TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 158, Number 2, August 1971

WORD PROBLEM FOR RINGOIDS OF NUMERICAL FUNCTIONS

BY
A. ISKANDER

Abstract. A. The composition ringoid of functions on (i) the positive integers, (ii) all integers, (iii) the reals and (iv) the complex numbers, do not satisfy any identities other than those satisfied by all composition ringoids.

B. Given two words u, v of the free ringoid, specific functions on the positive integers, $f_1,\ldots,f_k$ can be described such that $u(f_1,\ldots,f_k)$ and $v(f_1,\ldots,f_k)$, evaluated at 1, are equal iff $u=v$ is an identity of the free ringoid.

The word problem for different algebraic systems has been studied by several authors (cf. e.g. [1], [3], [4], [5], [7], [9], [10] and connected literature quoted there). The aim of this paper is to describe all identities satisfied in a class of certain ringoids.

In §I are formulated some imbeddability properties and representation of semirings and composition ringoids; and also those with nullary operations.

In §II we recall the construction of the free composition ringoid and formulate the main theorem of this paper (B of the Abstract) and some of its immediate corollaries (among which A of the Abstract). Thus there is an algorithm which describes the identities satisfied in $\boldsymbol{Z}^{\boldsymbol{Z}}$, $\boldsymbol{R}^{\boldsymbol{R}}$ w.r.t. pointwise addition, multiplication and composition of functions, which solves Problem 56, p. 158 of [1].

In §III some lemmas and their immediate corollàries are proved basically to provide the proof of the main theorem. Every word of the free composition ringoid is reducible to a canonical form and two words are equivalent iff they are reducible to the same canonical form.

In §IV how to modify the methods of the paper in order to apply them to ringoids with nullary operations is shown.

For notations of the theory of universal algebras, cf. e.g. [1], [3], [6], [8]; for the theory of recursive functions, cf. e.g. [4], [9], [10].

I would like to express my thanks to Garret Birkhoff, Kirby Baker and the referee for reading the original manuscript and making valuable indications.

I. Semirings and ringoids.

1. *Commutative semirings.* By a semiring will be meant a nonvoid set together with two associative and commutative binary operations: addition + and

Received by the editors November 18, 1968 and, in revised form, September 7, 1970.

AMS 1969 *subject classifications.* Primary 0830; Secondary 0270.

Key words and phrases. Semiring, free composition ringoid, functional extension, functions with finite range, canonical forms, depth, width, rank, algorithm.

multiplication $\times$; moreover, multiplication is distributive w.r.t. addition. A semiring is said to be with 0 if it contains a neutral—w.r.t. addition—element 0, such that the product of any element of the semiring and 0 is 0. A semiring is said to be with 1 if it contains a neutral—w.r.t. multiplication—element 1. A semiring is said to be with 0 and 1 if it is with 0 and with 1 and $0\neq 1$.

The sets (i) $\boldsymbol{N}_0$ of all nonnegative integers, (ii) $\boldsymbol{Z}$ of all integers, (iii) $\boldsymbol{Q}$ of all rational numbers, (iv) $\boldsymbol{R}$ of all real numbers, and (v) $\boldsymbol{C}$ of all complex numbers, together with natural addition and multiplication, are examples of semirings with 0 and 1.

The sets (i) $\boldsymbol{N}$ of all positive integers, (ii) of all positive rational numbers and (iii) of all positive real numbers are examples of semirings with 1 and without 0. The set of all positive even integers is a semiring without 0 and without 1.

As in semigroups and rings:

PROPOSITION 1. *Every semiring is imbeddable into a semiring with* 0 *and* 1.

2. *Composition ringoids.* By a ringoid will be meant a nonvoid set together with three binary operations: addition $+$, multiplication $\times$ and composition $\circ$, such that addition and multiplication define a semiring, composition is associative and is right distributive with regard to both addition and multiplication. The associative laws of addition, multiplication and composition, the commutative laws of addition and multiplication and the distributive laws of multiplication with regard to addition and of composition with regard to the other two operations will be called "*laws of ringoids.*"

A ringoid is said to be with 0 (and/or 1) if addition and multiplication define a semiring with 0 (and/or 1); moreover $0\circ a=0$ $(1\circ a=1)$ for all elements a of the ringoid. A ringoid is said to be with e if it has a neutral—w.r.t. composition—element e. A ringoid is said to be with 0, 1 and e if it is with 0, with 1 and with e; moreover, 0, 1 and e are three distinct elements.

