T H E U N I V E R S I T Y O F M I C H I G A N

COLLEGE OF LITERATURE, SCIENCE, AND THE ARTS
Department of Communication Sciences

TOWARD A HOMOLOGICAL ALGEBRA OF AUTOMATA

Yehoshafat Give'on

ORA Projects 03105 and 06689

under contract with:

U. S. ARMY RESEARCH OFFICE (DURHAM)
GRANT NO. DA-ARO(D)-31-124-G588, PROJECT NO. 4049-M
DURHAM, NORTH CAROLINA

and

DEPARTMENT OF THE NAVY
OFFICE OF NAVAL RESEARCH
CONTRACT NO. Nonr-1224(21)
WASHINGTON, D.C.

administered through:

OFFICE OF RESEARCH ADMINISTRATION ANN ARBOR

February 1965

TABLE OF CONTENTS

TOWARD A HOMOLOGICAL ALGEBRA OF AUTOMATA I:

1. The Representation and Completeness Theorem for Categories of Abstract Automata

ABSTRACT

In this paper the author formulates the categorical theory of abstract automata. Two immediate basic problems are posed. First, one wonders how restricted the study of abstract automata is when one confines himself to those properties which are formulated by means of the notions of category theory only. This is a mathematical question whose answer should be proved. The author proves the completeness of the categorical study of abstract automata for a wide class of input monoids, a class which includes all types of monoids employed in the theory of finite automata. In order to get this result, a general representation theorem for abstract automata is derived.

The second question is psychological. How well does the categorical study of automata suit our intuitions and our problem? The answer to such a problem is not a matter of proof. The development presented in this paper has convinced the author of the potentiality of this new approach toward automata. Thus, this paper serves as a prelude to a series of papers which will exploit homological and categorical algebra methods for the sake of a mathematical theory of automata.

0. INTRODUCTION

0.1 In this paper we represent automata in a general domain of systems which can be regarded as "input" or "recognition" systems. By the provision of suitable homomorphisms for such systems we get a category, denoted by $\mathcal{A}$.

Our main concern in this paper is to answer the following question: is a category-theoretic study of $\mathcal{A}$ sufficient for the study of automata represented by input systems? We are able to prove that the complete category-theoretic study of $\mathcal{A}$ is a complete study of $\mathcal{A}$. To use our terms, we prove that $\mathcal{A}$ is categorically complete.

0.2 In addition to the proof of the completeness theorem (in the sense defined in the sequel) for $\mathcal{A}$ we get the following results.

A representation theorem for automata and input systems in general, is derived. It is proved that every such a system is isomorphic to a system whose states are functions taken from a specific standard family of functions, and whose transition function is essentially function composition.

The manner in which we develop our presentation suggests a close analogy between automata theory and the almost classical theory of modules and abelian categories. Results which follow this suggestion, like the study of composition series of automata and extension theory for automata will appear in forthcoming papers.

These results dictate in fact a thorough study of the category of automata (as defined in this paper), which will be covered in a series of forthcoming papers.

0.3 Some elementary acquaintance with category theory is needed.

In particular we shall make use of the following notions:

(i) Category, its objects and its morphisms.

(ii) Covariant and contravariant functors.

(iii) Epic, monic, and isomorphism morphisms versus surjective, injective, and bijective functions.

(iv) Right and left equivalence of morphisms; subobjects and quotient objects versus sub-systems and quotient systems.

(v) Universal and couniversal diagrams.

The reader who is not familiar with these notions is referred to the literature on homological algebra and on category theory. (E.g.: Eilenberg and MacLane 1945, Cartan and Eilenberg 1956, Northcott 1960, MacLane 1963, Freyd 1964, Hilton 1964, MacLane 1964.)

0.4 In general we use the ordinary notation and conventions used in algebra.

In particular, we shall apply the following scheme for explicit description of functions:

$$\phi \ : \ T_1 \to T_2 \ : \ t \to t'$$

(This will always mean that ϕ is a function from T_1 to T_2 such that for all $t \in T_1$: $\phi(t) = t'$.)

We shall intentionally omit the universal quantifications like "for all $w \in W$" and "for all $s \in S_A$", whenever we feel that such an omission is agreeable.

0.5 A scheme of definition Q(x) of predicates in categories is said to be categorical iff its only nonlogical primitive is morphism composition. For example the notion of "x is a monic morphism" is defined by means of a categorical scheme: "x is a morphism which is left cancellable under morphism composition".

0.6 A predicate Q'(x) in a specific category $\mathcal{C}$ is said to be <u>represented</u> by the categorical scheme Q(x) iff Q'(x) is logically equivalent with Q(x) in $\mathcal{C}$. For example "x is an epimorphism" in any abelian category is represented by the scheme "x is epic" which is categorical (since it is defined as "x is a morphism which is right cancellative under morphism composition").

Note that "x is an epimorphism" in the category of monoids is <u>not</u> represented by "x is epic".

0.7 A category $\mathcal{C}$ is said to be <u>categorically complete</u> iff any predicate in $\mathcal{C}$ (either of morphisms or of objects through their identity morphisms, cf. Freyd, 1964) which is invariant under isomorphisms of $\mathcal{C}$, is represented by means of categorical schemes.

0.8 For any input monoid W we define a category $\mathcal{A}_W$ of abstract automata with W as input. We shall see that for a wide class of monoids W, the category $\mathcal{A}_W$ is categorically complete, by proving that for any automaton A in $\mathcal{A}_W$ (i.e., any object of $\mathcal{A}_W$) one can construct (though not in an effective manner) by means of categorical predicates in $\mathcal{A}_W$, an automaton Mor(A) which is isomorphic to A. A more general treatment of this problem will be given in a forthcoming paper.

1. THE CATEGORY $\mathbf{A}_W$

1.1 Following Rabin-Scott's model for finite automata (Rabin and Scott 1959), we are interested in systems of the form

$$A = (S_A \times W \xrightarrow{\tau_A} S_A)$$

where

(i) S_A is any non empty set, to be called the <u>set of states of A</u>;

(ii) W is any monoid (with 1_W as its identity element), <u>the input monoid of A</u>;

(iii) $\tau_A \ : \ S_A \times W \to S_A \ : \ (s, w) \to \tau_A(s,w)$ is a function, <u>the transition function of A</u>, satisfying the following two compatibility requirements:

$(iii)_1$ $\tau_A(s, 1_W) = s$,

$(iii)_2$ $\tau_A(s, w_1w_2) = \tau_A(\tau_A(s, w_1), w_2)$.

1.2 Thus the input-to-state-transition part of a Rabin-Scott's automaton, or of a sequential machine with output, is such a system with the free monoid generated by the input alphabet as its input monoid.

A seemingly different model for automata was suggested by Büchi (Büchi 1960). Namely that of monadic algebras (Birkhoff 1935). Following this suggestion one can directly apply the methods of abstract algebra to automata theory (Büchi 1960, Thatcher 1963). In particular a definition of homomorphism of automata is derived as a special instance of homomorphisms of abstract algebras. In fact, Büchi and Wright (Büchi 1960) were the first to define homomorphisms for automata and to stress the importance of the study of automata under homomorphisms.

Still, one can derive in a very natural manner, a suitable definition of homomorphisms of systems as defined above. To be explicit, a homomorphism $A \xrightarrow{f} B$ is defined to be determined by the function $f : S_A \to S_B$ iff the following diagram is commutative.

$$\begin{array}{ccc} S_A \times W & \xrightarrow{\tau A} & S_A \\ f \Big\downarrow \quad \Big\downarrow i_W & & \Big\downarrow f \\ S_B \times W & \xrightarrow{\tau B} & S_B \end{array}$$

By means of a functional equation the commutativity of the diagram amounts to

$$f \circ \tau_A = \tau_B \circ (f \times i_W) \quad ,$$

where i_W is the identity function of W and f x i_W is the cartesian product of the functions f and i_W:

$$(f \times i_W)(s, w) = (f(s), w) \quad .$$

It is a matter of a straightforward verification to realize that:

1.2.1 PROPOSITION: The class of systems defined in 1.1 as objects, together with the homomorphisms defined above as morphisms, is a category.

1.2.2 On the other hand, the class of monadic algebras with operators over W (Give'on, 1964) together with their homomorphisms (Birkhoff, 1935), also forms a category.

1.2.3 These two categories are isomorphic. Hence the only difference between these two models can be regarded as a difference in notation. Our forthcoming change of notation, identifies these two categories.

1.3 The systems defined in 1.1 are in fact sets with (a monoid W of) operators, a natural generalization of the concept of groups with (a ring of) operators. This leads us to the use of the following common algebraic notation:

$$s \underset{A}{*} w = \tau_A(s, w)$$

(sometimes we may even write just s•w wherever no confusion is possible).

Thus the compatibility requirements for transition functions are the well known axioms of modules (for the multiplication by scalars):

$$s \cdot 1 = s \quad \text{and} \quad s \cdot (w_1 w_2) = (s \cdot w_1) \cdot w_2$$

Whereas a function $f : S_A \to S_B$ is now said to <u>determine a morphism</u> $A \xrightarrow{f} B$ of <u>automata</u> iff

$$f(s \underset{A}{\circ} w) = f(s) \underset{B}{\circ} w$$

1.4 Let us denote the category under discussion (with a fixed monoid W) by $\mathcal{A}_W$. The objects of $\mathcal{A}_W$ will be referred to as "automata" even though the term automaton is used in a more specific context. Naturally, we omit the subscript W whenever it does not cause any confusion.

1.5 In order to be able to prove the completeness of $\mathcal{A}_W$ we have to be acquainted with some categorical predicates in $\mathcal{A}_W$.

1.6 The proofs of the following two propositions are exercises in verification of definitions and they are left for the reader.

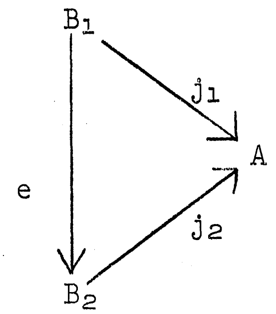
1.6.1 PROPOSITION: In the category $\mathcal{A}_W$ the (morphism) predicates of being surjective, injective or bijective are categorical and they are represented by the categorical schemes of being epic, monic or an isomorphism (resp.).

1.6.2 Naturally, an automaton A is said to a subautomaton of B, in symbols, $A \subseteq B$, iff S_A is a stable subset of S_B in B and the transition function τ_A of A is the restriction of τ_B of B to $S_A \times W$.

1.6.3 PROPOSITION: In the category $\mathcal{A}_W$ the set of all subautomata of any automaton A, as a predicate of automata, is categorical. It is represented by the right-equivalence classes of all monic morphisms with range A.

In fact, any two monic morphisms $B_1 \xrightarrow{j_1} A$ and $B_2 \xrightarrow{j_2} A$ are right-equivalent iff B_1 and B_2 are isomorphic and $j_1(S_{B_1}) = j_2(S_{B_2})$.

1.6.4 Note that $B_1 \xrightarrow{j_1} A$ and $B_2 \xrightarrow{j_2} A$ are right equivalent iff there is an isomorphism $B_1 \xrightarrow{e} B_2$ for which the following diagram is commutative.



1.7 If we allow an empty automaton ϕ_W to be an object of $\mathcal{A}_W$ with a family of morphisms $\phi_W \xrightarrow{j\phi} A$, one for each automaton A, with the stipulation

$$\phi_W \xrightarrow{j\phi} A \xrightarrow{f} B = \phi_W \xrightarrow{j\phi} B \quad ,$$

we get that ϕ_W is a subobject of any automaton A and it is represented by the stipulated morphism (which turns to be monic) $\phi_W \xrightarrow{j\phi} A$.

1.7.1 Furthermore, SUB(A), defined to be the set of all subautomata of A, is a complete lattice:

Let $\{A_\alpha\}$ be any family of subautomata of A then

$$\bigcap_\alpha A_\alpha \text{ is defined by } S_{\bigcap_\alpha A_\alpha} = \bigcap_\alpha S_{A_\alpha},$$

and

$$\bigcup_\alpha A_\alpha \text{ is defined by } S_{\bigcup_\alpha A_\alpha} = \bigcup_\alpha S_{A_\alpha}.$$

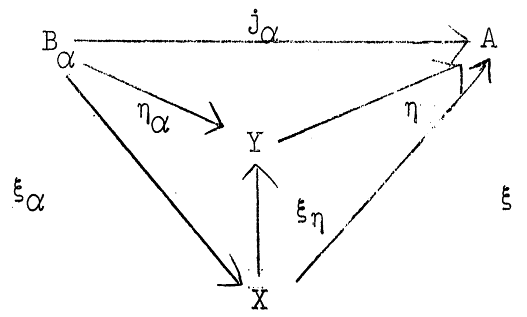
1.8 In order to verify that the predicate "X is isomorphic in $\mathcal{A}_W$ to the union of the family $\{A_\alpha\}$ of subautomata of A" is categorical, we assume that a family of monic morphisms

$$\{B_\alpha \xrightarrow{j_\alpha} A\}$$

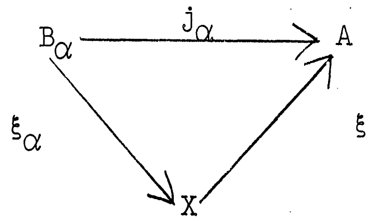
is given. Then we define $\sum_\alpha B_\alpha \xrightarrow{\sum_\alpha j_\alpha} A$ to be the right-equivalence class of any $X \xrightarrow{\xi} A$ provided that:

(i) for any α there is a monic $B_\alpha \xrightarrow{\xi_\alpha} X$ with $\xi\xi_\alpha = j_\alpha$;

(ii) if $Y \xrightarrow{\eta} A$ is any monic such that there exists a family of monic morphisms $B_\alpha \xrightarrow{\eta_\alpha} Y$ for which $\eta\eta_\alpha = j_\alpha$, then there is a monic $X \xrightarrow{\xi_\eta} Y$ for which the following diagram is commutative.



(That is, the diagram



is <u>universal</u> around X.)

1.8.1 To realize that we have represented the predicate "X is isomorphic in $\mathcal{A}_W$ to the union of the family $\{A_\alpha\}$ of subautomata of A", note that we have applied Prop. 1.6.3 to the definition of $\bigcup_\alpha S_{A_\alpha}$ as "the minimal subset of S_A which includes all S_{A_α} as subsets".

1.9 A dual construction yields the categoricity of "X is isomorphic to $\bigcap_{\alpha} A_{\alpha}$".

2. THE REPRESENTATION THEOREM FOR $\mathcal{A}_W$

2.1 Clearly, W can be regarded as an automaton by itself. We denote by M_W the automaton defined by

$$\begin{cases} S_{M_W} = W & ; \\ \tau_{M_W}(w_1, w_2) = w_1 \circ w_2 = w_1 w_2 & . \end{cases}$$

Obviously M_W is an object of $\mathcal{A}_W$ just because W is a monoid. We expect M_W to play a very significant role in $\mathcal{A}$, a role comparable to that of Z, the group of integers, in the category of abelian groups.

2.2 LEMMA: For any object A of $\mathcal{A}$, the map

$$Mor \; : \; S_A \to Hom(M_W, A) \; : \; s \to f_s(: \; W \to S_A \; : \; w \to s \circ w)$$

from the set of states of A to the set of all morphisms from M_W to A, is bijective.

Proof: For any $w_1, w_2 \in W$ we have

$$f_s(w_1 \circ w_2) = f_s(w_1 w_2) = s \circ w_1 w_2 = (s \circ w_1) \circ w_2$$

$$= f_s(w_1) \circ w_2 \quad .$$

Hence f_s determines a morphism $M_W \xrightarrow{f_s} A$.

If $f_{s_1} = f_{s_2}$ then in particular $f_{s_1}(1_W) = f_{s_2}(1_W)$, and so

$$s_1 = s_1 \cdot 1_W = f_{s_1}(1_W) = f_{s_2}(1_W) = s_2 \cdot 1_W = s_2 \quad .$$

On the other hand, for any morphism $M_W \xrightarrow{g} A$, since we have

$$g(w_1) \cdot w_2 = g(w_1 w_2)$$

we have in particular

$$f_{g(1_W)}(w) = g(1_W) \cdot w = g(w) \quad .$$

Hence for any morphism $M_W \xrightarrow{g} A$ we have

$$\mathrm{Mor}(g(1_W)) = f_{g(1_W)} = g \quad .$$

This completes the proof that Mor is bijective.

