqq k$, $(A, B) \in R_k$ if and only if*

$$[A/e(A, B) + 1][R_k][B/e(A, B) + 1] .$$

Then there is a unique relation R_{k+1} satisfying the same conditions (with k replaced by $k + 1$) and containing R_k.

Proof. We show first that such an extension is unique. Let (A, B) be in R_{k+1}; then $e(A, B) \leqq k + 1$, and by (iv),

$$[A/e(A, B) + 1][R_{k+1}][B/e(A, B) + 1] .$$

If A_i is in $[A/e(A, B) + 1]$ then $h(A_i) \leqq k + 1$, so if $A_i \neq A_j$, $e(A_i, A_j) \leqq k$ and similarly for $e(B_i, B_j)$ and $e(A_i, B_j)$. This means that $[R_k]$ can be applied. But R_{k+1} contains R_k hence $[R_{k+1}]$ and $[R_k]$ must agree for these sequences and it follows that R_{k+1} is unique.

We now define R_{k+1} by:

3.11. DEFINITION. $R_{k+1} = \{(A, B) : e(A, B) = k + 1$ and $[A/e(A, B)+1]$ $[R_k][B/e(A, B) + 1)\} \bigcup R_k$.

Properties (i) and (ii) are easily checked. In order to check (iv), suppose that $e(A, B) \leqq k + 1$. If $(A, B) \in R_{k+1}$ then

$$[A/e(A, B) + 1][R_k][B/e(A, B) + 1] ,$$

but $[R_{k+1}]$ agrees with $[R_k]$ whenever both are defined. Conversely, if $e(A, B) \leqq k + 1$ then $[R_{k+1}]$ agrees with $[R_k]$ and the definition implies that $(A, B) \in R_{k+1}$. Finally, to prove (iii) take $e = e(A, B) < e(B, C)$ and hence $< k + 1$. Then $A/e = B/e = C/e$ while $[A/e + 1][R_k][B/e + 1] =$ $[C/e + 1]$ and $(A, C) \in R_k \subseteqq R_{k+1}$. A similar proof is obtained if $e(A, C) >$ $e(B, C)$ or $e(A, C) = e(B, C) < k + 1$. If $e(A, C) = e(B, C) = k + 1$ then $(A, C) \in R_{k+1}$ because of the transitivity of $[R_k]$. This completes the proof of the lemma.

3.12. DEFINITION. $R_0 = \{(A, B) : e(A, B) = 0$ and $w(A) < w(B)\}$.

It is readily seen that R_0 satisfies the conditions of 3.10 For each $k > 0$ let R_{k+1} be the extension of R_k given in 3.10 and let $R = \bigcup R_i$, $k \geqq 0$.

3.13. DEFINITION. $A \leqq B$ *if and only if* ARB or $A = B$.

It can be shown, using § 3.8, that $\leqq$ is a simple ordering of $\boldsymbol{B}$ (strictly speaking, of the isomorphism types of members of $\boldsymbol{B}$). Two properties of $<$ obtained from sections 3.10–3.13 which we shall use are

3.14. If $w(A) < w(B)$ then $A < B$.

3.15. $A < B$ if and only if $A/e(A, B) + 1 < B/e(A, B) + 1$.

4. Dot product.

4.1. DEFINITION. If A and B are basic algebras then $A \cdot B$ is defined to be the subalgebra of $A \times B$ consisting of all pairs (x, y) for which $\deg(x)$ (in A) $= \deg(y)$ (in B).

The following facts are easily derived.

4.2. $A/k \cdot B/k \doteq (A \cdot B)/k$ (see 1.12).

4.3. $h(A \cdot B) = \min[h(A), h(B)]$.

4.4. $w(A \cdot B) = w(A)w(B)$.

The main theorem on the dot product is the following one and in it the properties of lexicographic order are used without mention. The order between the algebras is the one given in 3.13.

4.5. THEOREM. (i) *If* $A < B$ *and* $h(C) \leqq e(A, B)$ *then* $A \cdot C = B \cdot C$.
(ii) *If* $A < B$ *and* $h(C) > e(A, B)$ *then* $A \cdot C < B \cdot C$.

