DEFINING RELATIONS FOR FULL SEMIGROUPS OF FINITE TRANSFORMATIONS

Bjarni Jónsson

1. INTRODUCTION

A transformation f of a set I into itself is said to be *finite* if and only if $f(x) = x$ for all but finitely many elements x of I. Under the operation of composition the set F(I) of all finite transformations of I into itself is a semigroup having the identity map id_I as its identity element. As generators for F(I) we may take all the transpositions (x, y) and replacements (x/y) with $x, y \in I$ and $x \neq y$. Here (x/y) is the transformation that maps y onto x and leaves all the other elements of I fixed, while (x, y) is of course the permutation that interchanges x and y, leaving all the other elements fixed. By an *elementary transformation* we shall mean a transformation that is either a transposition or a replacement.

The purpose of this paper is to give a set of defining relations for F(I), taking the set of all elementary transformations as a generating set. The reason for taking this generating set rather than a smaller irredundant one is that the individual defining relations can then be given in a simple form particularly convenient for applications. This is illustrated in Section 4, where we outline a new proof of a theorem of Galler [1] concerning the relation between cylindric algebras and polyadic algebras.

2. CANONICAL REPRESENTATIONS

We consider a fixed set I consisting of at least three elements. By an *elementary sequence* we mean a finite sequence whose terms are elementary transformations. If $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ is an elementary sequence, then we let

$$a^\tau = a_0 a_1 \cdots a_{n-1}.$$

By a *representation* of a member f of F(I) we mean an elementary sequence a with $f = a^\tau$.

Since the set of all elementary transformations obviously generates F(I), every finite transformation f of I has a representation. We shall now single out certain representations of f that will be referred to as *canonical representations*. This concept is motivated by the consideration of the directed graph whose vertices are the elements of I and whose edges are in one-to-one correspondence with the elements of I in such a way that, for each x in I, the corresponding edge has x as its initial vertex and f(x) as its terminal vertex. Let J be the set of all members x of I such that $f^p(x) = x$ for some positive integer p. Clearly f maps J onto itself, and the restriction f' of f to J is a finite permutation. The graph of f' therefore consists of pairwise disjoint cycles, of which all but finitely many are degenerate, consisting of just one vertex.

Received April 5, 1961.

These investigations were supported in part by NSF Grant G8886.

For any x in I, the sequence x, f(x), $f^2(x)$, ⋯ must contain repetitions, and therefore $f^n(x) \in J$ for sufficiently large n. For x not in J, let p(x) be the smallest such positive integer n. If we now consider a fixed member y of J and all those members x of I - J for which $f^{p(x)}(x) = y$, then it is clear that the corresponding subgraph is a tree having y as its root. Thus the graph of f consists of pairwise disjoint cycles, all but finitely many of them degenerate, together with a finite number of finite trees whose roots are vertices on the cycles. This picture suggests a systematic although not unique way of representing f as a product of elementary transformations. Reading from right to left, we first represent f' as a product of transpositions (x, y) with $x, y \in J$, and then follow this by all the replacements (f(x)/x) with $x \in I - J$, the only restriction on their order being that if x and f(x) both belong to I - J, then $(f^2(x)/f(x))$ must precede (f(x)/x). In other words, we start at the bottom of each tree and work our way up. This condition is needed because $(f^2(x)/f(x))\,(f(x)/x)$ maps both x and f(x) onto $f^2(x)$, while $(f(x)/x)\,(f^2(x)/f(x))$ maps x onto f(x) and f(x) onto $f^2(x)$.

A formal definition of a canonical sequence will now be given. By a *defect* of an elementary sequence $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ we shall mean an ordered pair $\langle p, q \rangle$ of natural numbers p and q such that $p < q < n$ and one of the following conditions holds:

(1) a_p is a transposition and a_q is a replacement,

(2) $a_p = (x/y)$ and $a_q = (y, z)$,

(3) $a_p = (x/y)$ and $a_q = (y/z)$,

(4) $a_p = (x/y)$ and $a_q = (z/y)$,

where $x, y, z \in I$ and $x \neq y \neq z$. We say that $\langle p, q \rangle$ is a defect of a of *type* 1, 2, 3 or 4 in case it satisfies the condition (1), (2), (3) or (4), respectively. By a canonical sequence we mean an elementary sequence that has no defect.