2.3 In particular

$$\mathrm{Mor} \; : \; W \to \mathrm{Hom}(M_W, M_W)$$

is also bijective. Furthermore, since $f_w(w') = ww'$, we have also

$$f_{w_1} \cdot f_{w_2} = f_{w_1 w_2} \quad .$$

2.3.1 <u>COROLLARY</u>: The monoid $\mathrm{End}(M_W)$, whose carrier (set of elements) is $\mathrm{Hom}(M_W, M_W)$, with function composition as its operation, is isomorphic to W under

$$\mathrm{Mor} \; : \; W \to \mathrm{End}(M_W) \quad .$$

2.4 For any object A of $\mathcal{A}$ we define the system Mor (A) by

$$\begin{cases} S_{Mor(A)} = Hom(M_W, A) & ; \\ g \circ w = g \circ f_w & . \end{cases}$$

2.5 THEOREM (The representation theorem for $\mathcal{A}_W$). For any automaton A, the system Mor(A) is an automaton and

$$A \xrightarrow{Mor} Mor(A)$$

is an isomorphism which is determined by

$$Mor : S_A \to Hom(M_W, A) : s \to f_s .$$

Proof: Clearly we have

$$(f_s \circ f_w)(w') = f_s(ww') = s.ww' = (s.w).w'$$

$$= f_{s \circ w}(w') ;$$

hence $f_s \circ f_w = f_{s \circ w}$, and therefore

$$Mor(s \circ w) = f_{s \circ w} = f_s \circ f_w = f_s \circ w = Mor(s) \circ w ,$$

which shows that Mor determines a morphism of A into Mor(A). The rest of the theorem follows from our previous statements.

2.6 We can supplement Mor so that it becomes a functor Mor : $\mathcal{A} \rightsquigarrow \mathcal{A}$. This can be done naturally by defining

$$\mathrm{Mor}(A) \xrightarrow{\mathrm{Mor}(g)} \mathrm{Mor}(B)$$

for any morphism $A \overset{g}{\to} B$, as determined by

$$\mathrm{Mor}(g) \;:\; \mathrm{Hom}(M_W, A) \to \mathrm{Hom}(M_W, B) \;:\; f_s \to g \circ f_s \quad .$$

Clearly Mor: $\mathcal{A} \rightsquigarrow \mathcal{A}$ is a covariant functor of $\mathcal{A}$ into itself.

2.7 <u>LEMMA</u>: Let $A \overset{g}{\to} B$ be any morphism of automata, then for any $s \in S_A$ we have

$$g \circ f_s = f_{g(s)} \quad .$$

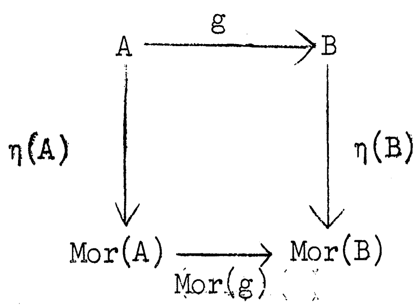
<u>Proof</u>: $(g \circ f_s)(w) \;=\; g(s \cdot w) \;=\; g(s) \cdot w \;=\; f_{g(s)}(w) \quad .$

2.7.1 <u>COROLLARY</u>: Mor: $\mathcal{A} \rightsquigarrow \mathcal{A}$ is a covariant functor of $\mathcal{A}$ into itself which is naturally equivalent by

$$\eta(A) \;=\; (A \xrightarrow{\mathrm{Mor}} \mathrm{Mor}(A))$$

to the identity functor of $\mathcal{A}$.

<u>Proof</u>: By Lemma 2.7, for any morphism $A \overset{g}{\to} B$, the following diagram is commutative.



2.8 In addition to End(A), the monoid of the morphisms $A \to A$ with respect to function composition, there is a more often applied monoid which is associated with A. Namely it is M(A) the monoid of transitions associated with A in the following manner.

For any object we define

$$t \;:\; W \to S_A^{S_A} \;:\; w \to \tau_w;\ \tau_w : \quad S_A \to S_A \;:\; s \to s\circ w$$

and clearly we have $\tau_{w_1} \circ \tau_{w_2} = \tau_{w_2 w_1}$. Thus t(W) is a submonoid of $S_A^{S_A}$ the monoid of all functions from S_A to S_A. We define

$$M(A) \;=_{df} \{t(w) \;:\; w \in W\}$$

We can rephrase the requirement on $f: \; S_A \to S_A$ for determining a morphism $A \xrightarrow{f} A$ by:

$$f \in End(A) \;\text{ iff }\; f \circ \tau_w = \tau_w \circ f \text{ for all } \tau_w \in M(A).$$

Hence we proved:

2.8.1 <u>THEOREM</u>: For any automaton A, End(A) is the centralizer of M(A) in $S_A^{S_A}$.

3. THE CATEGORICAL CHARACTERIZATION OF M_W.

3.1 Here we give a categorical characterization of M_W in those cases where W satisfies the following condition on its unit-elements:

3.1.1 For any $w_1, w_2 \in W$ if $w_1 w_2 = 1_W$ then we have $w_2 w_1 = 1_W$ as well.

We shall call a monoid which satisfies this condition, a unit-commutative monoid. Note that abelian monoids and right-cancellative monoids are unit-commutative. Hence, the restriction to this type of monoids does not affect the applicability of our results.

3.2 Let A be any automaton. Any subset $T \subseteq S_A$ determines a subautomaton A(T) of A which has

$$S_{A(T)} =_{df} \{t \cdot w \ : \ t \in T \ \& \ w \in W\}$$

as its set of states.

We say that A(T) is the subautomaton of A generated by T. A subset $T \subseteq S_A$ is said to be a set of generators for A iff A(T) = A. In particular, A is said to be monogenic iff A has a set of generators with a single generator. In such a case, when t is the only element of T, we write simply A(T) = A(t).

3.3 Note that M_W is always monogenic. For example, it is generated (as an automaton) by 1_W. One may easily prove that for any monoid W, $M_W = M_W(u)$ iff u is a right-unit of W.

3.4 LEMMA: A is monogenic iff for any set of generators T for A there is $t \in T$ such that $A(t) = A$.

3.4.1 REMARK: This lemma, whose proof is straight-forward and left for the reader, exhibits a significant property of automata. Intuitively speaking, in automata as we have defined them in 1.1, states do not interact.

3.5 THEOREM: An automaton A is monogenic iff there exists an epic morphism

$$M_W \xrightarrow{e} A \quad .$$

Proof: If $A = A(s_o)$ then the mapping

$$e_{s_o} \quad : \quad W \to S_A \quad : \quad w \mapsto s_o \cdot w \qquad ,$$

determines an epic morphism $M_W \xrightarrow{e_{s_o}} A(s_o)$. On the other hand, if $M_W \xrightarrow{e} A$ is epic, then $e(1_W)$ generates A.

3.6 REMARK: Note that an automaton is "strongly connected" iff it is generated by any one of its states. Put differently, A is strongly connected iff it has no proper nonempty subautomaton.

3.7 THEOREM: An automaton A is monogenic iff for any family $\{A_\alpha\}$ of sub-automata of A the following two statements are equivalent:

3.7.1 $\bigcup_\alpha A_\alpha = A$,

3.7.2 there is α for which $A_\alpha = A$.

Proof: If A is monogenic then $A = A(1c)$ for some $s_o \in S_A$. Hence $s_o \in S_\alpha$ for some α, and therefore $A_\alpha = A$. On the other hand define for all $s \in S_A$: $A_s = A(s)$ then clearly $\bigcup_s A_s = \bigcup_s A(s) = A$ and therefore there is an $s \in S_A$ for which $A_s = A$; hence A is monogenic.

3.7.3 COROLLARY: The predicate "X is a monogenic object of $\mathcal{A}_W$" is categorical.

Proof: By Theorem 3.7 and 1.8.

3.8 THEOREM: Assume that W is unit-commutative. If A is monogenic and $A \xrightarrow{e} M_W$ is epic then it is an isomorphism.

Proof: Let A be generated by s_o, then $e(S_o)$ generates M_W and therefore $e(s_o)\cdot u = 1_W$ for some $u \in W$. But W is unit-commutative and so $u\cdot e(s_o) = 1_W$ as well.

Assume that $e(s_o\cdot w_1) = e(s_o\cdot w_2)$ for some $w_1, w_2 \in W$. Then we have

$$w_1 = u\cdot e(s_o)\cdot w_1 = u\cdot e(s_o\cdot w_1) = u\cdot e(s_o\cdot w_2) = u\cdot e(s_o)\cdot w_2 = w_2$$

and therefore e is also monic.

3.9 The characterization of M_W in $\mathcal{A}_W$ is now straightforward:

3.9.1 <u>THEOREM</u>: Assume that W is unit-commutative. An object X of $\mathcal{A}_W$ is isomorphic to M_W iff the following two conditions hold:

(i) X is monogenic;

(ii) if A is monogenic then there exists an epic $X \overset{e}{\to} A$.

3.9.2 In other words we can say that an object of $\mathcal{A}_W$ is isomorphic to M_W iff it is an <u>initial object</u> in the subcategory of monogenic automata with epic morphisms only.

3.9.3 A more general characterization of M_W will be derived from a study of the projective objects in $\mathcal{A}_W$ to be presented in a forthcoming paper.

4. THE CATEGORICAL COMPLETENESS OF $\mathcal{A}_W$

4.1 Given any predicate of automata P(X) which is invariant under isomorphism of automata then we clearly have for any automaton A

$$P(A) \text{ iff } P(\mathrm{Mor}(A)) \quad .$$

By Theorem 3.9.1 we have that Mor(A) is categorical in the following sense. For any category $\mathcal{C}$ which is isomorphic to $\mathcal{A}_W$ say by J: . $\mathcal{A}_W \rightarrow \mathcal{C}$ and for any object A of $\mathcal{A}_W$, Mor(J(A)) is well defined and it is an automaton which is isomorphic to A. Hence P(A) holds iff P(Mor(J(A))) holds.

From this follows that <u>any</u> predicate P(X) of automata, is represented by P(Mor(X)) which is categorical.

Thus we have proved:

4.2 <u>THEOREM</u>: If W is a unit-commutative monoid, $\mathcal{A}_W$ is categorically complete.

4.3 In addition to the mathematical import of the completeness of $\mathcal{A}_W$ we know now that if one wishes to study automata (i.e., state diagrams) under categorical notions only, there is no theoretical objection to such a restriction. Any property of such automata has its representation in a form which is categorical. This does not imply that a categorical study of automata is necessarily the most appropriate mathematical approach to automata. It may however provide a persuasion to try to see what can be done in automata theory if one follows the problems and the notions that are studied in the traditional domains of category theory. Our next papers are directed towards this goal.

BIBLIOGRAPHY

Birkhoff, G., "Structure of Abstract Algebras," Proc. Cambridge Philos. Soc., 29, 441-464 (1935).

Büchi, J. R., "Mathematical Theory of Automata," Notes on material presented by J. B. Wright and J. R. Büchi, Communication Sciences 403, Fall 1960, The University of Michigan.

Cartan, H. & S. Eilenberg, "Homological Algebra," Princeton (1956).

Eilenberg, S. & S. MacLane, "General Theory of Natural Equivalence," Trans. AMS, 58, 231-294 (1945).

Freyd, P., "Abelian Categories: An Introduction to the Theory of Functors," Harper's Series in Modern Mathematics, New York (1964).

Give'on, Y., "Outline for an Algebraic Study of Event Automata," Tech. Rep. 05662, 06689, 03105-28-T, ORA, The University of Michigan (1964).

Hilton, P. J., "Catégories Non-Abelianes," Séminaire de Mathématiques Superiers, Université de Montreál, Dépt. de Math., Juillet 1964.

MacLane, S., "Categorical Algebra," Colloq. Lectures given at Boulder, Colorado, August 27-30, 1963, at the sixty-eighth Summer Meeting of the AMS (1963).

MacLane, S., Homology, Springer, N. Y., Berlin, Göttingen, and Heidelberg, (1963).

Northcott, D. G., "An Introduction to Homological Algebra," Cambridge (1960).

Rabin, M. O. & D. Scott, "Finite Automata and Their Decision Problems," IBM Journal, 3, 2, 114-125 (1959).

Thatcher, J. W., "Notes on Mathematical Automata Theory," Tech. Note 05602, 03105-26-T, ORA, The University of Michigan (1963).

TOWARD A HOMOLOGICAL ALGEBRA OF AUTOMATA II:

2. A Note on Some Well Known Functors of Automata

ABSTRACT

The provision of a suitable definition of homomorphisms of abstract automata (i.e., of state diagrams with an arbitrary fixed input monoid W) yields of category (denoted by $\mathcal{A}_W$). The naturalness of the application of category theory to the study of automata follows from the fact that many, if not most, of the processes employed in automata theory turn out to be functors of or into $\mathcal{A}_W$.

This observation, which is reviewed in the present paper, has led the author to experiment with a more thorough application of the category theory approach to $\mathcal{A}_W$. The results of this application are presented in the series of papers under the common title "Toward A Homological Algebra of Automata."

0. INTRODUCTION

0.1 Here we are going to present our observations which drove us to pursue the possibility of a homological theory for automata as it appears in this series of papers under the title "Toward a Homological Algebra of Automata."

Our observations can be summarized by the following. Most of the general procedures employed in automata theory are in fact functors of suitable categories of automata. Some pairs of these are shown to be naturally equivalent functors.

0.2 We cannot estimate now the importance of these observations. At least they suggest giving to category theory the opportunity to become the mathematical general framework for the theory of abstract automata.

0.3 Most of the proofs of our results here are routine. Therefore most of them will be left for the reader except for certain details that seem to have some significance. Furthermore, we do not intend to study the functors that we derive before we extend our knowledge of the category of automata itself.

In particular we postpone the study of the "algebraic" functors of automata; like the association of semigroup of machines and several notions of products of machine, each single one of them yields a wide domain of important problems and results. Hence this note will present more problems than solutions. We hope that our forthcoming research will shed some light on these problems as well.

0.4 Naturally, this note depends on the previous paper (Give'on 1964b) with its terminology and notation.

1. THE TRANSITION TRANSLATIONS OF AUTOMATA

1.1 Given any automaton A we define <u>M(A)</u>, the <u>monoid of A</u>, to be the monoid of the <u>transition translations</u>

$$\tau_w \; : \; S_A \to S_A \; : \; s \to s \cdot w$$

with respect to the opposite of function composition:

$$\tau_{w_1} * \tau_{w_2} = \tau_{w_2} \circ \tau_{w_1} \quad .$$

Note that we have

$$\tau_{w_1} \circ \tau_{w_2} = \tau_{w_2 w_1} \quad .$$

1.2 We have noted in (Give'on 1964b) that End(A), the monoid of endomorphisms of A, is the centralizer of M(A) in $S_A^{\,S_A}$, the monoid of all functions $S_A \to S_A$.

1.3 We define T(A) to be the system

$$T(A) = (M(A) \times W \xrightarrow{T(\tau_A)} M(A))$$

where $T(\tau_A)$ is given by

$$\tau_{w_1} \cdot w_2 = \tau_{w_1 w_2} \quad .$$

1.3.1 LEMMA: For any object A of $\mathcal{A}_W$, T(A) is an object of $\mathcal{A}_W$ satisfying the additional compatibility with the monoid structure M(A):

$$(\tau_{w_1} * \tau_{w_2}) \cdot w_3 = \tau_{w_1} * (\tau_{w_2} \cdot w_3) \quad .$$

Furthermore, T(A) is monogenic and generated by $1_{M(A)}$.

Proof: From the associativity of the operation of W it follows that

$$\tau_{w_1} * (\tau_{w_2} \cdot w_3), \; (\tau_{w_1} * \tau_{w_2}) \cdot w_3, \; \tau_{w_1} * \tau_{w_2 w_3}, \; \tau_{w_1} \cdot w_2 w_3$$

are all equal to $\tau_{w_1 w_2 w_3}$.