Proof. (i) is easy, for in this case $A \cdot C = (A/h(C)) \cdot C = (B/h(C)) \cdot C = B \cdot C$. (ii) is proved by induction on $e = e(A, B)$. If $e = 0$ then $A < B$ if and only if $w(A) < w(B)$, but $w(A \cdot C) = w(A)w(C) < w(B)w(C) = w(B \cdot C)$ and hence $A \cdot C < B \cdot C$. Now take $e > 0$, assuming (ii) for smaller values of e. If $A < B$ then $[A/e + 1] < [B/e + 1]$ and $[A/e] = [B/e]$. Let $[C/e + 1] = \{C_1, \cdots, C_p\}$; $h(C_i) \leqq e$, the same holding for the members of $[A/e + 1]$ and $[B/e + 1]$. If $h(C_i) \leqq e - 1$ then $[A/e + 1] \cdot C_i = [B/e + 1 \cdot C_i$. If $h(C_i) = e$, then let $A_m < B_m$ be the first pair in which $[A/e + 1]$ and $[B/e + 1]$ differ; then $A_m \cdot C_i < B_m \cdot C_i$ by the inductive hypothesis, while for $j < m$, $A_j \cdot C_i = B_j \cdot C_i$. Thus $[A/e + 1] \cdot C_i < [B/e + 1] \cdot C_i$ lexicographically. For any C_i in $[C/e + 1]$ then, either $[A/e + 1 \cdot C_i = [B/e + 1] \cdot C_i$ or $[A/e + 1] \cdot C_i < [B/e + 1] \cdot C_i$. But $[A/e + 1] \cdot [C/e + 1]$ is just the ordered union of $[A/e + 1] \cdot C_i$, $C_i \in [C/e + 1]$, and at least one strict inequality must hold. Hence, $[A/e + 1] \cdot [C/e + 1] < [B/e + 1] \cdot [C/e + 1]$ lexicographically, and $A/e + 1 \cdot C/e + 1 < B/e + 1 \cdot C/e + 1$, while $A/e \cdot C/e = B/e \cdot C/e (= B \cdot C/e)$ and $A \cdot C < B \cdot C$, by definition of $<$.

4.6. COROLLARY. *If* A, B, C *are infinite and* $A < B$ *then* $A \cdot C < B \cdot C$.

4.7. COROLLARY. *If* A, B, C *are basic algebras and* $A \leqq B$ *then* $A \cdot C \leqq B \cdot C$.

Up to isomorphism, the collection of infinite basic unary algebras with $\cdot$ forms a commutative semigroup which by 4.6 is ordered. This is the semigroup to which we apply the following lemma.

4.8. LEMMA. *If* $\langle S, \cdot, \leqq \rangle$ *if an ordered semigroup*[2], S^* denotes the set of all finite nonempty, nondecreasing sequences in S; for $\{x_i\}$ and $\{y_j\}$ in S^*, $\{x_i\} * \{y_j\}$ is defined as the nondecreasing sequence formed from $\{x_i \cdot y_j\}$; and $\leqq^*$ is the length lexicographic order; then $\langle S^*, *, \leqq^* \rangle$ is an ordered semigroup.

Proof. Suppose $x = \{x_i\}$, $y = \{y_j\}$, $z = \{z_m\}$ are in S^* and $x <^* y$. If length $x <$ length y then length $xz <$ length yz and $xz <^* yz$. If length $x =$ length y there is a $t > 0$ with $x_i = y_i$ for any $i < t$ and $x_t < y_t$. Let $\underline{x} = \{x_i : i < t\}$, $\bar{x} = \{x_i : i \geqq t\}$ and similarly for $\underline{y}$ and $\bar{y}$. The smallest elements in $\bar{y} * z$ and $\bar{y} *$ are formed from x_t, y_t, and z_1.

[2] We use ordered in the sense of Clifford [**2**], i.e., $a < b$ implies $a \cdot c < b \cdot c$.

Therefore, $\bar{x} * z < \bar{y} * z$. Now $\underline{x} = \underline{y}, \underline{x} * z = \underline{y} * z$ and we have $x * z = (\underline{x} \cup \bar{x}) * z < (\underline{y} \cup \bar{y}) * z = y * z$. The reason is: inserting equal sequences in two ordered sequences cannot change their order.