The following auxiliary concept will also be used in the next section: Suppose $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ is an elementary sequence that has no defect of type 1. If, for some $r < n$, a_r is a transposition, then the smallest such r is called the *critical index* of a, and we let

$$a^\pi = a_r a_{r+1} \cdots a_{n-1};$$

but if all the terms a_r are replacements, then we call n the critical index of a, and let $a^\pi = id_I$.

The next lemma shows to what extent two canonical representations of the same finite transformations can differ from each other.

LEMMA A. *For any canonical sequences*

$$a = \langle a_0, a_1, \cdots, a_{m-1} \rangle \quad \textit{and} \quad b = \langle b_0, b_1, \cdots, b_{n-1} \rangle,$$

$a^\tau = b^\tau$ *if and only if* $a^\pi = b^\pi$, a *and* b *have the same critical index* r, *and the sequences*

$$a' = \langle a_0, a_1, \cdots, a_{r-1} \rangle \quad \textit{and} \quad b' = \langle b_0, b_1, \cdots, b_{r-1} \rangle$$

are obtained from each other by a permutation of the terms.

Proof. If r is the critical index of a, and $a_i = (u_i/v_i)$ for $i = 0, 1, \cdots, r-1$, then $v_0, v_1, \cdots, v_{r-1}$ are precisely those elements x of I for which $(a^\tau)^k(x) \neq x$ for $k = 1, 2, \cdots$, and for each $i < r$ we have

$$a^\tau(v_i) = u_i \quad \text{and} \quad a^\pi(v_i) = v_i,$$

while all the remaining elements x of I satisfy the condition $a^\tau(x) = a^\pi(x)$. From this and the corresponding statement concerning b the lemma readily follows.

3. THE MAIN THEOREM

We express our principal result in terms of homomorphisms of F(I) into semi-groups with identity. It is understood that under such a homomorphism the identity element id_I of F(I) is to map onto the identity element of the other semi-groups; that is, the identity element is treated as a distinguished element.

THEOREM. *In order for a map*

$$(x, y) \to [x, y], \qquad (x/y) \to [x/y]$$

of the elementary transformations of I *into a semi-group* S *with identity* e *to extend to a homomorphism of* F(I) *into* S *it is necessary and sufficient that the following conditions hold for all* $x, y, z, u \in I$ *with* $x \neq y \neq z \neq x$ *and* $y \neq u \neq z$:

(i) $[x, y] = [y, x]$, (ii) $[x, y][x, y] = e$,

(iii) $[x, y][x, z] = [y, z][x, y]$, (iv) $[x, y][x/y] = [y/z][x, y]$,

(v) $[x, y][x/y] = [y/x]$, (vi) $[x/y][u/z] = [u/z][x/y]$,

(vii) $[x/y][u/y] = [u/y]$.

Proof. The conditions (i) to (vii) are clearly necessary, since the corresponding relations for the elementary transformations are easily verified. The proof of the converse will be based on a series of lemmas. It will be assumed throughout that (i) to (vii) hold. The condition (i) will frequently be used without being explicitly mentioned.

LEMMA B. *For any distinct elements* x, y, z, u *of* I *the following conditions hold:*

(viii) $[x, y][z, u] = [z, u][x, y]$, (ix) $[x, y][z/u] = [z/u][x, y]$,

(x) $[x/y][x, y] = [x/y]$, (xi) $[x, y][z/x] = [x/y][z/x]$,

(xii) $[x/y][y/x] = [x/y]$, (xiii) $[x/y][y, z] = [z/y][x/z]$,

(xiv) $[x/y][y/z] = [x/y][x/z]$.