The sets (i) of all functions with finite range on the positive integers, the reals, the complex numbers, (ii) of all primitive recursive functions, (iii) of all partial recursive functions, (iv) $\boldsymbol{N}^{\boldsymbol{N}}$, (v) $\boldsymbol{Z}^{\boldsymbol{Z}}$, (vi) $\boldsymbol{Q}^{\boldsymbol{Q}}$, (vii) $\boldsymbol{R}^{\boldsymbol{R}}$, (viii) $\boldsymbol{C}^{\boldsymbol{C}}$ together with pointwise addition and multiplication and the composition of functions are examples of ringoids. $\boldsymbol{N}^{\boldsymbol{N}}$ is a ringoid with 1 and e but without 0. The ringoids of (i) are without e but with 1 in the first case, with 1 and 0 in the other cases. All other ringoids above are with 0, 1 and e.

PROPOSITION 2. *Every ringoid is imbeddable into a ringoid with e.*

3. *Ringoids of semiring transformations.*

PROPOSITION 3. *If A is a semiring then A^A is a ringoid with e, where addition and multiplication are pointwise and composition is the composition of functions, e is the identical function on A; moreover, if A is with* 0 (*and/or* 1) *then A^A will be with* 0 (*and/or* 1); *the $O(1)$ is the constant $O(1)$-valued function.*

A^A will be called the full ringoid of transformations of A.

A converse of Proposition 3 is

PROPOSITION 4. *Every ringoid is imbeddable into a full ringoid of transformations with* 0, 1 *and* e.

Thus every ringoid can be considered a ringoid of transformations of a semiring with 0 and 1.

Propositions 1, 2, 3, 4 are similar to results in [2].

4. *Functional extensions.* Let A, B be semirings and $R(A)$, $R(B)$ be ringoids of transformations of A and B respectively. $R(B)$ will be called a functional extension of $R(A)$ if A can be identified with a subsemiring of B and, for any finite subset X of A and for any function $f \in R(A)$, there is a function $g \in R(B)$ such that the restrictions of f and g to X coincide.

II. The free ringoid

5. *The word algebra.* Let F be a countably infinite set. We recall the construction of the word algebra W over F with binary operations $+$, $\times$ and $\circ$ (cf. e.g. [1], [3], [6], [8]):

(a) Words of rank 0 are elements of F, i.e. $F \subseteq W$.

(b) If $u, v \in W$, the ranks of u, v are less than k, and at least one of u, v is of rank $k-1$, then $(u)+(v)$, $(u)\times(v)$, $(u)\circ(v) \in W$ are of rank k.

(c) Every word of W is obtained by repeated use of (a) and (b).

The operations $+$, $\times$, $\circ$ are defined on W as usual.

The word algebra with nullary operations is the word algebra over the union of F and the nullary operations.

$r(u)$ will denote the rank of u.

PROPOSITION 5. *The set W is primitive recursive; the rank function r has a primitive recursive extension* (*cf. e.g.* [4], [9], [10]).

If $u \in W$ and $a(u)$ denotes the number of distinct elements of F occurring in u, then

PROPOSITION 6. $1 \leqq a(u) \leqq 2^{r(u)}$; *both bounds are reached.*

6. *The free ringoid—the main theorem.* The free ringoid over F is the factor algebra of W by the congruence relation $\equiv$, where $u \equiv v$ iff u can be transformed to v by repeated use of laws of ringoids.

THEOREM. *Given any two words u, v in $f_1, \ldots, f_k \in F$, one can construct specific functions $f_1', \ldots, f_k'$ on the positive integers, such that*

$$u \equiv v \text{ iff } u(f_1', \ldots, f_k')(1) = v(f_1', \ldots, f_k')(1);$$

$$f_i'(x) = \exp(q; p^i(x+t)^s), \qquad 1 \leqq i \leqq k;$$

$$s = c(r(u+v)), \qquad t = (s+1)!;$$

$$p = (s+2)t^{s+1}, \qquad q = (s+2)p^{s+1};$$

$$c(n) = (n+1)\,\mathrm{sg}\,(2 \dot{-} n) + \exp(2; \exp(2; n \dot{-} 1))\,\mathrm{sg}\,(n \dot{-} 1).$$

The proof of the Theorem will be given in §III. We conclude §II by some applications of this Theorem.