5. Unraveled algebras.

Let A be a finite unary algebra, x a cyclic element of A and $X = C(x)$ (1.10). We associate with x an infinite basic algebra which we think of as "X unraveled backwards, starting at x", and call $W(x)$.

5.1. DEFINITION. $W(x) = \langle X \times I, *\rangle$ with $I = \{0, 1, \cdots\}$

$$\begin{aligned}(x, 0)^* &= (x, 0)\\ (x, k)^* &= (x', k-1) \text{ for } k > 0\\ (y, k)^* &= (y', k) \text{ for } y \neq x\ .\end{aligned}$$

It is not difficult to see that $W(x)$ is a basic algebra, the only cyclic element being $(x, 0)$. $(y, m) \in W(x)$ we still use $\deg(y, ɯ)$ as in 3.3. If x is any cyclic element in a connected algebra A and $y \in A$ then for some $n, y^n = x$; in this context we need

5.2. DEFINITION. $\deg_x(y) = m$ if and only if m is the least nonnegative integer for which $y^m = x$. If y is not in $C(x)$ then $\deg_x y$ is not defined.

If the cyclic part of a connected algebra is a p-cycle we say the algebra is p-cyclic. Lemma 5.3 follows immediately from the definitions.

5.3. *If* $(y, m) \in W(x)$ *and* $C(x)$ *is p-cyclic, then* $\deg(y, m) = \deg_x(y) + mp$.

5.4. LEMMA. *If a and x are in A, b and y are in $B, C(a)$ is p-cyclic, and $C(b)$ is q-cyclic; then in $A \times B$; $(x, y) \in C(a, b)$ if and only if* $\deg_a x = \deg_b y \bmod (p, q)$.

Proof. $(x, y) \in C(a, b)$ if and only if for some $m, (x, y)^m = (a, b)$, which is equivalent to $x^m = a$ and $y^m = b$. Such an m exists if and only if there are nonnegative integers r, s with

5.5. $m = \deg_a x + rp = \deg_b y + sq$.

The necessary and sufficient condition for the existence of r, s is that $\deg_a x = \deg_b y \bmod (p, q)$. This completes the proof.

If $(x, y) \in C(a, b)$ and $m = \deg_{(a,b)}(x, y)$ then the integers satisfying 5.5 are unique and will be denoted by

5.6. $r_0 = (\deg_{(a,b)}(x, y) - \deg_a x)/p, s_0 = (\deg_{(a,b)}(x, y) - \deg_b y)/q$.

A result on which the rest of the development depends is

5.7. THEOREM. *If A, B are finite unary algebras, $a \in A/0$ and $b \in B/0$; then $W(a) \cdot W(b) \sim W(a, b)$ in $A \times B$.*

Proof. Let $C(a)$ be p-cyclic and $C(b)$ be q-cyclic. Take an element $((x, k), (y, m))$ in $W(a) \cdot W(b)$ and using the definition of $\cdot$, and 5.3 obtain:

5.8. $\deg_a x + kp = \deg(x, k) = \deg(y, m) = \deg_b y + mq$.

We have then $\deg_a x \equiv \deg_b y \bmod (p, q)$ and can apply 5.4; yielding: $(x, y) \in C(a, b)$ and

5.9. $\deg_{(a,b)}(x, y) = \deg_a x + r_0 p = \deg_b y + s_0 q$.

Subtracting equation 5.9 from equation 5.8 and dividing by $[p, q]$, it is easily seen that the result is an integer h,

5.10. $$\begin{aligned} h = h((x, k), (y, m)) &= (\deg(x, k) - \deg_{(a,b)}(x, y))/[p, q] \\ &= (\deg(y, m) - \deg_{(a,b)}(x, y))/[p, q]. \end{aligned}$$

Clearly, h is a well defined function and we can now define a function f which we shall show is the required isomorphism,

5.11. $f((x, k), (y, m)) = ((x, y), h)$.