To realize that T(A) is generated by $1_{M(A)}$ note that

$$1_{M(A)} \cdot w = \tau_{1_W} \cdot w = \tau_w \quad .$$

1.4 In order to derive a functor of automata out of $A \to T(A)$ we observe the following:

1.4.1 LEMMA: If $A_1 \xrightarrow{e} A_2$ is an epic morphism of $\mathcal{A}_W$ then

$$e^* \quad : \quad M(A_1) \to M(A_2) \quad : \quad \tau^1_w \to \tau^2_w$$

is a surjective homomorphism of monoids which determines an epic morphism

$$T(A_1) \xrightarrow{e^*} T(A_2) \quad .$$

Proof: e^* is well defined precisely because of $A_1 \xrightarrow{e} A_2$ being an epic morphism of automata. For let $\tau^1_{w_1} = \tau^1_{w_2}$ for some $w_1, w_2 \epsilon W$ then we have $s \cdot w_1 = s \cdot w_2$ for all $s \epsilon S_A$. Since e is a morphism of automata we infer

$$e(s) \cdot w_1 = e(s \cdot w_1) = e(s \cdot w_2) = e(s) \cdot w_2 \quad \text{for all } s \epsilon S_A.$$

But e is surjective, hence we have $s' \cdot w_1 = s' \cdot w_2$ for all $s' \epsilon S_B$, which implies $\tau^2_{w_1} = \tau^2_{w_2}$.

The rest is routine.

1.4.2 Let us denote by $\mathcal{C}^e$ the epic-subcategory of a category $\mathcal{C}$, that is the category whose objects are all the objects of $\mathcal{C}$ and whose morphisms are the epic morphisms of $\mathcal{C}$.

Using this notation, we can define $T \;:\; \mathcal{A}^e_W \rightsquigarrow \mathcal{A}^e_W$ by adding

$$T(A_1 \xrightarrow{e} A_2) = T(A_1) \xrightarrow{e^*} T(A_2) \quad .$$

1.4.3 <u>THEOREM</u>: $T : \mathcal{A}_W^e \rightsquigarrow \mathcal{A}_W^e$ is a covariant functor of the epic-sub-category of $\mathcal{A}_W$.

<u>Proof</u>: Straightforward.

2. THE CATEGORY $\mathcal{M}_W$ OF MONOIDAL AUTOMATA

2.1 The additional properties of the automata that occur in the image of T lead us to define the following subcategory of $\mathcal{A}_W$.

The category $\mathcal{M}_W$ of monoidal automata has objects automata that have monoids for sets of states, such that the multiplication among the states is compatible with the transition function in the following manner:

$$s_1*(s_2\cdot w) = (s_1*s_2)\cdot w \quad ,$$

where "*" denotes the monoid operation among the states.

Such automata will be called monoidal automata.

A morphism $A_1 \xrightarrow{f} A_2$ of monoidal automata is defined to be a morphism of automata $A_1 \xrightarrow{f} A_2$ such that $f : S_{A_1} \to S_{A_2}$ is also a homomorphism of monoids.

2.2 An important subcategory of $\mathcal{M}_W$ is the full subcategory of the monogenic monoidal automata which are generated (as automata) by the identity element of the monoid of states. Such automata will be called unary monoidal automata and we denote their category by $\mathcal{M}_W^1$.

2.2.1 <u>LEMMA</u>: If A_1, A_2 are monoidal automata and A_2 is unary then there exists at most a single morphism $A_1 \xrightarrow{f} A_2$ of monoidal automata, and this morphism, in case it exists, is determined by a surjective homomorphism $f : S_{A_1} \to S_{A_2}$.

(<u>REMARK</u>: Note that in the category of monoids epic morphisms need not be surjective.)

<u>Proof</u>: If $A_1 \xrightarrow{f} A_2$ is a morphism of monoidal automata then $f(1_{S_{A_1}}) = 1_{S_{A_2}}$ and therefore

$$f(1_{S_{A_1}} \cdot w) = f(1_{S_{A_1}}) \cdot w = 1_{S_{A_2}} \cdot w \quad .$$

2.3 Let us denote by <u>Sur(W)</u> the category of surjective homomorphisms of W of the form

$$H = (W \xrightarrow{h} M_H) \quad .$$

A homomorphism $M_{H_1} \xrightarrow{g} M_{H_2}$ of monoids is said to determine a <u>morphism</u>

$$H_1 \xrightarrow{g} H_2$$

<u>of Sur(W)</u> iff the following diagram is commutative.

$$\begin{array}{ccc} W & \xrightarrow{h_1} & M_{H_1} \\ {\scriptstyle i_W}\updownarrow & & \downarrow{\scriptstyle g} \\ W & \xrightarrow{h_2} & M_{H_2} \end{array}$$

2.3.1 LEMMA: Sur(W) is a category in which Hom(H_1, H_2) contains at most a single morphism and this morphism is determined by a surjective homomorphism of monoids $M_{H_1} \to M_{H_2}$.

Proof: Immediate.

2.4 Define A : Sur(W) $\rightsquigarrow \mathcal{M}^1_W$ by the following.

Let H be an object of Sur(W) then A(H) is defined to be the system

$$A(H) = (M_H \times W \xrightarrow{A(h)} M_H)$$

where A(h) is given by $m \cdot w = m * h(w)$.

Let $H_1 \xrightarrow{g} H_2$ be a morphism of Sur(W) then let

$$A(H_1 \xrightarrow{g} H_2) = A(H_1) \xrightarrow{g} A(H_2) \quad .$$

2.4.1 THEOREM: A : Sur(W) $\rightsquigarrow \mathcal{M}^1_W$ is a covariant functor which establishes an isomorphism of categories between Sur(W) and $\mathcal{M}^1_W$.

Proof: Immediate.

2.5 Let $F : \mathcal{C}_1 \rightsquigarrow \mathcal{C}_2$ be a functor and $\mathcal{C}_3$ a subcategory of $\mathcal{C}_2$. We say that the image of F is essentially $\mathcal{C}_3$ iff for any object A of $\mathcal{C}_3$ there exists an isomorphic object A' in the image of F and the image of F is a subcategory of $\mathcal{C}_3$.

2.5.1 THEOREM: The image of $T : \mathcal{A}_W^e \rightsquigarrow \mathcal{A}_W^e$ is essentially $\mathcal{M}_W^1$.

2.5.2 REMARK: Obviously $\mathcal{M}_W^1$ is a subcategory of $\mathcal{A}_W^e$ and the image of T is a subcategory of $\mathcal{M}_W^1$. We shall prove the following analog of Cayley theorem that implies Theorem 2.5.1 directly.

2.5.3 LEMMA: For any object A of $\mathcal{M}_W^1$ we have an isomorphism of automata

$$A \xrightarrow{\eta(A)} T(A)$$

which is determined by

$$\eta(A) \quad : \quad S_A \to M(A) \quad : \quad 1_{S_A} \cdot w \to \tau_w \quad .$$

Proof: The function $\eta(A)$ is well defined since $1_{S_A} \cdot w_1 = 1_{S_A} \cdot w_2$ implies

$$\tau_{w_1}(s) = s \cdot w_1 = s * (1_{S_A} \cdot w_1) = s * (1_{S_A} \cdot w_2) = \tau_{w_2}(s)$$

for any $s \in S_A$. The rest is routine.

2.6 THEOREM: Let us denote by

$$T^1 : \mathcal{M}_W^1 \rightsquigarrow \mathcal{M}_W^1$$

the restriction of T to $\mathcal{M}_W^1$. Then the function η establishes a natural equivalence between T^1 and the identity functor of $\mathcal{M}_W^1$.

Proof: Let $A_1 \xrightarrow{f} A_2$ be any morphism of $\mathcal{M}_W^1$ then we have to show that the following diagram is commutative.

$$\begin{array}{ccc} A_1 & \xrightarrow{\eta(A_1)} & T(A_1) \\ f\downarrow & & \downarrow f^* \\ A_2 & \xrightarrow{\eta(A_2)} & T(A_2) \end{array}$$

In fact, let $1_{S^\cdot_{A_1}} w$ be any state of A_1 then we have

$$(f^* \circ \eta(A_1))(1_{S^\cdot_{A_1}} w) = f^*(\overset{1}{\tau_W}) = \overset{2}{\tau_W} ,$$

and

$$(\eta(A_2) \circ f)(1_{S^\cdot_{A_1}} w) = (\eta(A_2))(1_{S^\cdot_{A_2}} w) = \overset{2}{\tau_W} .$$

2.6.1 COROLLARY: The functor $T : \mathcal{A}_W^e \rightsquigarrow \mathcal{M}_W^1$ is essentially idempotent; i.e., $T \circ T$ is naturally equivalent with T.

3. FROM NONDETERMINISTIC TO DETERMINISTIC AUTOMATA

3.1 There are mainly two ways by which nondeterministic automata are transformed into (weakly equivalent) deterministic automata. Each one of them yields a functor from a category of nondeterministic automata to $\mathcal{A}_W$.

3.2 We define first $\underline{\mathcal{N}_W}$, the category of (abstract) nondeterministic automata with input monoid W, as follows.

The objects of $\mathcal{N}_W$ are systems of the form

$$N = (S_N \times W \xrightarrow{\nu_N} \mathcal{P}(S_N))$$

where $\mathcal{P}(S_N)$ is the set of all subsets of S_N, and ν_N satisfies the following compatibility requirements:

$$s \cdot w_1 w_2 = \bigcup \{ s' \cdot w_2 \ : \ s' \epsilon s \cdot w_1 \} \quad ,$$

and

$$s \cdot 1_W = \{s\} \quad .$$

The morphisms of $\mathcal{N}_W$ are defined to be of the form

$$N_1 \xrightarrow{f} N_2$$

where $f : S_{N_1} \to S_{N_2}$ is a function which yields the commutativity of the following diagram for

$$\mathcal{P}(f) \;:\; \mathcal{P}(S_{N_1}) \to \mathcal{P}(S_{N_2}) \;:\; T \to \{f(s) \;:\; s\in T\} \quad .$$

$$\begin{array}{ccc}
S_{N_1} \times W & \xrightarrow{\nu_{N_1}} & \mathcal{P}(S_{N_1}) \\
f \big\downarrow \quad \big\downarrow i_W & & \big\downarrow (f) \\
S_{N_2} \times W & \xrightarrow{\nu_{N_2}} & \mathcal{P}(S_{N_2})
\end{array}$$

3.2.1 PROPOSITION: $\mathcal{N}_W$ is a category in which epic and monic morphisms are determined by surjective and injective functions.

3.3 By means of the so called "subset construction" we associate with any object N of $\mathcal{N}_W$ a system

$$\mathcal{P}(N) = (\mathcal{P}(S_N) \times W \xrightarrow{\mathcal{P}(\nu_N)} \mathcal{P}(S_N))$$

where $\mathcal{P}(\nu_N)$ is given by (for any $T \subseteq S_N$)

$$T\cdot w = \bigcup\{s\cdot w \;:\; s\in T\} \quad .$$

3.3.1 LEMMA: For any object N of $\mathcal{N}_W$, $\mathcal{P}(N)$ is an object of $\mathcal{A}_W$.

As for the morphisms of $\mathcal{N}_W$ we naturally define

$$\mathcal{P}(N_1 \xrightarrow{f} N_2) = (\mathcal{P}(N_1) \xrightarrow{\mathcal{P}(f)} \mathcal{P}(N_2)) \quad .$$

3.3.2 LEMMA: If $N_1 \xrightarrow{f} N_2$ is a morphism of $\mathcal{N}_W$ then $\mathcal{P}(N_1 \xrightarrow{f} N_2)$ is a morphism of $\mathcal{A}_W$.

3.3.3 THEOREM: $\mathcal{P} : \mathcal{N}_W \rightsquigarrow \mathcal{A}_W$ is a covariant functor.

3.4 In addition to the subset construction one can derive a deterministic automaton weakly equivalent to a given nondeterministic automaton by means of a construction which is similar to $T : \mathcal{A}_W^e \rightsquigarrow \mathcal{M}_W^1$. That is, by means of the monoid of the transition relations.

3.4.1 Note that we hope that our notation for $\mathcal{N}_W$ confuses well the two isomorphic categories; that of nondeterministic automata and that of relational systems (cf. Thatcher 1964).

3.5 Given an object N of $\mathcal{N}_W$, we define M(N), the monoid of N, to be the monoid of the transition relations

$$\beta_W = \bigcup \{(s \cdot 1_W) \times (s \cdot w) \quad : \quad s \in S_N\} \quad ;$$

i.e.,

$$\langle s, s'\rangle \in \beta_W \text{ iff } s' \in s \cdot w$$

For any object N of $\mathcal{N}_W$ we define the system

$$B(N) = (M(N) \times W \xrightarrow{B(\nu_N)} M(N))$$

where $B(\nu_N)$ is given by

$$\beta_{w_1} \cdot w_2 = \beta_{w_1 w_2} = \beta_{w_1} \circ \beta_{w_2} \quad .$$

3.5.1 <u>LEMMA</u>: For any object N of $\mathcal{N}_W$, B(N) is a unary monoidal automaton; that is, an object of $\mathcal{M}^1_W$.

<u>Proof</u>: Similar to the proof of Lemma 1.3.1.

3.6 Following Lemma 1.4.1 we derive:

3.6.1 <u>LEMMA</u>: If $N_1 \xrightarrow{e} N_2$ is an epic morphism of $\mathcal{N}_W$ then

$$e* \ : \ M(N_1) \to M(N_2) \ : \ \beta^1_W \to \beta^2_W$$

is a surjective homomorphism of monoids which determines a morphism of monoidal automata

$$B(N_1) \xrightarrow{e*} B(M_2) \quad .$$

3.7 We define therefore

$$B \ : \ \mathcal{N}^e_W \rightsquigarrow \mathcal{M}^1_W$$

by adding

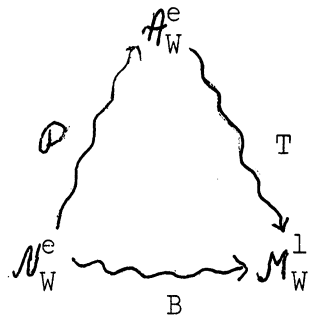
$$B(N_1 \xrightarrow{e} N_2) = B(N_1) \xrightarrow{e^*} B(N_2)$$

and we derive the following result:

3.7.1 <u>THEOREM</u>: $B : \mathcal{N}^e_W \rightsquigarrow \mathcal{M}^1_W$ is a covariant functor with image being essentially $\mathcal{M}^1_W$.

4. THE EQUIVALENCE OF B AND $T \circ \mathcal{P}$

4.1 From our previous results, we can derive monoidal unary automata from nondeterministic automata following the two paths in the next diagram of functors, where



$\mathcal{P} : \mathcal{N}^e_W \rightsquigarrow \mathcal{A}^e_W$ is the restriction of $\mathcal{P} : \mathcal{N}_W \rightsquigarrow \mathcal{M}_W$ to $\mathcal{N}^e_W$.

Obviously $T \circ \mathcal{P}$ and B are not identical functors but they are similar enough to be naturally equivalent. Still, this natural equivalence is trivial because of the following general theorem.

4.2 <u>THEOREM</u>: Let $F_1, F_2 : \mathcal{C} \rightsquigarrow \mathcal{C}_0$ be two functors from $\mathcal{C}$ into $\mathcal{C}_0$. If $\mathcal{C}_0$ is a category in which for any two objects A,B, Hom(A,B) contains at most a single morphism then a necessary and sufficient condition for the existence of a natural equivalence $\eta : F_1 \to F_2$ is that for any object A of

$\mathcal{C}$, $F_1(A)$ and $F_2(A)$ are isomorphic.