7. Corollary 1. *The graph of $\equiv$ is a primitive recursive set and so the set of all identities of the variety of all ringoids is primitive recursive.*

Denote by A_0 the subringoid of N^N generated by all functions $f_i'(x)$ described in the Theorem, for all $s \geqq 2$ and $1 \leqq i \leqq s$. Since it is clear that $f_i'(x)$ in the Theorem, once constructed, can be cut down to functions with finite range, we will consider $f_i'(x)$, functions with finite range. We have

Corollary 2. *For any $u, v \in W$, $u \equiv v$ iff $u = v$ is an identity in A_0.*

Corollary 3. *The ringoid A_0 generates the variety of all ringoids.*

Corollary 4. *If a ringoid A is a functional extension of A_0, then the algorithm of the Theorem determines the identities of A, and so $u = v$ is an identity in A iff it is an identity in every ringoid and A generates the variety of all ringoids.*

Let $u = v$ be an identity in A and let $g_1, \ldots, g_k \in A_0$. A can be considered a ringoid of transformations $R(B)$ where B is a semiring and N is a subsemiring of B. Let $X(n)$ be the set of all integers of N appearing in the computation of $u(g_1, \ldots, g_k)(n)$ and $v(g_1, \ldots, g_k)(n)$. $X(n)$ is finite for every $n \in N$. As A is a functional extension of A_0, there are $a_1, \ldots, a_k \in A$ such that the restrictions of a_i and g_i to $X(n)$ coincide, $1 \leqq i \leqq n$. Hence

$$\begin{aligned} u(g_1, \ldots, g_k)(n) &= u(a_1, \ldots, a_k)(n) \\ &= v(a_1, \ldots, a_k)(n) = v(g_1, \ldots, g_k)(n), \end{aligned}$$

i.e., for all $n \in N$, $g_1, \ldots, g_k \in A_0$, $u(g_1, \ldots, g_k)(n) = v(g_1, \ldots, g_k)(n)$.

Corollary 5. *The algorithm of the Theorem describes all identities in*

(a) *the ringoid of all functions on* (i) *the positive integers,* (ii) *the integers,* (iii) *the real numbers,* (iv) *the complex numbers;*

(b) *the ringoid of all functions with finite range on* (i), (ii), (iii) *and* (iv).

The algorithm of the Theorem describes all identities in any of the ringoids of functions on any subsemiring of the complex numbers given in §II.

Each of the ringoids concerned is clearly a functional extension of A_0.

The word problem for $\boldsymbol{Z}^{\boldsymbol{Z}}$ and $\boldsymbol{R}^{\boldsymbol{R}}$ has been suggested by G. Birkhoff in [1, Problem 56, p. 158].

III. **Proof of the Theorem.** To prove the Theorem we need some preparations and must prove some lemmas.

For any $u(1), \ldots, u(n) \in W$, we write
$\sum \{u(i) : 1 \leqq i \leqq n\}$ for $(\cdots(u(1)+u(2))+\cdots)+u(n)$,
$\prod \{u(i) : 1 \leqq i \leqq n\}$ for $(\cdots(u(1)\times u(2))\times\cdots)\times u(n)$,
nu for $\sum \{u(i) : 1 \leqq i \leqq n\}$,
u^n for $\prod \{u(i) : 1 \leqq i \leqq n\}$,
in case $u = u(1) = \cdots = u(n)$.

8. *Canonical forms.* We define by induction on a function d, called the depth, words of certain type, called canonical forms. We define equivalence of two such forms and also a function b, called the width of the form:

A canonical form of depth 0 is a word $u \in W$, $d(u)=0$ of the type:

$$u = \sum \left\{ t(i) \prod \{(f(ij))^{r(ij)} : 1 \leqq j \leqq k(i)\} : 1 \leqq i \leqq n \right\}, \tag{1}$$

where $f(ij) \in F$, $r(ij)$, $t(i)$, $k(i)$, $n \in N$. No two $f(ij)$ with same i and distinct j and also, no two $\{\{f(ij)\}^{r(ij)} : 1 \leqq j \leqq k(i)\}$ with distinct i are equal (via sets). (A^s is the sth cartesian power of A.)

$$b(u) = \max \left(\left\{ \sum \{t(i) : 1 \leqq i \leqq n\} \right\} \cup \left\{ \sum \{r(ij) : 1 \leqq j \leqq k(i)\} : 1 \leqq i \leqq n \right\} \right).$$

With u we associate the set

$$\{\{\{f(ij)\}^{r(ij)} : 1 \leqq j \leqq k(i)\}^{t(i)} : 1 \leqq i \leqq n\}.$$

Two canonical forms u, v of depth 0 are equivalent, and we write $u \operatorname{eq} v$ if their associated sets are equal.