Proof of (viii). By (ii) and (iii),

$$[x, y][z, u] = [x, y][y, z][y, z][z, u] = [y, z][x, z][z, u][y, u]$$
$$= [y, z][z, u][x, u][y, u] = [z, u][y, u][y, u][x, y] = [z, u][x, y].$$

Proof of (ix). By (ii) to (iv),

$$[x, y][z/u] = [x, y][y, z][y, z][z/u] = [x, z][x, y][y/u][y, z]$$
$$= [x, z][x/u][x, y][y, z] = [z/u][x, z][x, z][x, y] = [z/u][x, y].$$

Proof of (x). By (ii) to (v),

$$[x/y][x, y] = [x/y][x, z][x, z][x, y] = [x, z][z/y][x, y][y, z]$$
$$= [x, z][y, z][y/z][x, y][y, z] = [x, z][y, z][x, y][x/z][y, z]$$
$$= [x, z][x, y][x, z][x/z][y, z] = [x, z][x, y][z/x][y, z]$$
$$= [x, z][x, y][y, z][y/x] = [x, z][x, z][x, y][y/x] = [x/y].$$

Proof of (xi) *and* (xii). By (v) and (vii),

$$[x/y][z/x] = [x, y][y/x][z/x] = [x, y][z/x],$$
$$[x/y][y/x] = [x, y][y/x][y/x] = [x, y][y/x] = [x/y].$$

Proof of (xiii). By (iii) to (v) and (xi),

$$[x/y][y, z] = [x, y][y/x][y, z] = [x, y][y, z][z/x]$$
$$= [y, z][x, z][z/x] = [y, z][x/z] = [z/y][x/z].$$

Proof of (xiv). By (iv) to (vi),

$$[x/y][y/z] = [x, y][y/x][y/z] = [x, y][y/z][y/x]$$
$$= [x/z][x, y][y/x] = [x/z][x/y] = [x/y][x/z].$$

Let g be the given map of the set of all elementary transformations into S, $g((x, y)) = [x, y]$ and $g((x/y)) = [x/y]$; and for any elementary sequence $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ let

$$h(a) = g(a_0)\, g(a_1) \cdots g(a_{n-1}).$$

The set S' of all elementary sequences is a free semigroup under juxtaposition, generated by the one-termed sequences and with the null sequence $\emptyset$ as its identity element. The function h is a homomorphism of S' into S, and the map $a \to a^\tau$ is a homomorphism of S' onto F(I). The theorem is equivalent to the assertion that, for all a, b in S', $a^\tau = b^\tau$ implies that h(a) = h(b). Each of the conditions (i) to (xiv) permits us in certain cases to replace a 2-termed segment $\langle a_{k-1}, a_k \rangle$ of a by another 2-, 1-, or 0-termed sequence without changing a^τ or h(a). A sequence obtained from a by a finite number of such operations will be called a *transform* of a. Since we shall frequently use inductive arguments, it is important to observe that a transform of a has at most the same number of terms as a. Thus if $x, y, z, u \in I$ are distinct, then each of the following replacements is permissible:

$$\langle (x, y), (x/z) \rangle \leftrightarrow \langle (y/z), (x, y) \rangle, \quad \langle (x/y), (y/x) \rangle \rightarrow \langle (x/y) \rangle,$$

$$\langle (x, y), (x, y) \rangle \rightarrow \emptyset;$$

but in the last two cases we are not permitted to go in the opposite direction.

LEMMA C. *Suppose* $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ *is a sequence of transpositions.*

(1) *If* $a^\tau = id_I$, *then* $\emptyset$ *is a transform of* a.

(2) *If* $u \in I$ *and* $a^\tau(u) = v \neq u$, *then there exists a transform*

$$b = \langle b_0, b_1, \cdots, b_{m-1} \rangle$$

of a *such that*

$$b_0 = (u, v), \quad b_i(u) = u \quad \textit{for } i = 1, 2, \cdots, m - 1,$$

and $b_i(x) = x$ *whenever* $x \in I$, $a^\tau(x) = x$ *and* $i < m$.

Proof. For $n = 0, 1$, this is trivial. Consider a given $n > 1$, assuming the statement to be true for all smaller values of n.