Proof: Necessity is immediate. For the proof of sufficiency, assume that $A \xrightarrow{f} B$ is a morphism of $\mathcal{C}$ and denote by $F_1(A) \xrightarrow{\eta(A)} F_2(A)$ the isomorphism of $\mathcal{C}_o$ that is assumed to exist for any object A of $\mathcal{C}$. Obviously, the following diagram is commutative because of the trivial structure of $\mathcal{C}_o$.

$$\begin{array}{ccc} F_1(A) & \xrightarrow{\eta(A)} & F_2(A) \\ {\scriptstyle F_1(f)}\downarrow & & \downarrow{\scriptstyle F_2(f)} \\ F_1(B) & \xrightarrow{\eta(B)} & F_2(B) \end{array}$$

4.3 LEMMA: For any object N of $\mathcal{N}_W$ the function

$$\zeta(N) \; : \; M(N) \to M(\mathcal{P}(N)) \; : \; \beta_w \to (\mathcal{P}(\nu_N))_w \; ,$$

where

$$(\mathcal{P}(\nu_N))_w : \mathcal{P}(S_N) \to \mathcal{P}(S_N) \; : \; T \to T\cdot w \; ,$$

determines an isomorphism

$$B(N) \xrightarrow{\zeta(N)} [T\circ\mathcal{P}](N)$$

of $\mathcal{M}_W^1$.

Proof: Straightforward.

4.3.1 COROLLARY: $\zeta : B \to T \circ \mathcal{P}$ is a natural equivalence from $B : \mathcal{N}_W^e \rightsquigarrow \mathcal{M}_W^1$ to $T \circ \mathcal{P} : \mathcal{N}_W^e \rightsquigarrow \mathcal{M}_W^1$.

5. A REMARK ON THE RELATION BETWEEN THE SUBSET CONSTRUCTION AND THE CARTESIAN POWER OF AUTOMATON

5.1 The subset-construction as applied to automata yields a covariant functor

$$\mathcal{P} : \mathcal{A}_W \rightsquigarrow \mathcal{A}_W$$

as defined by

$$\text{(i)} \quad \mathcal{P}(A) = (\mathcal{P}(S_A) \times W \xrightarrow{\mathcal{P}(\tau_A)} \mathcal{P}(S_A)),$$

where $\mathcal{P}(\tau_A)$ is given by $T \cdot w = \{s \cdot w : s \in T\}$;

$$\text{(ii)} \quad \mathcal{P}(A_1 \xrightarrow{f} A_2) = \mathcal{P}(A_1) \xrightarrow{\mathcal{P}(f)} \mathcal{P}(A_2),$$

where $\mathcal{P}(f)$ is defined by $(\mathcal{P}(f))(T) = \{f(s) : s \in T\}$.

We shall see presently that $\mathcal{P}$ is a functor which is naturally related to the functor of cartesian products of automata.

5.2 In particular, we define for any set T:

$$P^T : \mathcal{A}_W \rightsquigarrow \mathcal{A}_W$$

by

(i) $P^T(A) = (S_A{}^T \times W \xrightarrow{P^T(\tau_A)} S_A{}^T)$,

where $S_A{}^T$ is the set of all functions $T \to S_A$, and $P^T(\tau_A) = \tau_A^T$ is given by

$$\phi \cdot w \ : \ T \to S_A \ : \ t \to \phi(t) \cdot w \ .$$

Naturally, we denote $P^T(A) = A^T$.

(ii) $P^T(A_1 \xrightarrow{f} A_2) = A_1{}^T \xrightarrow{f^T} A_2{}^T$,

where f^T is defined by

$$\begin{cases} f^T \ : \ S_{A_1}^T \to S_{A_2}^T \ : \ \phi \to f^T(\phi) \ , \\ f^T(\phi) \ : \ T \to S_{A_2} \ : \ t \to f(\phi(t)) \ . \end{cases}$$

5.3 <u>LEMMA</u>: Both $\mathcal{P}$ and P^T are covariant endofunctors of $\mathcal{A}_W$. For any fixed automaton A, $P^T(A)$ as a function of T induces in fact a contravariant functor

$$P^X(A) \ : \ \mathcal{S} \rightsquigarrow \mathcal{A}_W$$

of $\mathcal{S}$ the category of sets into $\mathcal{A}_W$. Furthermore, $P(T,A) = P^T(A)$ induces a bi-functor

$$P \ : \ \mathcal{S} \times \mathcal{A}_W \rightsquigarrow \mathcal{A}_W \ .$$

<u>Proof</u>: Naturally, we add to the definitions of $P^X(A) = A^X$ and $P(T, A) = A^T$ the following:

$$P^{(T_1 \xrightarrow{\psi} T_2)}(A) = A^{T_2} \xrightarrow{\psi^*} A^{T_1},$$

where

$$\psi^* \; : \; S_A^{T_2} \to S_A^{T_1} \; : \; \phi \to \phi \circ \psi;$$

and likewise

$$P((T_1 \xrightarrow{\psi} T_2), A) = A^{T_2} \xrightarrow{\psi^*} A^{T_1} .$$

The verification of the lemma is routine.

5.4 The main difference between A^T and $\mathcal{P}(A)$ lies in the fact that in A^T the states are ordered sets over S_A, while in $\mathcal{P}(A)$ they are just subsets of S_A. This calls of course for a "forgetful transformation" from automata of the form of A^T to automata of the form of $\mathcal{P}(A)$.

Let T be a fixed set. We define a transformation σ_T from the class of objects of $\mathcal{A}_W$ to the class of morphisms of $\mathcal{A}_W$ by

$$\sigma_T(A) \; : \; S_A^T \to \mathcal{P}(S_A) \; : \; \phi \to \{\phi(t) \; : \; t \in T\} .$$

5.4.1 <u>LEMMA</u>: The function $\sigma_T(A)$ determines a morphism

$$A^T \xrightarrow{\sigma_T(A)} \mathcal{P}(A)$$

of $\mathcal{A}_W$. Note that $\sigma_T(A)$ covers all the nonempty subsets of S_A iff S_A^T contains a surjective function $T \to S_A$.

Proof: Immediate.

5.4.2 THEOREM: For any set T

$$\sigma_T \ : \ P^T \to \mathcal{P}$$

as determined by

$$\sigma_T(A) = A^T \xrightarrow{\sigma_T(A)} \mathcal{P}(A)$$

is a natural transformation from $P^T : \mathcal{A}_W \rightsquigarrow \mathcal{A}_W$ to $\mathcal{P} : \mathcal{A}_W \rightsquigarrow \mathcal{A}_W$.

Proof: Let $A_1 \xrightarrow{f} A_2$ be any morphism of $\mathcal{A}_W$, then we have to show that the following diagram is commutative.

$$\begin{array}{ccc} A_1^T & \xrightarrow{f^T} & A_2^T \\ \sigma_T(A_1) \downarrow & & \downarrow \sigma_T(A_2) \\ \mathcal{P}(A_1) & \xrightarrow{\mathcal{P}(f)} & \mathcal{P}(A_2) \end{array}$$

Let ϕ be any state of A_1^T then we have:

$$\begin{aligned} [\mathcal{P}(f)][\sigma_T(A_1)](\phi) &= [\mathcal{P}(f)](\{\phi(t) \ : \ t\in T\}) \\ &= \{f(\phi(t)) \ : \ t\in T\} \\ &= [\sigma_T(A_2)](f^T(\phi)) \quad . \end{aligned}$$

6. EVENT FUNCTORS OF AUTOMATA

6.1 All the constructions discussed previously were introduced in order to derive transformation of automata which preserve the so called "behavior".

In this section we discuss briefly the definition of events by means of automata. A more complete study of the functors that are involved in this is necessary to the understanding of the theory of finite-state event-automata (Give'on 1964a).

6.2 Every automaton determines a function which associates with any choice of "initial" and "final" states a certain subset of the input-monoid. We define therefore for any object A of $\mathcal{A}_W$

$$E(A) \quad : \quad S_A \times \mathcal{P}(S_A) \to \mathcal{P}(W) \quad : \quad (s, T) \to \{w \ : \ s \cdot w \in T\} ,$$

and for any object N of $\mathcal{N}_W$

$$E(N) \quad : \quad \mathcal{P}(S_A) \times \mathcal{P}(S_A) \to \mathcal{P}(W) \quad : \quad (T_1, T_2) \to \{w : (T_1 \cdot w) \cap T_2 \neq \emptyset\} .$$

6.2.1 Thus, a Rabin-Scott finite-automaton (Rabin, Scott 1959) is defined as $\mathfrak{U} = \langle V, A, (s_0, F)\rangle$ where V is a finite set (the alphabet of $\mathfrak{U}$), A is an automaton with V* as input monoid such that S_A is finite, and $(s_0, F) \in S_A \times \mathcal{P}(S_A)$.

The event $T(\mathcal{U})$ defined by $\mathcal{U}$ is $[E(A)](s_o, F)$.

6.3.1 PROPOSITION: If $A_1 \xrightarrow{f} A_2$ is a morphism of $\mathcal{A}_W$ then for every $s \in S_A$ and $T \subseteq S_A$ we have

$$[E(A_1)](s,T) \subseteq [E(A_2)](f(s), f(T)) \quad .$$

6.3.2 PROPOSITION: If $N_1 \xrightarrow{f} N_2$ is a morphism of $\mathcal{N}_W$ then for every T_1, $T_2 \subseteq S_{N_1}$ we have

$$[E(N_1)](T_1, T_2) \subseteq [E(N_2)](f(T_1), f(T_2))$$

REMARK: For the sake of clarity, but with the price of rigor, we denote by f both the function as it is, and the induced function $\mathcal{P}(f)$ on the set of subsets of the domain of f.

6.4 THEOREM (Rabin-Scott): Let N be any object of $\mathcal{N}_W$. Denote by $[F]_N$, for $F \subseteq S_N$, the set of all subsets of S_M which overlap with F; i.e.,

$$[F]_N = T \subseteq S_N \ : \{T \cap F \neq 0\} \quad .$$

Then for any $S_o, F \subseteq S_N$ we have

$$[E(N)](S_o, F) = [E(\mathcal{P}(N))](S_o, [F]_N) \quad .$$

Proof: Follow the proof of (Rabin Scott 1959).

6.5 The definition of events by unary monoidal automata follows their special structure, naturally.

For any unary monoidal automaton A, we define

$$E^1(A) \quad : \mathcal{P}(S_A) \to \mathcal{P}(W) \quad : \quad T \to \{w : 1_{S_A} \cdot w \in T\}$$

6.5.1 <u>PROPOSITION</u>: If $A_1 \xrightarrow{e} A_2$ is a morphism of unary monoidal automata then for any $T \subseteq S_A$ we have

$$[E^1(A_1)](T) \subseteq [E^1(A_2)](f(T)) \quad ,$$

and

$$[E^1(A_1)](f^{-1}f(T)) = [E^1(A_2)](f(T)) \quad .$$

6.5.2 <u>THEOREM</u>: Let A be an automaton (i.e., object of $\mathcal{A}_W$) and let $s_o \in S_A$, $F \subseteq S_A$. Denote by $\tau_A[s_o, F]$:

$$\tau_A[s_o, F] = \{\tau_W : s_o w \in F\} \subseteq M(A) \quad .$$

Then we have

$$[E(A)](s_o, F) = [E(T(A))](\tau_A(s_o, F)) \quad .$$

6.6 These results yield in fact a natural category of event-definitions such that E, E, and E^1 turn out to be covariant functors of $\mathcal{A}_W$, $\mathcal{N}_W$, and $\mathcal{M}^1_W$ (resp.) into the category of event-definitions.

We leave the study of this category to a later stage of the development of the categorical theory of automata.

BIBLIOGRAPHY

Give'on, Y., (a) "Outline for an Algebraic Study of Event Automata," Tech. Rep. 05662, 06689, 03105-28-T, ORA, The University of Michigan (1964).

Give'on, Y., (b) "Toward a Homological Algebra of Automata I: 1. The Representation and Completeness Theorems for Categories of Abstract Automata," Tech. Rep. 06689, 03105-32-T, ORA, The University of Michigan (1964).

Rabin, M. O. and D. Scott, "Finite Automata and Their Decision Problems," _IBM Journal_, _3_, 2, 114-125 (1959).

Thatcher, J. W., "Notes on Mathematical Automata Theory," Tech. Note 05602, 03105-26-T, ORA, The University of Michigan (1963).

TOWARD A HOMOLOGICAL ALGEBRA OF AUTOMATA III:

3. Composition Series of Automata

4. Extensions of Q-Automata

ABSTRACT

3. COMPOSITION SERIES OF AUTOMATA

The classical results of commutative algebra on composition series (i.e., the theorems of Jordan, Holder, Zassenhaus, and Schreier) are derived for automata. The relevance of these results to the study of automata is discussed briefly by means of an alternative proof of these results.

4. EXTENSIONS OF Q-AUTOMATA

Previous results of the author concerning composition series for automata lead to the introduction of a specific type of quotient operation of an automaton relative to any subautomaton. Naturally, the problem of extensions, relative to this type of quotient, is posed. A complete characterization and a method of construction of all possible extensions of automata are derived for a broad class of automata.

TABLE OF CONTENTS

3. COMPOSITION SERIES OF AUTOMATA

1. BASIC NOTIONS

1.1 In this paper we regard automata as input monoids operating on sets. To be specific, we assume a fixed input monoid W and thus an automaton A is defined by its set of <u>states</u>, S_A and the manner by which W operates on it, that is by the multiplication rule

$$\tau_A \; : \; S_A \times W \to S_A \; : \; (s, w) \to s \cdot w$$

which assigns $s \cdot w$ to any pair $(s, w) \in S_A \times W$.

We assume the following requirements on τ_A, the <u>transition-function</u> of A:

(i) $s \cdot 1_W = s$ where 1_W is the identity element of W;

(ii) $s \cdot (w_1 w_2) = (s \cdot w_1) \cdot w_2$.

1.2 We do not assume anything on the size of the sets of states of our automata. Thus, for example, we have the following two particular automata:

1.2.1 O_W which has a single state only. (This specification defines O_W up to an isomorphism.)

On the other hand we have:

1.2.2 M_W which has W as its set of states and so M_W is in fact W regarded as operating on itself from the right:

$$w_1 \cdot w_2 = w_1 w_2 .$$

1.2.3 We shall find it useful to include the "empty automaton" $\emptyset_W$ in our discussion.

1.3 A subset S_B of S_A is regarded as a subautomaton B of A, in symobls, $B \subseteq A$, iff it is closed (or stable) under the multiplication by W. That is, iff $s \in S_B$ implies $s \cdot w \in S_B$ (for any $s \in S_A$ and $w \in W$, naturally).

Thus, $\emptyset_W$ is a subautomaton of any automaton. This is not true of 0_W.

An automaton is said to be simple if it has 0_W as its only proper non-empty subautomaton.

An automaton A is called irreducible iff $\emptyset_W$ is its only proper sub-automaton. For example, 0_W is irreducible.

1.3.1 Clearly the class of all subautomata of a given automaton is closed under intersections and unions. Hence this class forms a lattice.

1.3.2 PROPOSITION: The class of all subautomata of a given automaton is a complete modular lattice. In particular, let A, B and C be subautomata of a given automaton such that $B \subseteq A$, then

$$A \cap (C \cup B) = (A \cap C) \cup B .$$

Proof: Follow the corresponding proof for sets:

$$S_A \cap (S_C \cup S_B) = (S_A \cap S_C) \cup S_B .$$

1.3.3 We can define internal direct sum of two subautomata as their union iff they are disjoint. Thus, if A_1 and A_2 are subautomata of A then $A = (A_1 \oplus A_2)$ iff $A = (A_1 \cup A_2)$ and $(A_1 \cap A_2) = \emptyset_W$.

1.4 Homomorphisms of automata can be defined naturally. Thus, a function $f : S_A \to S_B$ is said to determine the morphism $A \xrightarrow{f} B$ iff

$$f(s \cdot w) = f(s) \cdot w .$$

Obviously we make use of all the traditional abuses of notations which are found to be quite useful and clarifying. E.g., we denote both the operation of A and that of B by the same symbol; we omit universal quantifiers that should occur at the beginning of our statements; etc.

Homomorphisms of automata cannot yield directly any fruitful notion of kernels. The reason for this lies in the fact that the only communication that takes place among states is done by means of transitions from single states. However, we can define a moderately interesting notion of quotient-automata as determined by subautomata and which are related to epimorphisms (surjective morphisms or epic morphisms) of automata in a natural manner. The reader is referred to the literature for a more detailed study of various categories associated with automata (Thatcher 1964, Give'on 1964).