It is clear that if $u \operatorname{eq} v$, $d(u)=d(v)=0$, then $b(u)=b(v)$.

Suppose all canonical forms of depth less than d, $d \in N$, their equivalence, their associated sets and their width have been defined. Let it also be true that for two such forms u, v, $u \operatorname{eq} v$ implies $d(u)=d(v)$ and $b(u)=b(v)$. A canonical form u of depth d is of type

$$u = \sum \left\{ t(i) \prod \{(u(ij))^{r(ij)} : 1 \leqq j \leqq k(i)\} : 1 \leqq i \leqq n \right\}, \tag{2}$$

where $t(i)$, $r(ij)$, $k(i)$, $n \in N$ and $u(ij) \in F$ or $u(ij)=f(ij) \circ (u_1(ij))$, where $u_1(ij)$ is a canonical form of depth less than d and at least one of $u(ij)$ is of depth $d-1$. No two $u(ij)$ with same i and distinct j and no two sets $\{\{u(ij)\}^{r(ij)} : 1 \leqq j \leqq k(i)\}$ with distinct i are equal, where two equivalent forms are considered equal; $(f \circ u) \operatorname{eq} (g \circ v)$ means $f=g$, $u \operatorname{eq} v$.

$$\begin{aligned} b(u) = \max \Big(& \left\{ \sum \{t(i) : 1 \leqq i \leqq n\} \right\} \\ & \cup \left\{ \sum \{r(ij) : 1 \leqq j \leqq k(i)\} : 1 \leqq i \leqq n \right\} \\ & \cup \{b(u(ij)) : 1 \leqq j \leqq k(i) : 1 \leqq i \leqq n\} \Big). \end{aligned} \tag{3}$$

With u we associate the set

$$\{\{\{u(ij)\}^{r(ij)} : 1 \leqq j \leqq k(i)\}^{t(i)} : 1 \leqq i \leqq n\}.$$

Two canonical forms u, v of depth d are equivalent if their associated sets are equal.

It is clear that each of the depth and width functions takes the same value at equivalent forms.

Proposition 7. *The set of all canonical forms is primitive recursive; moreover, the depth and width functions have primitive recursive extensions (cf. e.g.* [4], [9], [10]).

9. *Reduction to canonical forms.*

Proposition 8. *Every word of W can be reduced to a canonical form by repeated use of laws of ringoids.*

In other words, to every $u \in W$ we can construct a canonical form v such that $u \equiv v$; every congruence class of $\equiv$ contains a canonical form.

It is clear that in a canonical form no well formed part of the expression looks like $u \times (v+w)$, $(v+w) \times u$, $(v+w) \circ u$, $(v \times w) \circ u$ and reducing an expression to canonical form consists of repeated use of laws of ringoids, in order to remove expressions of the above form, and grouping similar terms (up to associativity and commutativity of $+$ and $\times$).

Although every congruence class of $\equiv$ in W has a canonical form, the set of all canonical forms is not a transversal for $W/\equiv$ in W (cf. e.g. [4]). We could have defined normal forms by lexicographically ordering the canonical forms and pointing, in every class, the form with minimal order.

If $c(n)$ is the maximum of all widths of all canonical forms of words of rank n, then

Proposition 9. $c(n) = (n+1) \operatorname{sg} (2 \dot{-} n) + \exp (2; \exp (2; n \dot{-} 1)) \operatorname{sg} (n \dot{-} 1)$.

10. *Number theoretic preparations.*

If $\boldsymbol{a}, \boldsymbol{b} \in N_0^4$ then we shall write $\boldsymbol{a}(i)$ for the ith component of $\boldsymbol{a}$, $1 \leqq i \leqq 4$; $\boldsymbol{a}^{\boldsymbol{b}}$ for $(\boldsymbol{a}(1))^{\boldsymbol{b}(1)} \times (\boldsymbol{a}(2))^{\boldsymbol{b}(2)} \times (\boldsymbol{a}(3))^{\boldsymbol{b}(3)} \times (\boldsymbol{a}(4))^{\boldsymbol{b}(4)}$: $\boldsymbol{a} \leqq \boldsymbol{b}$ for $\boldsymbol{a}(i) \leqq \boldsymbol{b}(i)$, $1 \leqq i \leqq 4$ and $\mathbf{0}$ for $(0, 0, 0, 0)$.