If $a^\tau = id_I$, and if we let $c = \langle a_1, a_2, \cdots, a_{n-1} \rangle$, then $c^\tau = a_0$ is a transposition (u, v), and we may apply the inductive hypothesis to infer that c has a transform $b = \langle b_0, b_1, \cdots, b_{m-1} \rangle$ such that $b_0 = (u, v)$ and, for $0 < i < m$, b_i leaves all the members of I fixed, except possibly v. Since a transposition moves two members of I, it follows that there can be no such terms b_i. Thus $m = 1$, $b = \langle b_0 \rangle = \langle a_0 \rangle$. Consequently $\langle a_0, a_0 \rangle$ is a transform of a, and according to (ii) so is $\emptyset$.

Under the hypothesis of (2), let k be the largest index such that $a_k(u) \neq u$. If $k = 0$, then $a_0 = (u, v)$. Consider the sequence $c = \langle a_1, a_2, \cdots, a_{n-1} \rangle$, and observe that $c^\tau(u) = u$ and $c^\tau(x) = x$ whenever $a^\tau(x) = x$. Reference to the inductive hypothesis easily leads to the desired conclusion; if $c^\tau \neq id_I$, we take in place of u an arbitrary element u' with $c^\tau(u') \neq u'$.

Finally suppose that $k > 0$. Then $a_{k-1} = (x, y)$ and $a_k = (z, u)$ with $x \neq y$ and $z \neq u$. We may also assume that $x \neq u$ and $y \neq z$. If $x = z$ and $y = u$, then we use (ii) to obtain an (n - 2)-termed transform of a, to which the inductive hypothesis may be applied. In the remaining three cases,

$$x = z, y \neq u, \quad x \neq z, y = u, \quad x \neq z, y \neq u,$$

we may in accordance with (iii) and (viii) replace $\langle a_{k-1}, a_k \rangle$ by

$$\langle (y, u), (x, y) \rangle, \quad \langle (z, u), (x, z) \rangle, \quad \langle (z, u), (x, y) \rangle,$$

respectively. In each case the resulting transform a' of a has the property that $k - 1$ is the largest index i such that $a_i'(u) \neq u$. Iteration of this process therefore leads either to the first subcase, or else to the case $k = 0$.

The lemma now follows by induction.

LEMMA D. *Every elementary sequence has a canonical transform.*

Proof. For $j = 1, 2, 3, 4$, we shall prove the following statement:

(D_j) *If an* n*-termed elementary sequence* $a = \langle a_0, a_1, \cdots, a_{n-1} \rangle$ *has no defect of type less than* j, *then* a *has a transform* a' *that either has fewer than* n *terms or else has no defect of type less than or equal to* j.

Proof of (D_1). If a has a defect of type 1, then there exists $p < n - 1$ such that a_p is a transposition and a_{p+1} is a replacement, say $a_p = (x, y)$ and $a_{p+1} = (z/u)$ with $x \neq y$ and $z \neq u$. We may also assume that $x \neq u$ and $y \neq z$. If $x = z$ and $y = u$, we use (v) to obtain an (n - 1)-termed transform of a, but in the remaining three cases,

$$x = z,\ y \neq u, \qquad x \neq z,\ y = u, \qquad x \neq z,\ y \neq u,$$

we employ (iv), (xi) and (ix) to obtain a transform a' of a that either has fewer transpositions than a, or else has the same number of transpositions but has fewer defects of type 1. Iteration of this process therefore leads either to the first case or else to a transform that has no defect of type 1.

Proof of (D_2). Let r be the critical index of a. By Lemma B, applied to the sequence $\langle a_r, a_{r+1}, \cdots, a_{n-1} \rangle$, we may assume that if $a^{\pi}(x) = x$, then $a_i(x) = x$ for $i = r, r + 1, \cdots, n - 1$. Therefore, if a has a defect of type 2, then for some $p < r$, a_p has the form $a_p = (x/y)$, where $a^{\pi}(y) = z \neq y$. Choose the largest p for which this is true. Again using Lemma B, we may assume that $a_r = (y, z)$.