1.5 Let B be a subautomaton of A. We define A/B by the following:

$$S_{A/B} =_{df} (S_A - S_B) \cup \{s^*_B\} \text{ , where } s^*_B \text{ is not an element of } S_A;$$

$$s \cdot w = \begin{cases} s \cdot w \text{ in A if } s \cdot w \in S_{A/B}, \\ s^*_B \quad \text{otherwise} \quad . \end{cases}$$

Thus A/B is derived from A by replacing O_W instead of B. For example we have the following peculiar unique situation: $A/\emptyset_W = A \oplus O_W$. To be more general we have

$$(A \oplus B)/B = (A \oplus O_W) \quad ,$$

for any automata A, B. (Note that $(A \oplus \emptyset_W) = A$). On the other hand we have $A/B = A$ iff $B = O_W \subseteq A$.

1.6 LEMMA: A/B is completely determined by $S_A - S_B$. Furthermore, if $S_A \neq \emptyset$ then the identity function of $S_A - S_B$ can be extended uniquely into a function $q_B : S_A \to S_{A/B}$ which determines an epimorphism

$$A \xrightarrow{q_B} A/B$$

(the canonical epimorphism of A onto A/B).

Proof: Immediate.

1.6.1 REMARK: Note that not every epimorphism of automata is equivalent to a canonical epimorphism onto a quotient automaton.

1.6.2 REMARK: Our notion of quotient automata is in fact a generalization of Rees's concept of quotients for semigroups. And so our development generalizes Rees's theory of composition series for semigroups (Rees 1940).

1.6.2 COROLLARY: The mapping $q_B : S_A \to S_{A/B}$ extended by the subset functor to $P(q_B) : P(S_A) \to P(S_{A/B})$, (that is $P(q_B)(S) = \{q_B(s) : s \in S\}$ for all $S \subseteq S_A$), determines a bijective correspondence between the subsets of S_A which include B and between the nonempty subsets of $S_{A/B}$. In particular, q_B determines a bijective correspondence between the subautomata of A which include B and the nonempty subautomata of A/B.

1.6.3 COROLLARY: An automaton B is a maximal proper subautomaton of A iff A/B is simple.

1.7 LEMMA: If A_1 and A_2 are subautomata of A then we have

$$(A_1 \cup A_2)/A_2 \cong A_1/(A_1 \cap A_2) \quad .$$

In fact the isomorphism is a single point extension of the identity mapping of $S_{A_1} - S_{A_2}$.

Proof: By Lemma 1.6 it is sufficient to show that

$$S_{(A_1 \cup A_2)} - S_{A_2} = S_{A_1} - S_{(A_1 \cap A_1)}$$

Indeed,

$$S_{(A_1 \cup A_2)} - S_{A_2} = (S_{A_1} \cup S_{A_2}) - S_{A_2}$$

$$= S_{A_1} - S_{A_2} = S_{A_1} - (S_{A_1} \cap S_{A_2})$$

$$= S_{A_1} - S_{(A_1 \cap A_2)} \quad .$$

1.7.1 REMARK: Note that if $(A_1 \cap A_2) = \phi_W$ we have $(A_1 \cup A_2) = (A_1 \oplus A_2)$ and we have noticed already (cf. 1.5) that $(A_1 \oplus A_2)/A_2 = (A_1 \oplus O_W)$ and $A_1/\phi_W = (A_1 \oplus O_W)$.

1.8 LEMMA: Let A, B and C be automata. If $A \supseteq B \supseteq C$ then $A/C \supseteq B/C$ and

$$(A/C)/(B/C) \cong A/B$$

where the isomorphism is a one point extension of the identity mapping of $S_A - S_B$.

Proof: $S_{A/C} = (S_A - S_C) \cup \{s_C^*\}$, $S_{B/C} = (S_B - S_C) \cup \{s_C^*\}$,

hence, $S_{B/C} \subseteq S_{A/C}$ and so $B/C \subseteq A/C$; and furthermore,

$$S_{A/C} - S_{B/C} = S_A - S_B \quad .$$

2. COMPOSITION SERIES

2.1 A normal series of an automaton A is a finite sequence of subautomata

$$\alpha \ : \qquad A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_{n-1} \supseteq A_n = \phi_W \quad .$$

The length of α is defined to be $\ell(\alpha) = n$.

The factor series of the normal series

$$\alpha : A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_{n-1} \supseteq A_n = \phi_W$$

is defined to be the sequence

$$Q(\alpha) = \langle A_0/A_1, A_1/A_2, A_2/A_3, \dots, A_{n-1}/A_n \rangle .$$

Two normal series α and β are said to be equivalent iff $\ell(\alpha) = \ell(\beta)$ and $Q(\alpha)$ is a permutation of $Q(\beta)$.

2.2 Let us denote by N(A) the set of all normal series of A. Since for any automaton A, $A \supseteq \phi_W$ is a normal series, N(A) is never empty.

We define a partial order $\prec$ in N(A) by:

$\alpha \prec \beta$ iff every subautomaton of A which occurs in α occurs also in β.

A normal series which is a maximal element in N(A) with respect to $\prec$, and all its subautomata are different, is called a composition series of A.

2.2.1 Note that every finite automaton has a composition series. While M_W, for a free monoid W for instance, has no composition series.

Our aim is to prove the analogous to Jordan's, Hölder's and Schreier's theorems for automata. For the proofs of these theorems we apply the proofs of the analogous theorems for modules (for Theorem 2.3 and Theorem 2.4, see for example Zariski and Samuel 1958) and of Schreier theorem for groups with operators and for sets (Papy 1961).

2.3 THEOREM (JORDAN): If an automaton A has a composition series of length n then every composition series of A has length n. Furthermore, every normal series of A without repetitions can be refined to a composition series.

Proof: By induction on n. If n = 1 then A is irreducible (i.e., it has no proper nonempty subautomaton) and therefore $A \supsetneq \emptyset_W$ is its only normal series. (The case for n = 0 is utterly trivial.)

Assume that the theorem is true for automata having composition series of length less than n where $n > 1$.

Since A has a composition series, say

$$\alpha \ : \ A \ = \ A_0 \supsetneq A_1 \supsetneq \ldots \supsetneq A_{n-1} \supsetneq A_n \ = \ \emptyset_W$$

of length n, A cannot have any composition series of length less than n.

We shall show that for any normal series of A without repetitions, say

$$\beta \ : \ A \ = \ B_0 \supsetneq B_1 \supsetneq \ldots \supsetneq B_{m-1} \supsetneq B_m \ = \ \emptyset_W$$

we have $\ell(\beta) \ = \ m \leq n \ = \ \ell(\alpha)$.

Case 1: $B_1 = A_1$

By α, B_1 has a composition series of length n-1, and by β, a normal series without repetitions of length m-1. Hence by the induction hypothesis $m-1 \leq n-1$, that is $m \leq n$.

Case 2: $B_1 \subset A_1$

By α, A_1 has a composition series of length n-1, and by β, a normal series without repetitions of length m; hence $m \leq n-1$ and so $m < n$.

Case 3: B_1 is not included in A_1

Since there are no subautomata between A and A_1 we have $A = A_1 \cup B_1$. By Lemma 1.7 we get

$$A/A_1 \ = \ (A_1 \cup B_1)/A_1 \ \cong \ B_1/(A_1 \cap B_1) \ .$$

Since A/A_1 is simple, so is $B_1/(A_1 \cap B_1)$ and therefore there are no subautomata between B_1 and $(A_1 \cap B_1)$.

Since A_1 has a composition series of length n-1 and $(A_1 \cap B_1) \subset A_1$, every normal series without repetition of $(A_1 \cap B_1)$ has length at most n-2, and hence $(A_1 \cap B_1)$ has a composition series of length at most n-2. Since there are no subautomata between B_1 and $(A_1 \cap B_1)$, B_1 has a composition series of length at most n-1. By induction hypothesis we have $m-1 \leq n-1$ and thus again $m \leq n$.

2.3.1 <u>COROLLARY:</u> If an automaton A has a composition series then every subautomaton of A has composition series.

<u>Proof:</u> Let $B \subseteq A$. Since A has a composition series, if $A \supseteq B \supseteq \phi_W$ is without repetitions it has a refinement which is a composition series and so does B. If $A \supseteq B \supseteq \phi_W$ has repetitions then either B = A or $B = \phi_W$.

2.3.2 <u>COROLLARY:</u> If an automaton A has a composition series then every subautomaton B of A occurs in a composition series of A.

2.4 <u>THEOREM (HÖLDER):</u> If an automaton A has a composition series then any two composition series of A are equivalent.

<u>Proof:</u> Let α and β (by Theorem 2.3 we know that $\ell(\alpha) = \ell(\beta)$) be any two composition series of A; say

$$\alpha \; : \; A = A_0 \supset A_1 \supset \ldots \supset A_{n-1} \supset A_n = \phi_W ,$$

$$\beta \; : \; A = B_0 \supset B_1 \supset \ldots \supset B_{n-1} \supset B_n = \phi_W .$$

For n = 0, 1 the theorem holds trivially. Assume therefore that it holds for all automata having composition series of length less than n where $n > 1$.

If $A_1 = B_1$, then we have two equivalent composition series for $A_1 = B_1$ and since $A/A_1 = A/B_1$, we have that α and β are equivalent.

If not, then $A = (A_1 \cup B_1)$. Since $(A_1 \cap B_1) \subset A$, $A_1 \cap B_1$ has a composition series, say γ. From γ we obtain two composition series

$$\delta_1 \; : \; A \;=\; (A_1 \cup B_1) \supset A_1 \supset (A_1 \cap B_1) \supset \ldots \gamma \ldots \quad ;$$

$$\delta_2 \; : \; A \;=\; (A_1 \cup B_1) \supset B_1 \supset (A_1 \cap B_1) \supset \ldots \gamma \ldots \quad .$$

Lemma 1.7 implies that δ_1 and δ_2 are in fact composition series. It also implies that they are equivalent.

Now δ_1 and α are equivalent because of the occurrence of A_1, and δ_2 and β are equivalent because of B_1. Hence α and β are equivalent.

2.4.1 <u>COROLLARY</u>: Let B be a subautomaton of A and let A have a composition series. Denote by Q(C) the set of the quotients appearing with their repetitions in $Q(\gamma)$ for any composition series γ of C. Then

$$Q(A) \;=\; Q(B) \cup Q(A/B).$$

2.5 Thus, we can define for any automaton A, its <u>length $\ell(A)$</u> to be ∞ if A does not have any composition series; otherwise $\ell(A)$ is defined to be the length of any composition series of A. In particular $\ell(\emptyset_W) = 0$ and $\ell(0_W) = 1$.

2.6 <u>THEOREM</u>: If B is a subautomaton of A then

$$1 + \ell(A) \;=\; \ell(B) + \ell(A/B) \quad .$$

<u>Proof</u>: Let

$$\beta \; : \; B \;=\; B_0 \supset B_1 \supset \ldots \supset B_{m-1} \supset B_m \;=\; \emptyset_W$$

be any normal series of B without repetitions. By Corollary 1.6.2, A/B has a normal series without repetitions of the form

$$\gamma \ : \ A/B \ = \ C_0/B \supset C_1/B \supset \ldots \supset C_{n-1}/B \ = \ O_W \supset \phi_W$$

where $A = C_0 \supset C_1 \supset \ldots \supset C_{n-1} = B \supset \phi_W$ is a normal series without repetitions. Hence we get a normal series of A without repetitions

$$\alpha \ : \ A \subset C_0 \supset C_1 \supset \ldots \supset C_{n-2} \supset C_{n-1} \supset B_1 \supset \ldots \supset B_{m-1} \supset B_m \ = \ \phi_W$$

having length $m + n - 1$.

If either $\ell(B)$ or $\ell(A/B)$ is infinite then either m or n (resp.) can be made arbitrarily large and so $\ell(A) = \infty$.

On the other hand, if both $\ell(B)$ and $\ell(A/B)$ are finite, we can assume that β and γ are composition series for B and A/B (resp.). The assumption on γ that it ends with B/B is possible because of Corollary 2.3.2. Hence, by Lemma 1.8, α is a composition series for A of length equal to $\ell(B) + \ell(A/B) - 1 = \ell(\beta) + \ell(\gamma) - 1$.

2.6.1 COROLLARY: If A_1 and A_2 are subautomata of A then

$$\ell(A_1) + \ell(A_2) \ = \ \ell(A_1 \cup A_2) + \ell(A_1 \cap A_2) \quad .$$

Proof: Immediate by Lemma 1.7.

2.6.2 COROLLARY: $\ell(A_1 \oplus A_2) \ = \ \ell(A_1) + \ell(A_2)$.

2.7 We turn now to prove directly the analogous theorem to Schreier's. Following the scheme of proof of Papy (Papy 1961) we prove first the "four automata lemma"; i.e., the counterpart of Zassenhaus theorem. In fact, this way of proof shows that the composition theorems for automata are much closer to these of sets than to these of groups or modules.

2.8 <u>LEMMA (The four automata lemma)</u>: Let A, B, C and D be automata such that $B \subseteq A$ and $D \subseteq C$. Then

$$(A \cap D \cup B) \subseteq (A \cap C \cup B) \ , \ (C \cap B \cup D) \subseteq (C \cap A \cup D) \ ,$$

and

$$(A \cap C \cup B)/(A \cap D \cup B) \cong (C \cap A \cup D)/(C \cap B \cup D)$$

<u>REMARK</u>: Our assumptions permit us to apply the modular law (1.3.2) and to save brackets.

<u>Proof</u>:

$$S_{(A \cap D \cup B)} = S_A \cap S_D \cup S_B \quad ,$$

$$S_{(A \cap C \cup B)} = S_A \cap S_C \cup S_B \quad ;$$

but $S_D \subseteq S_C$, hence $(S_D \cup S_B) \subseteq (S_C \cup S_B)$ and $S_A \cap (S_D \cup S_B) \subseteq S_A \cap (S_C \cup S_B)$. Similarly we have $(C \cap B \cup D) \subseteq (C \cap A \cup D)$.

Now,

$$S_{\left((A \cap C \cup B)/(A \cap D \cup B)\right)} = (S_{(A \cap C \cup B)} - S_{(A \cap D \cup B)}) \cup \{s_1^*\},$$

$$S_{\left((C \cap A \cup D)/(C \cap B \cup D)\right)} = (S_{(C \cap A \cup D)} - S_{(C \cap B \cup D)}) \cup \{s_2^*\}.$$

But

$$S_{(A \cap C \cup B)} - S_{(A \cap D \cup B)} = (S_A \cap S_C \cup S_B) - (S_A \cap S_D \cup S_B)$$

and

$$S_{(C \cap A \cup D)} - S_{(C \cap B \cup D)} = (S_C \cap S_A \cup S_D) - (S_C \cap S_B \cup S_D)$$

Hence, by the appropriate theorem on sets (cf. Papy 1961) we get

$$S_{(A \cap C \cup B)} - S_{(A \cap D \cup B)} = S_{(C \cap A \cup D)} - S_{(C \cap B \cup B)}.$$

Thus by Lemma 1.6 we have established the isomorphism which is again a single point extension of an identity function.

2.9 As in other domains where Schreier's theorem holds, it is derived directly from the appropriate version of Zassenhaus' theorem. (See for example, Papy 1961). This is done by means of the mutual refinement of normal series and we leave the details of the proof to the reader.

2.9.1 THEOREM (SCHREIER): Any two normal series of an automaton A have equivalent refinements.

3. DISCUSSION

3.1 Parallel to commutative algebra, we find that an automaton has a composition series iff it satisfies both maximum and minimum conditions on its chains of subautomata. Hence, in particular, finite automata always have compositions series.

3.2 The basis for the proof of the composition series theorems seems to rely quite heavily on the set theoretic properties of the set of states of the subautomata. Thus, the impression that one gets naturally is that our theorems are related to the trivial composition series theorems for sets.

In the rest of the paper we shall apply a well known construction and show to what extent the composition series have any relevance to the structure of automata (i.e., to the structure of the systems defined in 1.1).

This construction will provide in fact an alternative proof for our previous theorems and also some insight into their meaning and significance.

3.3 Let A be an automaton. We define the binary relation $\prec$ on S_A as follows:

$$s_1 \prec s_2 \text{ iff}_{df} \; s_2 \in s_1 \cdot W \quad .$$

Denote by S^*_A the set of equivalence classes of S_A defined by the symmetric part of $\prec$ and partially ordered by $\prec$ itself. That is, s_1 and s_2 belong to the same block in S^*_A (in symbols, $[s_1]=[s_2]$) iff $s_1 \prec s_2$ and $s_2 \prec s_1$; A block $[s_1]$ in S^*_A precedes $[s_2]$ (in symbols, $[s_1] \prec [s_2]$) iff $s_1 \prec s_2$.