Lemma 1. *Let $\boldsymbol{n}, \boldsymbol{u} \in N^4$, $a_i, b_i \in N_0$, $a_i, b_i < \boldsymbol{u}(1)$ for all $\mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}$ and let $1 < \boldsymbol{u}(i)$, $(1+\boldsymbol{n}(i))(\boldsymbol{u}(i))^{(1+\boldsymbol{n}(i))} \leqq \boldsymbol{u}(i+1)$, $1 \leqq i \leqq 3$ and*

$$\sum \{a_{\boldsymbol{i}} \boldsymbol{u}^{\boldsymbol{i}} : \mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}\} = \sum \{b_{\boldsymbol{i}} \boldsymbol{u}^{\boldsymbol{i}} : \mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}\}. \tag{4}$$

Then $a_i = b_i$ for all $\mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}$.

Proof. Rewrite each side of (4) as a polynomial in $\boldsymbol{u}(4)$. Consider the coefficients of $(\boldsymbol{u}(4))^k$ in both sides, say y_k, z_k, where

$$\begin{aligned} y_k &= \sum \{a_{\boldsymbol{i}} \boldsymbol{u}(1)^{\boldsymbol{i}(1)} \boldsymbol{u}(2)^{\boldsymbol{i}(2)} \boldsymbol{u}(3)^{\boldsymbol{i}(3)} : \mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}, \boldsymbol{i}(4) = k\} \\ &< \sum \{\boldsymbol{u}(1)^{1+\boldsymbol{i}(1)} \boldsymbol{u}(2)^{\boldsymbol{i}(2)} \boldsymbol{u}(3)^{\boldsymbol{i}(3)} : \mathbf{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}, \boldsymbol{i}(4) = k\} \\ &< (1+\boldsymbol{n}(1)) \boldsymbol{u}(1)^{(1+\boldsymbol{n}(1))} \sum \{\boldsymbol{u}(2)^{\boldsymbol{i}(2)} \boldsymbol{u}(3)^{\boldsymbol{i}(3)} : 0 \leqq \boldsymbol{i}(2) \leqq \boldsymbol{n}(2), 0 \leqq \boldsymbol{i}(3) \leqq \boldsymbol{n}(3)\} \\ &\leqq \sum \{\boldsymbol{u}(2)^{1+\boldsymbol{i}(2)} \boldsymbol{u}(3)^{\boldsymbol{i}(3)} : 0 \leqq \boldsymbol{i}(2) \leqq \boldsymbol{n}(2), 0 \leqq \boldsymbol{i}(3) \leqq \boldsymbol{n}(3)\} \\ &< (1+\boldsymbol{n}(2)) \boldsymbol{u}(2)^{1+\boldsymbol{n}(2)} \sum \{\boldsymbol{u}(3)^{\boldsymbol{i}(3)} : 0 \leqq \boldsymbol{i}(3) \leqq \boldsymbol{n}(3)\} \\ &\leqq \sum \{\boldsymbol{u}(3)^{1+\boldsymbol{i}(3)} : 0 \leqq \boldsymbol{i}(3) \leqq \boldsymbol{n}(3)\} \\ &\leqq (1+\boldsymbol{n}(3)) \boldsymbol{u}(3)^{1+\boldsymbol{n}(3)} \leqq \boldsymbol{u}(4). \end{aligned}$$

Thus $y_k < \boldsymbol{u}(4)$, the same is true for z_k, i.e. we have two representations of the same integer as $\boldsymbol{u}(4)$-polynomial and hence $y_k = z_k$ for all $0 \leqq k \leqq \boldsymbol{n}(4)$. Repeating the same argument for the coefficients of $\boldsymbol{u}(3)^m$ in $y_k = z_k$, we deduce that the coefficients of $\boldsymbol{u}(3)^m\boldsymbol{u}(4)^k$ in both sides of (4) are equal. Repeating the same process once more we get that the coefficients of $\boldsymbol{u}(2)^p\boldsymbol{u}(3)^m\boldsymbol{u}(4)^k$ in both sides of (4) are equal, i.e.