For $p < k < r$, we have $a_k = (u_k/v_k)$ with $v_k \neq u_k, y, z$. Letting $u'_k = a_r(u_k)$ and $a'_k = (u'_k/v_k)$, we see by (iv) and (ix) that $\langle a_k, a_r \rangle$ may be replaced by $\langle a_r, a'_k \rangle$. Doing this successively for $k = r - 1, r - 2, \cdots, p + 1$, and then replacing $\langle a_p, a_r \rangle$ by $\langle (z/y), (x/z) \rangle$ if $x \neq z$, but by $\langle (x/y) \rangle$ in case $x = z$, we obtain a transform of a that has no defects of type 1, and has fewer transpositions than a. Iteration of this process leads to the desired result.

Proof of (D_3). Assuming that a is an n-termed elementary sequence that has no defects of type 1 or 2, but does have a defect of type 3, we associate with a three natural numbers p, q and s. First, p and q are so defined that $\langle p, q \rangle$ is a defect of a of type 3, with q as small as possible and, for the given value of q, with p as large as possible. Secondly, s is defined to be the largest integer with $p \leq s \leq q$ for which there exist $u_p, u_{p+1}, \cdots, u_{s+1} \in I$ such that $a_k = (u_{k+1}/u_k)$ for $k = p, p + 1, \cdots, s$. The objective is to show that a has a transform a' which satisfies one of the following three conditions:

(α) a' has fewer than n terms,

(β) a' has no defect of type 1, 2, or 3,

(γ) a' has no defect of type 1 or 2, but does have a defect of type 3, and the associated numbers p', q' and s' are such that either $q' > q$, or $q' = q$ and $p' > p$, or else $q' = q$, $p' = p$ and $s' < s$.

Observe that $u_p, u_{p+1}, \cdots, u_s$ are distinct. If $s = q$, then $u_{q+1} = u_p$. By $q - p - 1$ applications of (xiii), followed by a single application of (xii), we find that the segment $\langle a_p, a_{p+1}, \cdots, a_q \rangle$ can be replaced by the sequence

$$\langle (u_{p+1}/u_p), (u_{p+1}, u_{p+2}), (u_{p+2}, u_{p+3}), \cdots, (u_{q-1}, u_q) \rangle,$$

and since the resulting transform of a has fewer than n terms, our assertion is proved for this case.

Next suppose $s = q - 1$. Then $a_q = (u_p/x)$, where $x \neq u_p, u_q$. If $x = u_k$ with $p < k < q$, we apply (vi) $q - k - 1$ times and then (vii) once, to replace the segment $\langle a_k, a_{k+1}, \cdots, a_q \rangle$ by the shorter sequence $\langle a_q, a_{k+1}, a_{k+2}, \cdots, a_{q-1} \rangle$; but if $x \neq u_k$ for $k = p + 1, p + 2, \cdots, q - 1$, then we use (vi) $q - p - 1$ times and (xiv) once, to replace the segment $\langle a_p, a_{p+1}, \cdots, a_q \rangle$ by the sequence

$$\langle a_p, (u_{p+1}/x), a_{p+1}, a_{p+2}, \cdots, a_{q-1} \rangle .$$

The resulting transform a' of a clearly has no defects of type 1 or 2. Furthermore, if a' does have a defect of type 3, then it is not difficult to show that the associated number q' is greater than q.

Finally, suppose that $s < q - 1$. Then $a_{s+1} = (x/y)$ with $y \neq x, u_{s+1}$ and $x \neq u_s$. If $y = u_s$, then a_s may be dropped from the sequence, according to (vii); but if $y \neq u_s$, then a_s and a_{s+1} may be interchanged, according to (vi). For the resulting transform a' of a, we have $q' = q$ and $p' = p + 1$ in case $s = p$, but $p' = p$ and $s' = s - 1$ in case $s > p$. Thus (γ) applies in this case.

Thus in all cases one of the conditions (α), (β), (γ) applies. By an iteration of this process we must eventually come to a case in which either (α) or (β) holds, and this proves (D_3).