3.4 We can regard S^*_A as <u>nondeterministic</u> automaton whose operation is

$$[s]\cdot W =_{df} \{[s_1\cdot W] \; : \; s_1 \in [s]\} \; .$$

3.5 For our needs here we do not use all the information given in S^*_A. Thus we define D(A) to be a <u>directed graph</u> defined by:

3.5.1 The nodes of D(A) are the blocks of S^*_A;

3.5.2 The binary relation of D(A) is $\prec$ as defined in S^*_A (cf. 3.3).

3.6 In order to verify that in fact D(A) determines the structure of the composition series of A we need the following notion.

We call a collection $\mathcal{I}$ of nodes of D(A) (i.e., of blocks in S^*_A) an <u>ideal</u> of D(A) (i.e., of S^*_A) iff it is closed to the right under $\prec$. That is, $\mathcal{I}$ is an ideal iff

$$[s_1] \in \mathcal{I} \text{ and } [s_1] \prec [s_2] \text{ imply } [s_2] \in \mathcal{I} \; .$$

For example, S^*_A itself is an ideal. We denote by $\mathcal{I}(A)$ the class of all ideals of D(A) partially ordered by set inclusion.

3.6.1 LEMMA: The mapping

$$J \; : \; SUB(A) \to \mathcal{J}(A) \; : \; B \to \{[s] : s \in S_B\}$$

is an isomorphism of the lattice SUB(A) of the subautomata of A and the lattice $\mathcal{J}(A)$ of the ideals in D(A).

Proof: Immediate.

3.6.2 COROLLARY: Let A_1 and A_2 be two subautomata of A, then A_1 is a maximal subautomaton of A_2 iff $J(A_2) - J(A_1)$ contains a single node of D(A).

Clearly we have now:

3.6.3 THEOREM: (i) An automaton A has a composition series iff S_A^* is finite.

(ii) If A has a composition series then $\ell(A)$ is exactly the cardinality of S_A^*.

(iii) If A has a composition series then the number of all composition series of A is exactly the number of all possible extensions of $\dashv$ into a complete order of S_A^*.

3.7 These results imply that the study of composition series of automata is in fact the study of the relation $\dashv$ associated with automata.

3.8 Every morphism $A \xrightarrow{f} B$ of automata (cf. 1.4) determines a homomorphism $D(A) \xrightarrow{D(f)} D(B)$ defined by

$$[D(f)]([s]) =_{df} [f(s)]$$

($D(f)$ is well defined since $s_1 \sim s_2$ implies $f(s_1) \sim f(s_2)$). Thus we have defined in fact a functor from the category of automata to the category of (directed graphs of) partial orders.

4. EXTENSIONS OF Q-AUTOMATA

1. DEFINITIONS

1.1 Our problem is to characterize all automata B such that for given A and C we have $B/A = C$.

It is obvious that it is necessary that O_W is a subautomaton of C. On the other hand, any occurrance of O_W as a subautomaton of C presents of course a different task of extensions.

1.2 We define therefore a <u>q-automaton</u> to be a pair (C,s_O) where s_O is a state of the automaton C for which $s_O \cdot w = s_O$ for all $w \in W$.

A morphism $C \xrightarrow{f} C'$ is said to be a <u>q-morphism</u> of (C,s_O) into (C',s_O') iff s_O is the only state of C which is mapped by f on s_O'.

1.3 Let B be any automaton, (C,s_O) be a q-automaton. Then, for a morphism $B \xrightarrow{\sigma} (C,s_O)$, which is determined by the morphism $B \xrightarrow{\sigma} C$, we can define $\mathrm{Ker}\sigma$ as the maximal subautomaton of B which is mapped under σ onto s_O (or more precisely, onto the subautomaton of C generated by s_O).

A morphism $B \xrightarrow{\sigma} (C,s_O)$ is said to be a <u>contraction</u> iff apart from $\mathrm{Ker}\sigma \to O_W$, σ is injective. That is iff for any $s_1, s_2 \in S_B - S_{\mathrm{Ker}\sigma}$, $\sigma(s_1) = \sigma(s_2)$ implies $s_1 = s_2$. It is said to be a <u>canonical contraction</u> iff for any $s \in S_B - S_{\mathrm{Ker}\sigma}$, $\sigma(s) = s$.

1.4 An <u>extension sequence</u> (<u>from A to (C,s_O)</u>) is a diagram

$$E = (x,\sigma): \quad A \xrightarrow{x} B \xrightarrow{\sigma} (C,s_O)$$

where

(i) A and B are automata,

(ii) $A \xrightarrow{x} B$ is monic,

(iii) (C,s_O) is a q-automaton,

(iv) $B \xrightarrow{\sigma} (C, s_O)$ is a contraction,

(v) $x(A) = \mathrm{Ker}\sigma$

(vi) $s_o \notin S_B$.

$E = (x,\sigma)$ is said to be a canonical extension iff $A \overset{x}{\rightarrow} B$ is the inclusion morphism (i.e., $x(s) = s$ for all $s \in S_A$) and σ is a canonical contraction.

1.4.1 PROPOSITION: If A is a subautomaton of B then

$$A \overset{j_A}{\longrightarrow} B \overset{q_A}{\longrightarrow} (B/A, s_A^*)$$

(for the inclusion morphism j_A and the canonical morphism $B \overset{q_A}{\rightarrow} B/A$) is a canonical extension.

1.5 An Ext-morphism $\Gamma = E \rightarrow E'$ is a triple $\Gamma = (\alpha,\beta,\gamma)$ of morphisms for which the following diagram is commutative;

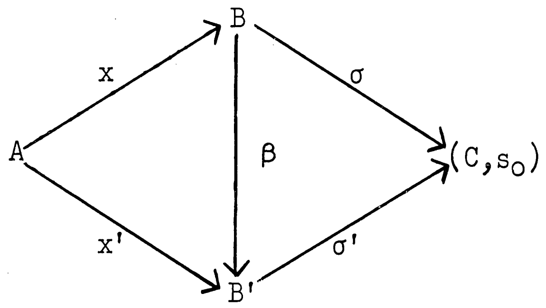
$$\begin{array}{ccccccc} E & : & A & \overset{x}{\longrightarrow} & B & \overset{\sigma}{\longrightarrow} & (C\ ,s_o) \\ \Gamma \downarrow & & \alpha \downarrow & & \downarrow \beta & & \downarrow \sigma' \\ E' & : & A' & \overset{x'}{\longrightarrow} & B' & \longrightarrow & (C',s_o') \end{array}$$

where naturally we require that γ is a q-morphism.

1.5.1 Obviously the class of extension sequences and Ext-morphisms forms a category.

1.6 LEMMA: If $\Gamma = (i_A,\beta,i_C) : E \rightarrow E'$ is an Ext-morphism (where i_A and i_C are identity morphisms) then $B \overset{\beta}{\rightarrow} B'$ is an isomorphism.

Proof: We have to consider the following commutative diagram.



Assume first that $\beta(s_1) = \beta(s_2)$ for some s_1, $s_2 \in S_B$.

If both s_1 and s_2 are in the image of x; say $s_1 = x(t_1)$ and $s_2 = x(t_2)$ for t_1, $t_2 \in S_A$. Then we have

$$x'(t_1) = \beta(x(t_1)) = \beta(x(t_2)) = x'(t_2) ,$$

which implies $t_1 = t_2$ let alone $s_1 = s_2$.

If both s_1 and s_2 are outside of the image of x then we have

$$\sigma(s_1) = \sigma'(\beta(s_1)) = \sigma'(\beta(s_2)) = \sigma(s_2) .$$

But σ is a contraction and therefore we derive $s_1 = s_2$.

If $s_1 \in S_{x(A)}$ and $s_2 \in S_B - S_{x(A)}$, then $\sigma(s_1) = s_0$ and $\sigma(s_2) \neq s_0$. But now we have again

$$\sigma(s_1) = \sigma'(\beta(s_1)) = \sigma'(\beta(s_2)) = \sigma(s_2) .$$

In conclusion $\beta(s_1) = \beta(s_2)$ always implies $s_1 = s_2$ and therefore β is monic.

Now let $s \in S_B$. If s is in the range of x', say $s = x'(t)$ for $t \in S_A$. Then $\beta(x(t)) = x'(t) = s$. If s is not in the range of x' then there is $s_b \in S_B$ such that $\sigma(s_b) = \sigma'(s)$. Hence

$$\sigma'(\beta(s_b)) = \sigma(s_b) = \sigma'(s) ,$$

but s is not in $\mathrm{Ker}\sigma'$ and therefore we have $\beta(s_b) = s$. Thus β is epic.

1.6.1 REMARK: Note that if $\Gamma = (i_A, \beta, i_C) : E \to E'$ is an Ext-morphism then β is the unique morphism for which $(i_A, \beta, i_C) : E \to E'$ is an Ext-morphism. This follows from Lemma 1.6 and the immediate fact that if (i_A, β, i_C) is an Ext-morphism of E into itself it is the identity Ext-morphism.

1.6.2 We define two extension sequences E and E' to be congruent (in symbols, $E \equiv E'$) iff there is an Ext-morphism $\Gamma = (i_A, \beta, i_C) : E \to E'$.

By Lemma 1.5 we have that the congruence of extension sequences is an equivalence relation.

1.7 Let A be an automaton and (C, s_0) a q-automaton. We denote by $Ext(C, s_0, A)$ the set of all congruence classes of the extension sequences from A to (C, s_0).

2. CLASSICAL RESULTS

2.1 Before we characterize $Ext(C, s_0, A)$ by means of the particular properties of extensions of automata we shall give several examples that show how close $Ext(C, s_0, A)$ is to the classical notion of extension in commutative algebra. In fact some of the proofs of the following "classical" properties, follow their seniors closely (cf. MacLane 1963).

2.2 LEMMA: If

$$E : A \overset{x}{\to} B \overset{\sigma}{\to} (C, s_0)$$

is an extension sequence and if

$$(C', s_0') \overset{\gamma}{\to} (C, s_0)$$

is a q-morphism, then there exists an extension sequence

$$E_\gamma : A \xrightarrow{x'} B' \xrightarrow{\sigma'} (C', s_0')$$

and an Ext-morphism

$$\Gamma_\gamma \;=\; (i_A,\beta,\gamma) : E_\gamma \to E$$

where (E_γ,β) is unique up to a congruence of E_γ.

<u>Proof:</u> Let B' be the subautomaton of B x C' defined by

$$S_{B'} \;=\; \{(s_b,s_{c'}) : \sigma(s_b) \;=\; \gamma(s_{c'})\} \;.$$

$S_{B'}$ is a closed set of states in B x C' since

$$(s_b,s_{c'})\cdot w \;=\; (s_b\cdot w,\ s_{c'}\cdot w) \;,$$

and

$$\sigma(s_b\cdot w) \;=\; \sigma(s_b)\cdot w \;=\; \gamma(s_{c'})\cdot w \;=\; \gamma(s_{c'}\cdot w) \;.$$

For the completion of the following diagram

$$\begin{array}{ccccccc}
E_\gamma & : & A & \overset{x'}{\dashrightarrow} & B' & \overset{\sigma'}{\dashrightarrow} & (C',s_0') \\
\Gamma_\gamma \downarrow & & \| & & \vdots\ \beta & & \downarrow \gamma \\
E & : & A & \overset{x}{\longrightarrow} & B & \overset{\sigma}{\longrightarrow} & (C,\ s_0)
\end{array} \;,$$

define

$$\sigma' : S_{B'} \to S_{C'} : (s_b,s_{c'}) \to s_{c'}$$

$$x' : S_A \to S_{B'} : s \to (x(s),s_0') \;,$$

and

$$\beta : S_{B'} \to S_B : (s_b,s_{c'}) \to s_b \;;$$

then obviously we have $\sigma\beta = \gamma\sigma'$ and $\beta x' = x$.

We have to check whether the following sequence is in fact an extension sequence.

$$A \xrightarrow{x'} B' \xrightarrow{\sigma'} (C', s_0') \ .$$

Now, $\sigma'(s_b, s_{c'}) = s_0'$ iff $s_{c'} = s_0$; but $(s_b, s_0') \epsilon S_{B'}$ iff $\sigma(s_b) = \gamma(s_0') = s_0$. Hence $(s_b, s_{c'})$ is in Kerσ' iff s_b is in $x(A)$ and $s_c' = s_0'$.

Let $(s_b, s_{c'})$ be a state of B' which is not in Kerσ'; in particular we have $s_{c'} \neq s_0'$. From $\sigma(s_b) = \gamma'(s_{c'})$ it follows that $\sigma(s_b) \neq s_0$, since γ is a q-morphism. Hence, there is a unique $s_b \in S_B$ such that $\sigma(s_b) = \gamma(s_{c'})$ and therefore σ' is a contraction from B' to (C', s_0') with Ker$\sigma' = x'(A)$.

Obviously $A \xrightarrow{x'} B'$ is monic since $x'(s_1) = x'(s_2)$ implies in particular $x(s_1) = x(s_2)$. Therefore E_γ is an extension sequence.

The uniqueness of (E_γ, β) will follow from the next lemma.

2.3 LEMMA (The Couniversal Property of E_γ):

For any Ext-morphism

$$\Gamma_1 = (\alpha_1, \beta_1, \gamma) : E_1 \to E$$

there is a unique factorization (up to a congruence) of Γ_1 through $\Gamma_\gamma : E_\gamma \to E$, of the form:

$$\Gamma_1 = (E_\gamma \xrightarrow{(i_A, \beta, \gamma)} E)\ (E_1 \xrightarrow{(\alpha_1, \beta', i_{C'})} E_\gamma) \ .$$

Proof: We have the following diagram for Γ_1:

$$\begin{array}{ccccccc} E_1 & : & A_1 & \xrightarrow{x_1} & B_1 & \xrightarrow{\sigma_1} & (C', s_0') \\ \Gamma_1 \downarrow & & \downarrow \alpha_1 & & \downarrow \beta_1 & & \downarrow \gamma \\ E & : & A & \xrightarrow{x} & B & \xrightarrow{\sigma} & (C, s_0) \end{array}$$

and we want to stretch it to become the following commutative diagram which includes the diagram of Γ_γ:

$$
\begin{array}{ccccccccc}
E_1 & : & A_1 & \xrightarrow{x_1} & B_1 & \xrightarrow{\sigma_1} & (C', s_0') & & \\
\Gamma' \big\downarrow & & \big\downarrow & \alpha_1 & \big\downarrow & \beta' & \big\updownarrow = & & \\
E_\gamma & : & A & \xrightarrow{x'} & B' & \xrightarrow{\sigma'} & (C', s_0') & & \\
\Gamma_\gamma \big\downarrow & & \big\updownarrow & = & \big\downarrow & \beta & \big\downarrow \gamma & & \\
E & : & A & \xrightarrow{x} & B & \xrightarrow{\sigma} & (C, s_0) & . &
\end{array}
$$

The only way to guarantee that $\beta_1 = \beta\beta'$ and that the above diagram is commutative is to define:

$$\beta' : S_{B_1} \to S_B : s_{b_1} \to (\beta_1(s_{b_1}), \sigma_1(s_{b_1})) .$$

2.3.1 <u>REMARK:</u> The uniqueness of E_γ now follows immediately. For assume that for some $\Gamma = (i_A, \beta'', \gamma)$ we have $\Gamma : E' \to E$ then by Lemma 2.3, Γ has the factorization

$$(i_A, \beta'', \gamma) = (i_A, \beta, \gamma)(i_A, \beta', i_{C'})$$

with a factor $(i_A, \beta', i_{C'}) : E' \to E_\gamma$ which is a congruence of E_γ.

Similarly we can show that if $E_1 \equiv E_2$ then $(E_1\gamma) \equiv (E_2\gamma)$.

2.3.2 Hence, q-morphisms into (C, s_0) induce Ext-morphisms into $\mathrm{Ext}(C, s_0, A)$, and with this Ext (C, s_0, A), varying on (C, s_0), becomes a controvariant functor from the category of q-automata and q-morphisms into the category of extensions of automata (being the congruence classes of extension sequences) and Ext-morphisms.