$$\sum \{a_i\boldsymbol{u}(1)^{\boldsymbol{i}(1)} : \boldsymbol{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}, \boldsymbol{i}(2) = p, \boldsymbol{i}(3) = m, \boldsymbol{i}(4) = k\}$$
$$= \sum \{b_i\boldsymbol{u}(1)^{\boldsymbol{i}(1)} : \boldsymbol{0} \leqq \boldsymbol{i} \leqq \boldsymbol{n}, \boldsymbol{i}(2) = p, \boldsymbol{i}(3) = m, \boldsymbol{i}(4) = k\}.$$

Again we have two $\boldsymbol{u}(1)$-representations of the same integer from which Lemma 1 follows.

It may be noticed that the coefficient of any product of powers of $\boldsymbol{u}(1)$, $\boldsymbol{u}(2)$, $\boldsymbol{u}(3)$, $\boldsymbol{u}(4)$ in both sides of (4) are equal.

11. Lemma 2. *If u, v are canonical forms in $f_1, \ldots, f_k$, $f_1', \ldots, f_k'$ are as in the Theorem with $k, b(u), b(v) < s$, $(s+1)! \leqq t$, $(s+1)!t^{s+1} < p$ and $(s+1)p^{s+1} < q$ then u eq v iff $u(f_1', \ldots, f_k')(1) = v(f_1', \ldots, f_k')(1)$.*

Proof. Let $w(f_1', \ldots, f_k')(1) = w^*$ for any $w \in W$. Since if u eq v then $u = v$ is an identity in every ringoid, the lemma will be proved if we show that $u^* = v^*$ implies u eq v. The proof will be by induction on

$$D(u, v) = \max\{d(u), d(v)\} + \max\{b(u), b(v)\} \geqq 1. \tag{5}$$

If $D(u, v) = 1$, then $d(u) = d(v) = 0$ and $b(u) = b(v) = 1$. So $u = f$ and $v = g$, $f, g \in F$ and the lemma is immediate for this case.

Let the lemma be true for all canonical forms u, v with $D(u, v) < D$, $1 < D$ and let u, v be canonical forms with $D(u, v) = D$ and let

$$u^* = v^*. \tag{6}$$

Since u, v are of the form (2), (6) is of the form

$$\begin{aligned}(7)\qquad &\sum \Big\{t(i) \exp \Big(q; \sum \{r(ij)p^{m(ij)}(u_1^*(ij)+t)^s : 1 \leqq j \leqq k(i)\}\Big) : 1 \leqq i \leqq n\Big\} \\ &= \sum \Big\{t'(i) \exp \Big(q; \sum \{r'(ij)p^{m'(ij)}(v_1^*(ij)+t)^s : 1 \leqq j \leqq k'(i)\}\Big) : 1 \leqq i \leqq n'\Big\},\end{aligned}$$

where $m(ij)$ is the index of the element $f(ij)$, i.e. $1 \leqq m(ij), m'(ij) \leqq k$.

If one of the $u(ij)$ is simply $f(ij)$, then $u_1^*(ij) = 1$,

$$\sum \{t(i) : 1 \leqq i \leqq n\} \quad \text{and} \quad \sum \{t_i' : 1 \leqq i \leqq n'\} \leqq s < q.$$

Then, comparing the q-representations of $u^* = v^*$ in (7), we get that the coefficients of every power of q in both sides of (7) are the same. Let two powers of q in the left-hand side of (7) be equal, i.e.

$$\begin{aligned}(8)\qquad &\sum \{r(ij)p^{m(ij)}(u_1^*(ij)+t)^s : 1 \leqq j \leqq k(i)\} \\ &= \sum \{r(i'j)p^{m(i'j)}(u_1^*(i'j)+t)^s : 1 \leqq j \leqq k(i')\}.\end{aligned}$$

All $u_1^*(ij)$ and $u_1^*(i'j)$ are sums of powers of q whose coefficients do not contain any power of p or t and both $\sum\{r(ij) : 1 \leqq j \leqq k(i)\}$, and $\sum\{r(i'j) : 1 \leqq j \leqq k(i')\}$ are less than $s \leqq s! < t$.