To see that f is one-to-one and onto one need only take $((x, y), h)$ in $W(a, b)$ and solve equation 5.10 for k and m, using 5.8, the solution being unique. It remains to be shown that f commutes with the operations involved. Using $*$ for the operations in the W algebras, and recalling that on $W(a) \cdot W(b)$, $*$ is defined componentwise, let $z = ((x, k), (y, m))$. We want to show that $f(z^*) = [f(z)]^*$ and we need to consider three cases:

(1) $x \neq a$;

(2) $x = a, y = b$, neither k nor $m = 0$; and

(3) $x = a, y = b, k = m = 0$. No other cases are needed, for if $(y, m) = (b, 0)$ then $(x, k) = (a, 0)$, otherwise z would not be in $W(a) \cdot W(b)$. All other possible cases are taken care of by symmetry.

Case 1. $[f(z)]^* = [(x, y), h]^* = [(x', y'), h]$ since $(x, y) \neq (a, b)$, $z^* = [(x', k), (y', m)]$ the value of m being unimportant, and $f(z^*) = [(x', y'), h]$ in which h is calculated from 5.10; $\underline{h} = (\deg(x', k) - \deg_{(a,b)}(x', y'))/[p, q]$. But $\deg(x', k) = \deg(x, k) - 1$ and $\deg_{(a,b)}(x', y') = \deg_{(a,b)}(x, y) - 1$, hence $\underline{h} = h$ and this case is complete.

Case 2. $[f(z)]^* = [(a, b), h]^* = [(a', b'), h - 1]$ and $z^* = [(a', k - 1), (b', m - 1)]$, $f(z^*) = [(a', b'), \underline{h}]$. We calculate h and $\underline{h}$:

$$\begin{aligned} h[(a, k), (b, m)] &= (\deg(a, k) - \deg_{(a,b)}(a, b))/[p, q] \\ &= (\deg_a a + kp - 0)/[p, q] = kp/[p, q] . \end{aligned}$$

$$\begin{aligned}\underline{h}[(a', k-1), (b', m-1)] &= (\deg_a a' + (k-1)p - [p, q])/[p, q] \\ &= (p + (k-1)p - [p, q])/[p, q] = h - 1\,.\end{aligned}$$

This completes the proof of the theorem, since Case 3 is trivial.

We now associate with any unary algebra the collection of its W algebras by

5.12. DEFINITION. If A is a unary algebra $W(A) = \{W(a) : a \in A/0\}$.

Since $A/0 \times B/0 \sim A \times B/0$ it follows that $W(A \times B) = \{W(a, b) : (a, b\} \in (A \times B)/0\}$ which is naturally pairwise isomorphic to $\{Wa \cdot Wb : a \in A/0, b \in B/0\}$. This last expression we write $W(A) \cdot W(B)$ instead of $*$ as in Lemma 4.8 This proves

5.13. THEOREM. $W(A \times B) \sim W(A) \cdot W(B)$.

5.14. THEOREM. *If A, B are connected, finite, and A is p-cyclic, B is q-cyclic, then $A \sim B$ if and only if $p = q$ and for some $a \in A_0$, $b \in B_0$, $W(a) \sim W(b)$.*

Proof. One of the implications is clear; for the other, let f be an isomorphism f: $W(a) \sim W(b)$ for some $a \in A/0, b \in B/0$. We have seen that isomorphisms preserve degree and they certainly preserve number of predecessors. Thus, $f(a, 0) = (b, 0)$ and since $(a, 1)$ may be characterized as the only element of degree p with infinitely many predecessors $f(a, 1)$ must be the corresponding element of $W(b)$. But $p = q$ so that this element is $(b, 1)$. Moreover, $f: A \times 0 \sim B \times 0$ since these are the sets of elements which do not precede $(a, 1)$ and $(b, 1)$ respectively. It then follows immediately that the first coordinate of f is an isomorphism of A onto B.