2.4 <u>LEMMA:</u> For any extension sequence

$$E : A \overset{x}{\to} B \overset{\sigma}{\to} (C, s_0)$$

and any morphism $A \overset{\alpha}{\to} A'$ there is an extension sequence

$$\alpha E : A' \xrightarrow{x'} B' \xrightarrow{\sigma'} (C, s_0)$$

and an Ext-morphism

$$\alpha\Gamma = (\alpha, \beta, i_C) : E \to \alpha E$$

where $(\alpha E, \beta)$ is unique up to a congruence of αE.

<u>Proof:</u> We are concerned now with the following diagram.

$$\begin{array}{ccccccc} E & : & A & \xrightarrow{x} & B & \xrightarrow{\sigma} & (C, s_0) \\ \alpha\Gamma \big\downarrow & & \big\downarrow & \alpha & \big\downarrow & \beta & \big\updownarrow = \\ \alpha E & : & A' & \xrightarrow{x'} & B' & \xrightarrow{\sigma'} & (C, s_0) \end{array}$$

In this case we define $B \overset{\beta}{\to} B'$ by a congruence relation $\sim\alpha$ in B which is induced by $A \overset{\alpha}{\to} A'$.

Set $s_1 \sim\alpha\ s_2$ (for any s_1, $s_2 \in S_B$) iff either they are both in $x(A) = \mathrm{Ker}\sigma$ and then $\alpha(x^{-1}(s_1)) = \alpha(x^{-1}(s_2))$, or else, if $s_1 = s_2$.

In order to verify that $\sim\alpha$ is a congruence of B, consider the crucial case where $s_1 \sim\alpha\ s_2$ holds because $s_1 = x(s_1')$ $s_2 = x(s_2')$ and $\alpha(s_1') = \alpha(s_2')$.

Now for any $w \in W$ we have that both $s_1 \cdot w$ and $s_2 \cdot w$ are in $x(A)$ and

$$\begin{aligned} \alpha(x^{-1}(s_1 \cdot w)) &= \alpha(x^{-1}(x(s_1') \cdot w)) = \alpha(x^{-1}(x(s_1' \cdot w))) \\ &= \alpha(s_1' \cdot w) = \alpha(s_1') \cdot w = \alpha(s_2') \cdot w \\ &= \alpha(x^{-1}(s_2 \cdot w)) . \end{aligned}$$

Thus $s_1 \sim\alpha\ s_2$ implies $s_1 . w \sim\alpha\ s_2 \cdot w$.

Hence $B' =_{df} B/{\sim\alpha}$ is well defined together with a canonical morphism

$$B \overset{\beta}{\to} B/{\sim\alpha} .$$

The definitions of $A' \xrightarrow{x'} B'$ and of $B' \xrightarrow{\sigma'} (C, s_0)$ follow naturally. The verification that we have now an Ext-morphism $\alpha\Gamma = (\alpha, \beta, i_C) : E \to \alpha E$, where

$$\alpha E : A' \xrightarrow{x'} B' \xrightarrow{\sigma'} (C, s_0) ,$$

is routine.

The uniqueness of $(\alpha E, \beta)$ follows from the next lemma.

2.5 <u>LEMMA (The Universal Property of αE):</u> Any Ext-morphism

$$\Gamma_1 = (\alpha, \beta_1, \gamma_1) : E \to E_1$$

can be factorized uniquely through $E \to \alpha E$:

$$\Gamma_1 = (\alpha E \xrightarrow{(i_A, \beta', \gamma_1)} E_1)\ (E \xrightarrow{(\alpha, \beta, i_C)} \alpha E) .$$

<u>Proof:</u> We define $B' \xrightarrow{\beta'} B_1$ by

$$\beta' : S_{B'} = (S_B)/{\sim}\alpha \to S_{B_1}$$

$$\beta'([s_b]) = \begin{cases} x_1(s'_a) \text{ if } x'(s'_a) = [s_b] , \\ \\ \gamma_1(\sigma'([s_b])) \text{ otherwise} ; \end{cases}$$

which is the only way to make the following diagram commutative. The

$$\begin{array}{ccccccc}
E & : & A & \xrightarrow{x} & B & \xrightarrow{\sigma} & (C, s_0) \\
\alpha\Gamma \Big\downarrow & & \Big\downarrow & \alpha & \Big\downarrow & \beta & \Big\updownarrow = \\
\alpha E & & A' & \xrightarrow{x'} & B' & \xrightarrow{\sigma'} & (C, s_0) \\
\Gamma' \Big\downarrow & & \Big\updownarrow & = & \Big\downarrow & \beta' & \Big\downarrow \gamma_1 \\
E_1 & : & A' & \xrightarrow{x_1} & B_1 & \xrightarrow{\sigma_1} & (C_1, s'_0)
\end{array}$$

rest follows by a direct verification.

2.5.1 Again we have that αE is determined up to a congruence; and therefore, morphisms of automata induce Ext-morphisms of extensions. Now we have that

$\text{Ext}(C,s_0,A)$, varying on A, is a covariant functor from the category of automata into the category of extensions.

2.5.2 The following proposition (cf. MacLane 1963) which is in fact a direct corollary of Lemmata 2.3 and 2.5, implies that $\text{Ext}(C,s_0,A)$ is a bifunctor.

2.5.3 PROPOSITION: Let

$$E : A \overset{x}{\to} B \overset{\sigma}{\to} (C,s_0)$$

by an extension sequence; then for any morphism α of A and any q-morphism γ into (C,s_0) we have

$$\alpha(E_\gamma) \equiv (\alpha E)_\gamma .$$

Proof (MacLane): We have the Ext-morphisms

$$E_\gamma \xrightarrow{(i_A,\beta_1,\gamma)} E, \qquad E \xrightarrow{(\alpha,\beta_2,i_C)} \alpha E$$

and their composition

$$E_\gamma \xrightarrow{(\alpha,\beta_2\beta_1,\gamma)} \alpha E .$$

By the universal properties of $E_\gamma \to E$ and $E \to \alpha E$ applied to $(\alpha E)\gamma \to \alpha E$ and to $E_\gamma \to \alpha(E_\gamma)$, we get the following two factorizations of $E_\gamma \to \alpha E$:

$$E_\gamma \xrightarrow{(\alpha,\beta',i)} (\alpha E)_\gamma \xrightarrow{(i,\beta_2\beta_1,\gamma)} \alpha E$$

and

$$E_\gamma \xrightarrow{(\alpha,\beta_2\beta_1,i)} \alpha(E_\gamma) \xrightarrow{(i,\beta'',\gamma)} \alpha E .$$

Consider any one of them; say, $E_\gamma \xrightarrow{(\alpha,\beta',i)} (\alpha E)_\gamma$. The morphism α induces the Ext-morphism $E_\gamma \xrightarrow{(\alpha,\beta^*,i)} \alpha(E_\gamma)$, and therefore by the uniqueness of

$\alpha(E_\gamma)$ we infer $(\alpha E)_\gamma \equiv \alpha(E_\gamma)$.

2.5.4 The following proposition is another example of a result derived by a direct application of the universal properties of the functor $\mathrm{Ext}(C, s_o, A)$ following the classical example (cf. MacLane 1963).

2.5.5 PROPOSITION: For any Ext-morphism $\Gamma = (\alpha, \beta, \gamma) : E_1 \to E_2$ we have $\alpha E_1 \equiv E_2\gamma$.

Proof (MacLane): By the universal property of $E \to \alpha E$, Γ can be factorized through $\alpha\Gamma : E_1 \to \alpha E_1$:

$$\Gamma = \Gamma_1 (\alpha\Gamma), \Gamma_1 = (i_A, \beta', \gamma) : \alpha E_1 \to E_2 .$$

But Γ_1 is a definition of $\Gamma_\gamma : E_{2\gamma} \to E_2$ hence $\alpha E_1 \equiv E_{2\gamma}$.

2.6 We can interpret the functor $\mathrm{Ext}(C, s_o, A)$ as applied to morphisms of A as a mapping

$$E^* : \mathrm{Hom}(A_1, A) \to \mathrm{Ext}(C, s_o, A) : \alpha \to \alpha E$$

defined for any $E \in \mathrm{Ext}(C, s_o, A_1)$.

Dually, for any $E \in \mathrm{Ext}(C', s_o', A)$ we have a mapping

$$E_* : \mathrm{Hom}_q((C', s_o'), (C, s_o)) \to \mathrm{Ext}(C, s_o, A) : \gamma \to E\gamma;$$

(where $\mathrm{Hom}_q(X, Y)$ denotes of course the class of all q-morphisms from X to Y).

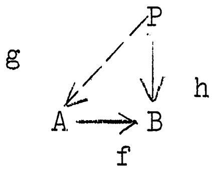
We shall be interested mainly in the "connecting" mapping

$$E_* : \mathrm{Hom}(A_1, A) \to \mathrm{Ext}(C, s_o, A) : \alpha \to \alpha E$$

because it gives rise to a complete characterization of $\mathrm{Ext}(C, s_o, A)$.

3. PROJECTIVE EXTENSIONS

3.1 An automaton P is said to be projective iff for any morphism $P \overset{h}{\to} B$ and any epic $A \overset{f}{\to} B$ there exists a morphism $P \overset{g}{\to} A$ for which the following diagram is commutative.



3.1.1 For example, the automaton M_W defined by

$$S_{M_W} = W$$

$$w_1 \cdot w_2 = w_1 w_2$$

is projective.

This follows from the fact that the homomorphic images of M_W are exactly the monogenic automata and $\mathrm{Hom}(M_W, A)$ is in a bijective correspondence with S_A.

In fact, as one can easily prove, the free automata are exactly the direct multiples of M_W, and every free automaton is projective.

3.2 LEMMA: If P is projective and $E_1 : P_1 \overset{j}{\to} P \overset{q}{\to} (C', s_0')$ is an extension sequence, then for any extension sequence

$$E : A \overset{x}{\to} B \overset{\sigma}{\to} (C, s_0)$$

and any q-morphism $(C', s_0') \overset{\gamma}{\to} (C, s_0)$ there exists an Ext-morphism

$$\Gamma = (\alpha, \beta, \gamma) : E_1 \to E .$$

Proof: By the projectivity of P we have a morphism $P \overset{\beta}{\to} B_1$ for which the following diagram is commutative.

$$\begin{array}{ccc} P & \xrightarrow{q} & (C', s'_o) \\ \beta \big\downarrow & & \big\downarrow \gamma \\ B & \xrightarrow{\sigma} & (C, s_o) \end{array}$$

Since q and σ are contractions, the commutativity of the previous diagram implies also $\beta(\text{Ker} q) = \text{Ker}\sigma$. Hence, since $A \overset{x}{\rightarrow} B$ is monic, there exists a morphism $P_1 \overset{\alpha}{\rightarrow} A$ such that the following diagram is commutative.

$$\begin{array}{ccccccc} E_1 & : & P_1 & \xrightarrow{j} & P & \xrightarrow{q} & (C', s'_o) \\ \Gamma \big\downarrow & & \big\downarrow \alpha & & \big\downarrow \beta & & \big\downarrow \gamma \\ E & : & A & \xrightarrow{x} & B & \xrightarrow{\sigma} & (C, s_o) \end{array}$$

Hence $\Gamma = (\alpha, \beta, \gamma) \; : \; E_1 \rightarrow E$.

3.2.1 <u>COROLLARY</u>: Let

$$E_1 \; : \; P_1 \overset{i}{\rightarrow} P \overset{q}{\rightarrow} (C, s_o)$$

be any extension sequence where P is projective; then for any $E \epsilon \text{Ext}(C, s_o, A)$ there exists an $\alpha \epsilon \text{Hom}(P_1, A)$ such that $\alpha E_1 \equiv E$.

<u>Proof</u>: Set $\gamma = i_C$ and get

$$\Gamma = (\alpha, \beta, i_C) \; : \; E_1 \rightarrow E$$

but this implies $\alpha E_1 \equiv E$.

A rephrasing of this Corollary, using the notation of 2.6, yields the following theorem.

3.2.2 THEOREM: Let E_1 be an extension sequence with P projective

$$E_1 \quad : \quad P_1 \overset{j}{\to} P \overset{q}{\to} (C,\ s_o) \quad ,$$

then for any automaton A

$$E_1^* \quad : \quad \mathrm{Hom}(P_1,\ A) \to \mathrm{Ext}(C,\ s_o,\ A)$$

is surjective.

3.2.3 If $(C,\ s_o)$ is a q-automaton which has a projective extension; i.e., if there exists an extension sequence of the form

$$E_1 \quad : \quad P_1 \overset{j}{\to} P \overset{q}{\to} (C,\ s_o)$$

where P is projective; then, by Theorem 3.2.2 we can construct all the extensions of $\mathrm{Ext}(C,\ s_o,\ A)$ for any automaton A.

However, since not every q-automaton has a projective extension, this result is not general enough.

4. THE CHARACTERIZATION OF $\mathrm{Ext}(C,\ s_o,\ A)$ BY MEANS OF THE CONNECTING HOMOMORPHISM

4.1 In order to get a general characterization of $\mathrm{Ext}(C,\ s_o,\ A)$ we construct the following extension sequence.

Denote by $S_C \times M_W$ the automaton which has $S_C \times W = \{(s,\ w) \ : \ s \in S_C,\ w \in W\}$ as its set of states and whose transition function is $(s,\ w_1) \cdot w_2 = (s,\ w_1 w_2)$. Clearly, $S_C \times M_W$ is the direct sum (i.e., disjoint union) of isomorphic copies of M_W indexed by the states of C. Thus $S_C \times M_W$ is a free automaton and in particular we have the natural morphism

$$S_C \times M_W \xrightarrow{\ \tau_C\ } C$$

which is determined by

$$\tau_C \; : \; S_C \times W \to S_C \; : \; (s, w) \to s \cdot w$$

the transition function of C itself.

The q-automaton (C, s_o) determines a subset of states of $S_C \times M_W$:

$$K =_{df} \{(s, w) \; : \; s \cdot w = s_o\} \; ,$$

which is closed under transitions. Hence it determines a subautomaton <u>$Con(C, s_o)$</u> of $S_C \times M_W$ whose set of states is K.

The <u>free extension sequence of (C, s_o), $F(C, s_o)$</u>, is defined to be

$$F(C, s_o) \; : \; Con(C, s_o) \overset{j}{\to} S_C \times M_W \overset{q}{\to} (q_j(S_C \times M), s_o')$$

as determined by $Con(C, s_o) \subseteq S_C \times M_W$, where

$$q_j(S_C \times M_W) = (S_C \times M_W)/Con(C, s_o)$$

4.2 The morphism $S_C \times M_W \xrightarrow{\tau_C} C$ determines a q-morphism

$$(q_j(S_C \times M_W), s_o') \overset{\gamma}{\to} (C, s_o)$$

in a natural manner: if $s \cdot w \neq s_o$ then we set $\gamma(s, w) = s \cdot w$, otherwise we set $\gamma(s_o') = s_o$.

This q-morphism determines an Ext-morphism

$$\Gamma = (i, \beta^*, \gamma) \; : \; F(C, s_o) \to E(C, s_o)$$

where $E(C, s_o)$ is the canonical extension in $Ext(C, s_o, Con(C, s_o))$:

$$E(C, s_o) \; : \; Con(C, s_o) \xrightarrow{j^*} (C, s_o)^* \xrightarrow{q^*} (C, s_o)$$

$$S_{(C, s_o)^*} = K \cup S_C - \{s_o\}$$

The transition function of $(C, s_o)^*$ is composed of those of C and of $S_C \times M_W$, together with the stipulation:

$$s \cdot w \;=\; (s,\ w) \quad \text{whenever} \quad s \cdot w \;=\; s_o \text{ in } C.$$

The morphism $S_C \times M_W \xrightarrow{\beta^*} (C,\ s\ )^*$ is defined naturally by

$$\beta^*(s,\ w) \;=\; s \cdot w \quad \text{in} \quad (C,\ s_o)^*.$$

The commutativity of the following diagram

$$\begin{array}{ccccccc}
F(C,\ s_o) & : & Con(C,\ s_o) & \xrightarrow{j} & S_C \times M_W & \xrightarrow{q} & (q_j(S_C \times M_W),\ s_o') \\
\Gamma \big\downarrow & & \big\updownarrow = & & \big\downarrow \beta^* & & \big\downarrow \gamma \\
E(C,\ s_o) & : & Con(C,\ s_o) & \xrightarrow{j^*} & (C,\ s_o)^* & \xrightarrow{q^*} & (C,\ s_o)
\end{array}$$

is straightforward.