Proof of (D_4). If a has no defect of type 1, 2, or 3, but does have a defect $\langle p, q \rangle$ of type 4, choose p and q so that p is as large as possible. For $k = p, p + 1, \cdots, q$ we have $a_k = (u_k/v_k)$, where $v_p = v_q$. If $p < k < q$, then $u_q \neq v_k$ and $v_q (= v_p) \neq u_k$, because a has no defect of type 3, and also $v_q \neq v_k$ by the choice of p. By (vi) we may therefore successively interchange a_k and a_q for $k = q - 1, q - 2, \cdots, p + 1$, and from the sequence so obtained we may drop a_p, according to (vii), thereby obtaining a transform of a having only $n - 1$ terms.

This completes the proof of (D_1) to (D_4), and the lemma follows by induction.

LEMMA E. *Any two elementary sequences that represent the same finite transformation have a common transform.*

Proof. By Lemma D we may assume that the given sequences are canonical, and by Lemma A we may further assume that the terms are either all transpositions or else all replacements. In the former case the conclusion is an easy consequence of Lemma C, and we therefore consider only the latter case.

If the two given sequences are

$$a = \langle a_0, a_1, \cdots, a_{m-1} \rangle \quad \text{and} \quad b = \langle b_0, b_1, \cdots, b_{n-1} \rangle ,$$

then according to Lemma A, $m = n$, and there exists a permutation ϕ of the indices $0, 1, \cdots, m - 1$ such that $b_i = a_{\phi(i)}$ for $i < m$. If $a_i = (u_i/v_i)$ for $i = 0, 1, \cdots, m - 1$, then $v_0, v_1, \cdots, v_{m-1}$ are distinct and

(1) $$u_q \neq v_p \quad \text{and} \quad u_{\phi(q)} \neq v_{\phi(p)} \quad \text{whenever } p \leq q < m .$$

Assuming that ϕ is not the identity permutation, let s be the smallest index such that $\phi(s) \neq s$. Then $s = \phi(t)$, where $s < t < m$, therefore $\phi(t - 1) > s = \phi(t)$, and it follows by (1) that

$$u_{\phi(t-1)} \neq v_{\phi(t)} \quad \text{and} \quad u_{\phi(t)} \neq v_{\phi(t-1)} .$$

By (vi) we may therefore interchange the terms b_{t-1} and b_t of b. The resulting transform b' of b is canonical, for in general, if we interchange two successive terms b_{t-1} and b_t of a canonical sequence b, the new sequence b' is canonical unless $\langle t-1, t \rangle$ is a defect of b', which is not the case in the present situation.

The sequence b' is obtained from a by the permutation ϕ' of the indices, where $\phi'(t-1) = \phi(t) = s$, $\phi'(t) = \phi(t-1)$, and $\phi'(k) = \phi(k)$ for $k \neq t-1, t$. Assuming that ϕ' is not the identity permutation, let s' be the smallest index such that $\phi'(s') \neq s'$, and let t' be the index with $\phi'(t') = s'$. Since $\phi'(k) = \phi(k) = k$ for $k < s$, we have $s < s'$. If $t = s+1$, then $\phi'(s) = s$, so that $s < s'$; but if $t > s+1$, then $s' = s$ and $t' = t-1$. Induction on $n - s$ and t therefore shows that in the present case a is actually a transform of b.

Our theorem is an immediate consequence of this last lemma; for if a and b are two elementary sequences with $a^T = b^T$, then they have a common transform c, and it follows that $h(a) = h(c) = h(b)$.

4. APPLICATIONS TO CYLINDRIC ALGEBRAS

We recall that a *cylindric algebra* is a Boolean algebra A with certain distinguished elements $d_{i,j}$ and unary operations C_i, where i and j run through some set I, such that the following conditions hold whenever $a, b \in A$, $i, j, k \in I$, and $i \neq k \neq j$:

$$C_i(0) = 0, \qquad a \leq C_i(a), \qquad C_i(aC_i(b)) = C_i(a)\,C_i(b),$$

$$C_i\,C_j = C_j\,C_i, \qquad d_{i,j} = 1, \qquad C_k(d_{i,k}\,d_{k,j}) = d_{i,j},$$

$$C_i(ad_{i,k})\,C_i(bd_{i,k}) = C_i(abd_{i,k}).$$

The cardinal of I is called the *dimension* of the cylindric algebra, and the algebra is said to be *locally finite* provided for each $a \in A$ there are only finitely many $i \in I$ with $C_i(a) \neq a$.