The conditions of Lemma 1 are satisfied here. We infer that the coefficients of every power of p in both sides of (8) are the same, i.e.

$$\begin{aligned}(9)\qquad &\sum\{r(ij)(u_1^*(ij)+t)^s : 1 \leqq j \leqq k(i), m(ij) = r\}\\ &\qquad = \sum\{r(i'j)(u_1^*(i'j)+t)^s : 1 \leqq j \leqq k(i'), m(i'j) = r\}\end{aligned}$$

for all $1 \leqq r \leqq k$.

From (2), $u_1(ij)$, $u_1(i'j)$ are canonical forms of depth less than $d(u)$ and of width not exceeding that of u. Hence $D(u_1(ij), u_1(ij'))$, $D(u_1(i'j), u_1(i'j')) < D$. If in (9) $u_1^*(ij) = u_1^*(ij')$, then by the induction hypothesis $u_1(ij)$ eq $u_1(ij')$ and hence

$$u(ij) = f(ij) \circ u_1(ij) \operatorname{eq} f(ij') \circ u_1(ij') = u(ij')$$

$(f(ij) = f(ij') = f_r)$ which contradicts the writing of canonical form if $j \neq j'$. Thus all $u_1^*(ij)$, $1 \leqq j \leqq k(i)$, $m(ij) = r$ are distinct.

The same is true for all $u_1^*(i'j)$, $1 \leqq j \leqq k(i')$, $m(i'j) = r$. Comparing different powers of t (by Lemma 1) in (9) we get

$$\begin{aligned}&\sum\left\{\binom{s}{s-h} r(ij)(u_1^*(ij))^h : 1 \leqq j \leqq k(i); m(ij) = r\right\}\\ &\qquad = \sum\left\{\binom{s}{s-h} r(i'j)(u_1^*(i'j))^h : 1 \leqq j \leqq k(i'); m(i'j) = r\right\}, \qquad 0 \leqq h \leqq s.\end{aligned}$$

Dividing by $\binom{s}{s-h}$ we get

$$\begin{aligned}(10)\qquad &\sum\{r(ij)(u_1^*(ij))^h : 1 \leqq j \leqq k(i); m(ij) = r\}\\ &\qquad = \sum\{r(i'j)(u_1^*(i'j))^h : 1 \leqq j \leqq k(i'); m(i'j) = r\}, \qquad 0 \leqq h \leqq s.\end{aligned}$$

Again

$$s > \sum\{r(ij) : 1 \leqq j \leqq k(i)\}, \quad \sum\{r(i'j) : 1 \leqq j \leqq k(i')\}.$$

By the theory of symmetric functions, we deduce that, for some rearrangement of the terms $r(ij) = r(i'j)$, $u_1^*(ij) = u_1^*(i'j)$ for all j such that $m(ij) = m(i'j) = r$. Hence $u_1(ij)$ eq $u_1(i'j)$. But $f(ij) = f(i'j) = f_r$. Hence $u(ij)$ eq $u(i'j)$ and so

$$(u(ij))^{r(ij)} \operatorname{eq} (u(i'j))^{r(i'j)}.$$

Thus the equality of exponents of q in the left-hand side of (9) implies the equivalence of the corresponding products in the canonical form u.

From the writing of the canonical forms we should have the exponents of q for distinct i, $1 \leqq i \leqq n$, distinct, i.e. the left-hand side of (9) contains precisely n distinct powers of q. The same could be said about the right-hand side of (9), i.e. it contains precisely n' distinct powers of q. Since the coefficients of every power of q in both sides must be equal we get $n=n'$ and for some rearrangement of indices

$$\begin{aligned} &\sum \{r(ij)p^{m(ij)}(u_1^*(ij)+t)^s : 1 \leqq j \leqq k(i)\} \\ (11) \qquad &\qquad = \sum \{r'(ij)p^{m'(ij)}(v_1^*(ij)+t)^s : 1 \leqq j \leqq k'(i)\}, \\ &t(i) = t'(i), \qquad 1 \leqq i \leqq n. \end{aligned}$$

$d(v_1(ij))<d(v)$ and $b(v_1(ij))\leqq b(v)$ and so $D(u_1(ij), v_1(ij'))<D$. Using the same argument as above we get

$$(u(ij))^{r(ij)} \text{ eq } (v(ij))^{r'(ij)},$$

$1\leqq j\leqq k(i)=k'(i)$, $1\leqq i\leqq n=n'$ (up to a reordering of indices), i.e. u eq v.

The other part of Lemma 2 is immediate and this concludes the proof of Lemma 2.