Notice that in the connected case, the existence of an isomorphism between any $W(a)$ and $W(b)$ is sufficient, (with $p = q$), to insure the isomorphism of A and B. If the two sequences $W(A)$ and $W(B)$ have the same number of elements, then we must have $p = q$ and conversely. This yields

5.15. COROLLARY. *If A, B are finite and connected then $A \sim B$ if and only if $W(A) \sim W(B)$.*

6. Cancellation. We can now apply the preceding results to the cancellation problem for finite unary algebras.

It is readily seen that in any ordered semigroup either of $x \cdot x = y \cdot y$ or $x \cdot z = y \cdot z$ implies $x = y$. The system of infinite basic algebras with $\cdot$ and $\leqq$ is (up to isomorphism) such a semigroup. This system includes W algebras and we apply Lemma 4.8 to the system of finite sequences of W algebras. From these considerations we obtain for finite unary algebras A, B, C, 6.1. LEMMA. *$W(A) \cdot W(A) \sim W(B) \cdot W(B)$ or $W(A) \cdot W(C) \sim W(B) \cdot W(C)$ implies $W(A) \sim W(B)$.*

6.2. LEMMA. *If A, B, and C are finite unary algebras and $A^2 \sim B^2$ or $A \times C \sim B \times C$, then $W(A)$ is pairwise isomorphic to $W(B)$.*

Proof. From 5.13 $W(A) \cdot W(A) \sim W(A^2) \sim W(B^2) \sim W(B) \cdot W(B)$, and similarly for $A \times C \sim B \times C$. The lemma follows by applying 6.1.

6.3. THEOREM. *If A, B, C, are connected finite unary algebras and $A^2 \sim B^2$ or $A \times C \sim B \times C$, then $A \sim B$.*

Proof. The theorem follows from 6.1 and 5.15.

If an algebra is not connected let us say that it is *pure* if all the components are p-cyclic for some fixed p and use the term p-cyclic for pure algebras as well as connected algebras.

6.4. THEOREM. *If A, B, and C are pure finite unary algebras and $A^2 \sim B^2$; or $A \times C \sim B \times C$ and $A/0 \sim B/0$, then $A \sim B$.*

Proof. From 6.2 we obtain $W(A) \sim W(B)$. Since we have unique square roots for cyclic algebras (2.3) and from the hypothesis in the other case we see that the cyclic structure of both A and B is the same. They are both pure and consequently there is an integer p such that all of the cycles of A and B are p-cycles. Given $W(A)$ and $W(B)$ and p we can put each of the elements of $W(A)$ and $W(B)$ back together again—see 5.14 and its proof. This will yield the components of A and B each repeated p times, hence A and B must be isomorphic.

If A is a finite algebra we can write $A = A_1 \cup A_2 \cup \cdots \cup A_n$ in which each A_i is a pure subalgebra (a collection of components) and the decomposition is maximal in the sense that $A_i \cup A_j$ is not pure. This decomposition is clearly unique up to order and the integer n is called the length of A. We can now complete the solution of the square root problem with

6.5. THEOREM. *If A and B are finite unary algebras and $A^2 \sim B^2$ then $A \sim B$.*

The proof is by induction on n, the length of A (and in view of 2.3, also the length of B). For $n = 1$ the conclusion is part of § 6.4. For $n > 1$, assuming the result for smaller n, we know from 2.3 that the cyclic structure of A and B is the same. Hence, in the decomposition into pure subalgebras, $A = A_1 \cup A_2 \cup \cdots \cup A_n$, $B = B_1 \cup B_2 \cup \cdots \cup B_n$, we may assume that both A_i and B_i consist of p_i-cyclic algebras with $A_i/0 \sim B_i/0$, and $p_1 < p_2 < \cdots < p_n$.

It is not possible for A_i to be isomorphic to B_i for all $i \neq j$ and

$A_j \not\sim B_j$. For we know that $W(A) \sim W(B)$ and if the above condition were to hold then there would be a one-to-one correspondence between the W algebras obtained from A_i $i \neq j$ and B_i $i \neq j$ and hence between those obtained from A_j and B_j. But this and the fact that A_j and B_j have the same cyclic structure implies that $A_j \sim B_j$.