In the investigations of Galler [1] into the connection between cylindric algebras and polyadic algebras, the problem arose of introducing into a locally finite, infinite-dimensional cylindric algebra an operation corresponding to the logical operation of substitution. This should be a homomorphism of F(I) into the semigroup of all functions on A into itself. The logical analogue dictates what the images of the elementary transformations should be, and the principal difficulty consists in showing that the map can be extended to a homomorphism. The direct proof of this fact, which was outlined by Galler [1], is rather involved. We shall now indicate briefly how a proof of this result can be based on the principal theorem of this paper.

The result in question can be stated as follows.

THEOREM. *For any locally finite, infinite-dimensional cylindric algebra* $\langle A, d_{i,j}, C_i \rangle_{i,j \in I}$ *there exists a homomorphism* S *of* F(I) *into the semigroup of all functions on* A *into itself such that for all* i, j, r ∈ I *with* $i \neq j \neq r \neq i$ *and for all* $a \in A$ *with* $C_r(a) = a$.

$$S_{(i/j)}(a) = C_j(d_{i,j}a), \qquad S_{(i,j)}(a) = S_{(j/r)}\,S_{(i/j)}\,S_{(r/i)}(a).$$

(In order to qualify as a substitution, the map S must of course satisfy certain additional conditions. These are, however, easily verified, see for example Galler [1].)

Outline of proof. Given $i, j \in I$ with $i \neq j$, let

$$[i/j](a) = C_j(d_{i,j}\, a) \qquad \text{for all } a \in A .$$

Using various known elementary arithmetic properties of cylindric algebras (see for example Galler [1] or Henkin and Tarski [2]), one easily shows that the conditions (vi), (vii), (xii), (xiv) are satisfied. We would also like to define the function $[i, j]$ on A into itself in such a way that

$$[i,j](a) = [j/r][i/j][r/i](a) \qquad \text{for all } a \in A,$$

where for each a in A the corresponding member r of I is chosen so that $C_r(a) = a$ and $i \neq r \neq j$; but it must be ascertained that this definition is unambiguous and does not depend on the particular element r that is chosen. For this purpose we first verify that, with the above restrictions on r,

$$[i/r][r/j](a) = [i/j](a) . \tag{1}$$

Assuming now that $i, j, r, s \in I$ are distinct and that $a \in A$ is such that

$$C_r(a) = C_s(a) = a ,$$

we infer that

$$[j/s][i/j][s/i](a) = [j/s][i/j][s/r][r/i](a)$$

$$= [j/s][s/r][i/j][r/i](a) = [j/r][i/j][r/i](a) .$$

In the last step, use is made of the facts that the set of all $x \in A$ with $C_s(x) = x$ is closed under the Boolean operations and under the operations C_i, and that it contains all the elements $d_{i,j}$ with $i, j \neq s$. Thus in the present case the element

$$b = [i/j][r/i](a)$$

belongs to this set, and (1) can be used with r and a replaced by s and b.

After the proposed definition of $[i, j]$ has been shown to be unambiguous, it only remains to verify the conditions (i) to (v). In each case the proof, based primarily on (vi), (vii), (xii) and (xiv), and on (1), is straight-forward and offers no difficulty. Once the conditions (i) to (vii) have been established, the existence of the desired homomorphism follows from our main theorem.

REFERENCES

1. B. A. Galler, *Cylindric and polyadic algebras*, Proc. Amer. Math. Soc. 8 (1957), 176-183.

2. L. Henkin and A. Tarski, *Cylindric algebras*, Proc. of Symposia in Pure Math. 2 (1961), 83-113.

The University of Minnesota