12. Corollary 6. *If u, v are canonical forms then u* eq *v iff $u\equiv v$.*

If u eq v then $u\equiv v$ is obvious, the converse is also obvious if one notices that $u\equiv v$ implies that $u=v$ is an identity in N^N and hence $u(f_1',\ldots,f_k')$, and $v(f_1',\ldots,f_k')$ are equal elements and they have the same value at 1.

Now we conclude the proof of the Theorem. Let $u, v \in W$ and reduce u to a canonical form $K(u)$ and v to $K(v)$. We have $u\equiv K(u)$ and $v\equiv K(v)$. Since $b(K(u))\leqq c(r(u))<c(r(u+v))$, Lemma 2 can be applied to $K(u)$ and $K(v)$ for the given functions $f_1',\ldots,f_k'$ in the Theorem.

Corollary 7. *If $u, v \in W$ then $u\equiv v$ iff the canonical forms of u and v are equivalent.*

This solves also the word problem for the free ringoid.

IV. Ringoids with nullary operations.

13. The algorithm of the Theorem can be modified to solve the word problem for ringoids with nullary operations. We sketch out here the case where all 0, 1, e are present; the other cases are similar.

The word algebra W' is constructed as in n°5. The free ringoid with 0, 1, e generated by F is the factor algebra of W' by $\equiv'$, where $u\equiv' v$ iff u can be transformed to v by repeated use of the basic identities of ringoids with 0, 1 and e. Canonical forms are defined as in n°8; but instead of F, $F \cup \{0, 1, e\}$ is used. They should also be restricted to the following conditions: (having in mind (3)) all $u(ij)$ are of the form

(a) $f \circ (u)$, where $f \in F$ and $u-a$ canonical form, $u\neq e$,

(b) f or e, $f\in F$,

(c) 1 only in case $k(i)=1=s(ij)$,

(d) 0 only in case $1=n=k(1)=t(i)=s(ij)$.

Every word u can be reduced to a canonical form $K(u)$ such that $K(u)\equiv' u$.

All the results of §II can be reformulated for ringoids with 0, 1 and e. In place of N one should use N_0 and in substitution by functions on the nonnegative integers

0, 1, e must be substituted by the constant functions $0(x)=0$, $1(x)=1$ and the identical function $e(x)=x$, respectively.

14. It may be noted that the results of this paper could be used to solve the word problem for the free or numerical algebras, whose operations are a subset of $\{+, x, \circ, 0, 1, e\}$ and satisfying all the laws of ringoids with 0, 1, e except those in which occur any of the deleted operations. For the case of semirings this is essentially the well-known algorithm of elementary algebra.

References

1. G. Birkhoff, *Lattice theory*, 3rd ed., Amer. Math. Soc. Colloq. Publ., vol. 25, Amer. Math. Soc., Providence, R. I., 1967. MR **37** #2638.

2. G. Berman and R. J. Silverman, *Embedding of algebraic systems*, Pacific J. Math. **10** (1960), 777–786. MR **22** #11060.

3. P. M. Cohn, *Universal algebra*, Harper & Row, New York, 1965. MR **31** #224.

4. M. Davis, *Computability and unsolvability*, McGraw-Hill Series in Information Processing and Computers, McGraw-Hill, New York, 1958. MR **23** #A1525.

5. T. Evans, *The word problem for abstract algebras*, J. London Math. Soc. **26** (1951), 64–71. MR **12**, 475.

6. G. Grätzer, *Universal algebra*, Van Nostrand, Princeton, N. J., 1967. MR **40** #1320.

7. P. Hall, *Some word problems*, J. London Math. Soc. **33** (1958), 482–496. MR **21** #1331.

8. A. G. Kuroš, *Lectures on general algebra*, Fizmatgiz, Moscow, 1962; English transl., Chelsea, New York, 1963; Internat. Series of Monographs in Pure and Appl. Math., vol. 70, Pergamon Press, Oxford, 1965. MR **25** #5097; MR **28** #1228; MR **31** #3483.

9. S. Kleene, *Introduction to metamathematics*, Van Nostrand, Princeton, N. J., 1952. MR **14**, 525.

10. A. I. Mal′cev, *Algorithms and recursive functions*, "Nauka," Moscow, 1965; English transl., Wolters-Noordhoff, Groningen, 1970. MR **34** #2453.

University of Aarhus,
Aarhus, Denmark
University of Cairo,
Cairo, Egypt