Hence, if $A \not\sim B$ then for some smallest $j < n$ $A_j \not\sim B_j$. If I is the set of indices for which $p_i, i \in I$ divides p_j; let $P = \bigcup\{A_{p_i}: i \in I\}$, $Q = \bigcup\{B_{p_i}: i \in I\}$ and define A'', B'' so that $A = P \cup A''$, $B = Q \cup B''$. Then $A^2 = P^2 \cup PA'' \cup A''P \cup A''^2$. But for integers m, p, q; $[p, q]$ divides m if and only if p divides m and q divides m. Hence the components of P^2 are those which are k-cyclic with k dividing p_j. From this it follows that when the isomorphism. given between A^2 and B^2 is restricted to P^2, it maps P^2 isomorphically onto Q^2. Hence $P \sim Q$ since P and Q are shorter than A and B. This implies that $A_j \sim B_j$ which is a contradiction and completes the proof.

7. Summary.

We have seen that all finite unary algebras have unique (if any) square roots, and that in some cases $A \times C \sim B \times C$ implies $A \sim B$. This last implication does not hold in general for finite algebras. The simplest example of its failure is: A a 2-cycle and B two 1-cycles. In this case $A \times A \sim B \times A$ and $A \not\sim B$.[3] It is easy to see that if A is a k-cycle and B is any collection of p_i-cycles with $p_i \mid k$ and $\sum p_i = k$ then the same situation obtains.

In view of 6.2 it would be reasonable to conjecture that if the cyclic structure of A and B is the same then $A \times C \sim B \times C$ implies $A \sim B$. Whenever there is only one way of putting the W algebras back together, as in the pure case when the size of the cyclic parts is determined, we can obtain cancellation.

In the infinite case, it is known that an algebra need not have a unique square root, a simple example being: A and B free unary algebras with k and l generators, $k \neq l$. Then $A^2 \sim B^2$ but $A \not\sim B$. It seems likely that the results of this paper could be generalized to suitable classes of infinite algebras such as basic algebras, locally finite connected algebras, or algebras satisfying some kind of descending chain condition. We have not as yet attempted such generalizations.

8. Proof of Theorem 3.8.

THEOREM. *If A, B are basic algebras with $A/k \sim B/k$ for all $k \geqq 0$, then $A \sim B$.*

Proof. If A, B are finite the theorem is trivial; we assume that they are infinite. For each k let I_k be the set of isomorphisms of A/k

[3] This example is attributed to B. Jónsson by Birkhoff [**1**], p. 96, ex. 4.

onto B/k. I_k is not empty, and since A_k is finite, so is I_k. If $m > k$ and $\phi \in I^m$ then $(\phi)A/k(\phi$ restricted to $A/k) \in I_k$; hence, some members of I_k must be the restrictions of infinitely many isomorphisms of greatet degree, and in fact of arbitrarily great degree. Let E_k be the subser of I_k consisting of isomorphisms of this type. If $\phi \in E_k$ there is a member of E_{k+1}, ψ, with $(\psi)A/k = \phi$, let E_ϕ be the subset of E_{k+1} satisfying this condition. By the axiom of choice there is a function f which selects for each ϕ in E_k an $f(\phi)$ in E_ϕ.

We now define ϕ_0: $A/0 \sim B/0$ by $\phi_0(a) = b$ (this is the only member of I_0); and for $k > 0$ $\phi_k = f(\phi_{k-1})$. We show that $\phi = \bigcup \phi_k$ is an isomorphism, $\phi : A \sim B$. In the sequence $\phi_0, \phi_1, \cdots$ each ϕ is the restriction of ϕ_{i+1} to A/i so that ϕ is a function. Since $\bigcup A/i$ and each A/i is the domain of ϕ_i the domain of ϕ is A. If $x \in A$ then $x \in A/i$ for some i $\phi(x') = \phi_i(x') = \phi_i(x)' = \phi(x)'$. It is equally easy to see that ϕ is one-to-one and onto B, and consequently is an isomorphism.

References

1. Garrett Birkhoff, *Lattice Theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, rev. ed., 1948.

2. A. H. Clifford, *Totally ordered commutative semigroups*, Bull. Amer. Math. Soc., **64** (1958), 305-316.

3. B. Jónsson and A. Tarski, *Direct decompositions of finite algebraic systems*, Notre Dame Mathematical Lectures, No. 5, (1947), 64 pp.

Fresno State College