4.3 THEOREM: For any automaton A and any q-automaton $(C,\ s_o)$, the mapping

$$E^*(C,\ s_o):\ \text{Hom}(\text{Con}(C,\ s_o),\ A) \to \text{Ext}(C,\ s_o,\ A):\ \alpha \to \alpha E(C,\ s_o)$$

is a bijection.

Proof: We define a map

$$\text{Con}^* \;:\; \text{Hom}(\text{Con}(C,\ s_o),\ A) \to \text{Ext}(C,\ s_o,\ A)$$

as follows.

For any $\alpha \in \text{Hom}(\text{Con}(C,\ s_o),\ A)$ we obviously have $\alpha = \oplus\alpha_s$ where s varies on S_C with the provision that $s_o \in s \cdot W$; and α_s is the restriction of α to the morphism of $I(s)$, the subautomaton of $\text{Con}(C,\ s_o)$ whose set of states is

$$S_{I(s)} =_{df} \{(s,\ w) \;:\; s \cdot w \;=\; s_o\} \;.$$

Note that $I(s)$ is isomorphic to a subautomaton of M_W and that

$$\mathrm{Con}(C,\ s_o) \ = \ \bigoplus_s I(s) \quad .$$

To summarize, we have in fact:

$$\mathrm{Hom}(\mathrm{Con}(C,\ s_o),\ A) \ = \ \bigoplus_s \mathrm{Hom}(I(s),\ A) \ : \ \alpha \ = \ \bigoplus_s \alpha_s \ ,$$

and $\alpha_s = \alpha | I(s)$.

We define $\mathrm{Con}(\alpha)$ as the automaton whose set of states is

$$S_{\mathrm{Con}(\alpha)} =_{df} S_C \cup S_A - \{s_o\}$$

and whose transition function is

$$s \cdot w \ = \begin{cases} \alpha(s,\ w) \ = \ \alpha_s(s,\ w) & \text{if} \quad (s,\ w) \in I(s) \ , \\ s \cdot w \text{ in } C \text{ if } s \in S_C & \text{and} \quad (s,\ w) \notin I(s) \ , \\ s \cdot w \text{ in } A, \text{ otherwise} & . \end{cases}$$

Denote by $\mathrm{Con}^*(\alpha)$ the canonical extension sequence

$$\mathrm{Con}^*(\alpha) \ : \ A \xrightarrow{x_\alpha} \mathrm{Con}(\alpha) \xrightarrow{\sigma_\alpha} (C,\ s_o)$$

which is naturally associated with $\mathrm{Con}(\alpha)$.

We leave to the reader the verification of the following statements which lead to the conclusion of the proof of the theorem.

4.3.1 Con^* maps $\mathrm{Hom}(\mathrm{Con}(C,\ s_o),\ A)$ in a bijective manner onto the class of all canonical extension sequences

$$A \overset{x}{\to} B \overset{\sigma}{\to} (C,\ s_o)$$

of A by $(C,\ s_o)$ with $A \subseteq B$.

4.3.2 <u>LEMMA</u>: For any two canonical extension sequences E_1 and E_2, $E_1 \equiv E_2$ holds iff $E_1 = E_2$.

4.3.3 For any $\alpha \epsilon \mathrm{Hom}(\mathrm{Con}(C, s_o), A)$ we have the congruence

$$\alpha E(C, s_o) \equiv \mathrm{Con}^*(\alpha) \quad .$$

4.3.4 Alternatively, one can define an Ext-morphism

$\Gamma(\alpha) = (\alpha, \alpha^*, i) : E(C, s_o) \to \mathrm{Con}^*(\alpha)$ by defining a morphism $(C, s_o)^* \xrightarrow{\alpha^*} \mathrm{Con}(\alpha)$ in a very natural manner. Then, by the uniqueness of $\alpha E(C, s_o)$ we infer 4.3.3.

BIBLIOGRAPHY

1. Give'on, Y., "Outline for an Algebraic Study of Event Automata," Tech. Report 05662, 06689, 03105-28-T, ORA, The University of Michigan (1964).

2. MacLane, S., Homology, Academic Press, New York, (1963).

3. Papy, Groupes, Dunod, Paris, 1961.

4. Rees, D., "On Semi-Groups," Proc. Cambridge Philos. Soc., 36, 381-400, (1940).

5. Thatcher. J. W., "Notes on Mathematical Automata Theory," Tech. Note 05662, 03105-26-T, ORA, The University of Michigan (1963).

6. Zariski, O. and Samuel, P., Commutative Algebra, Van Nostrand Co., Inc., Princeton, N.J., 1962.

TOWARD A HOMOLOGICAL ALGEBRA OF AUTOMATA IV:

5. The Characterization of Projective Automata

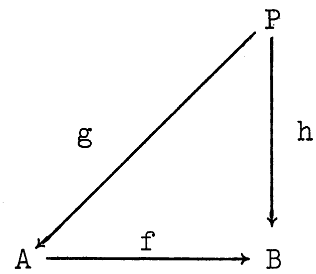
0. INTRODUCTION

0.1 Following the main problem of our first paper in this series, we want to characterize the projective objects of $\mathcal{A}_W$, the category of automata (as state diagrams) with W as input.

0.2 Naturally, we follow our notation and terminology set up in our previous papers (Give'on 1964).

1. BASIC NOTIONS

1.1 We recall that an automaton P is projective iff for any morphism $P \xrightarrow{h} B$ and any epic $A \xrightarrow{f} B$ there exists a morphism $P \xrightarrow{g} A$ for which the following diagram is commutative.



1.2 For any automaton A and any set T we define $T \cdot A$ to be the automaton whose set of states is

$$T \times S_A = \{(t, s) : t \in T \;\&\; s \in S_A\}$$

and whose transition function is defined by

$$(t, s) \cdot w =_{df} (t, s \cdot w) \quad .$$

Obviously $T \cdot A = \bigoplus_{t \in T} (\{t\} \cdot A)$ and $\{t\} \cdot A \approx A$.

1.3 It is easy to verify that for any set T, $T \cdot M_W$ is free and projective.

1.4 We are trying to follow the study of projective modules as closely as possible.

1.4.1 An <u>epic</u> $A \overset{f}{\to} B$ is said to <u>split</u> iff there is a morphism $B \overset{g}{\to} A$ for which

$$B \overset{g}{\to} A \overset{f}{\to} B = i_B \quad .$$

1.4.2 A <u>monic</u> $B \overset{g}{\to} A$ is said to <u>split</u> iff there is a morphism $A \overset{f}{\to} B$ for which

$$B \overset{g}{\to} A \overset{f}{\to} B = i_B \quad .$$

1.4.3 In general we say a morphism f that it <u>splits</u> iff it is a unit in the composition algebra of the morphisms of $\mathcal{A}_W$. Obviously a morphism splits iff it is either a monic or an epic which splits.

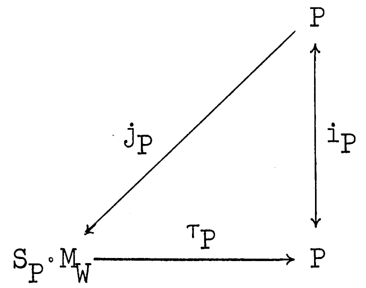
1.4.4 A sequence $A \overset{g}{\to} B \overset{f}{\to} A$ is said to be a <u>splitting sequence of A through B</u> iff $fg = i_A$.

Clearly in this case f is an epic and g is a monic which split.

1.5 <u>LEMMA</u>. An automaton P is projective iff it has a splitting sequence through some free automaton $T \cdot M_W$.

<u>Proof</u>: We always have an epic $S_P \cdot M_W \xrightarrow{\tau_P} P$ defined by $\tau_P(s, w) = s \cdot w$. Assume that P is projective then for $P \xrightarrow{i_P} P$ there exists a morphism

$P \xrightarrow{j_P} S_P\cdot M_W$ for which the following diagram is commutative,



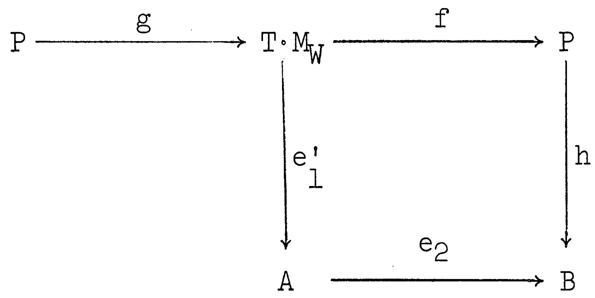
this yields a splitting sequence

$$P \xrightarrow{j_P} S_P\cdot M_W \xrightarrow{\tau_P} P$$

of P through $S_P\cdot M_W$. We shall refer to this sequence as <u>the canonical splitting sequence of P.</u> On the other hand, assume that

$$P \xrightarrow{g} T\cdot M_W \xrightarrow{f} P$$

is a splitting sequence. Let $P \xrightarrow{h} B$ be any morphism and $A \xrightarrow{e_2} B$ be an epic. Since $T\cdot M_W$ is projective, there exists a morphism $T\cdot M_W \xrightarrow{e_1'} A$ for which the following diagram is commutative.



Hence, for $e_1 = e_1'g$ we have

$$e_2e_1 = e_2e_1'g = hfg = h$$

which proves that P is projective.

1.5.1 REMARK: Our arguments show in fact that P_1 is projective iff it has a splitting sequence through some projective automaton P_2.

1.5.2 COROLLARY: Any projective automaton is a direct sum (i.e., disjoint union) of monogenic (i.e., epic images of M_W) projective automata.

Proof: We refer again to the canonical splitting sequence of P

$$P \xrightarrow{j_P} S_P \cdot M_W \xrightarrow{\tau_P} P$$

defined in the proof of Lemma 1.5.

Since $S_P \cdot M_W = \underset{s}{\oplus}\{s\} \cdot M_W$ and $P \xrightarrow{j_P} S_P \cdot M_W$ is monic, we have a decomposition of P as a direct sum $P = \underset{s}{\oplus} P_s$ where

$$S_{P_s} = \{s' \epsilon S_P : j_P(s') \epsilon s \cdot W\} \quad ,$$

and a family of monic morphisms

$$P_s \xrightarrow{j_P^s} \{s\} \cdot M_W$$

defined by

$$j_P^s \quad : \quad S_{P_s} \to \{s\} \times W \quad : \quad s' \to j_P(s') \quad .$$

On the other hand we define a family of morphisms

$$\{s\} \cdot M_W \xrightarrow{\tau_P^s} P$$

by

$$\tau_P^s \quad : \quad \{s\} \times W \to S_P \quad : \quad (s, w) \to s \cdot w \quad .$$

Obviously, for any $s \in S_P$ we have:

$$i_{P_s} = i_P|P_s = \tau_P j_P|P_s = \tau_P j_P^s = \tau_P^s j_P^s \quad ,$$

hence $\tau_P^s(\{s\}\cdot M_W) = P_s$ and therefore P_s is monogenic.

1.5.3 COROLLARY: (The converse of Cor. 1.5.2)

A direct sum of projective automata is projective.

Proof: By Lemma 1.5 we have for $P = \bigoplus_s P_s$ a family of splitting sequences

$$P_s \xrightarrow{g_s} T_s\cdot M_W \xrightarrow{f_s} P_s$$

and we can assume that all the T_s are disjoint. Hence we have the splitting sequence

$$\bigoplus_s P_s \xrightarrow{\bigoplus_s g_s} (\bigcup_s T_s)\cdot M_W \xrightarrow{\bigoplus_s f_s} \bigoplus_s P_s$$

where $\bigoplus_s g_s$ and $\bigoplus_s f_s$ are morphisms defined as the unions of $\{g_s\}$ and of $\{f_s\}$ (resp.). Thus P is projective.

1.6 Thus we have that a direct sum of automata is projective iff each summond is projective. Furthermore, an automaton is projective iff it is a direct sum of monogenic projective automata.

Hence, in order to characterize the projective objects of $\mathcal{A}_W$ we have only to characterize the monogenic projective automata.

2. MONOGENIC PROJECTIVE AUTOMATA

2.1 An automaton P is monogenic iff there exists an epic $M_W \overset{e}{\to} P$.

If P is projective we have a splitting sequence

$$P \overset{j}{\to} M_W \overset{e}{\to} P$$

of P through M_W. Hence, if P is a monogenic projective automaton it is isomorphic to a monogenic subautomaton of M_W.

2.2 An element $u \in W$ is said to be <u>projective</u> iff the subautomaton $M_W(u)$ of M_W generated by u is projective.

2.2.1 Note that the set of states of $M_W(u)$ is the principal right ideal of W generated by u:

$$I(u) = \{uw \ : \ w \in W\} \ .$$

2.3 A rephrasing of Lemma 1.5, as applied to monogenic projective automata, expressed in terms of the elements of W, yields the following proposition.

2.3.1 <u>PROPOSITION:</u> An element $u \in W$ is projective iff there is $j(u) \in W$ for which

(i) $uw_1 = uw_2$ iff $j(u)w_1 = j(u) \cdot w_2$;

and

(ii) $u = uj(u)$.

<u>Proof</u>: By Lemma 1.5 and by 2.1, $M_W(u)$ is projective iff there exists a splitting sequence of $M_W(u)$ through M_W:

$$M_W(u) \xrightarrow{j} M_W \xrightarrow{e_u} M_W(u)$$

where $M_W \xrightarrow{e_u} M_W(u)$ is the canonical morphism determined by

$$e_u \ : \ W \to I(u) \ : \ w \to uw \ .$$

Hence, if $M_W(u)$ is projective, the morphism $M_W(u) \xrightarrow{j} M_W$ is monic. That is,

$$j(uw_1) = j(uw_2) \quad \text{iff} \quad uw_1 = uw_2 \ .$$

But $j(uw_i) = j(u)w_i$, hence (i). In addition to this, $e_u j = i_{M_W(u)}$, and so

$$u = (e_u \circ j)(u) = e_u(j(u)) = uj(u) \ .$$

On the other hand, assume (i) and (ii). Define

$$M_W(u) \xrightarrow{j} M_W$$

by

$$j \ : \ I(u) \to W \ : \ uw \to j(u)w \ ,$$

by (i), j is monic. For the canonical epic $M_W \xrightarrow{e_u} M_W(u)$ we get by (ii)

$$\begin{aligned}(e_u \circ j)(uw) &= e_u(j(uw)) = e_u(j(u)w) \\ &= (uj(u))w = uw \ ,\end{aligned}$$

hence

$$M_W(u) \overset{j}{\to} M_W \overset{e_u}{\longrightarrow} M_W(u)$$

is a splitting sequence and therefore $M_W(u)$ is projective.

2.4 <u>REMARKS</u>: It follows immediately from Prop. 2.3.1 that if u is an idempotent of W then it is projective; set $j(u) = u$.

However, this is not a necessary condition for u being projective. For example, if u is a left-cancellative element of W (i.e., if $uw_1 = uw_2$ always implies $w_1 = w_2$), then u is projective. In fact if u is such an element of W, $M_W \overset{e_u}{\to} \dot{M}_W(u)$ is an isomorphism.

Hence in particular, if W is a group or a free monoid, or any left cancellative monoid, then the only monogenic projective automaton is M_W (up to an isomorphism, of course).

To be more general, if u is an element of W for which there is x in W such that $u = uxu$, then u is projective; set $j(u) = xu$. For example, if $u = u^n$ for some $n > 1$.

2.5 From the characterization of the projective elements in W given by Prop. 2.3.1, it follows that if u is projective then $j(u)$ is an idempotent of W:

$$uj(u) = u1_W, \quad \text{hence} \quad j(u)j(u) = j(u)\cdot 1_W \quad .$$

This observation yields the following complete characterization of the monogenic projective automata.

2.5.1 THEOREM: A monogenic automaton is projective iff it is isomorphic to a monogenic subautomaton of M_W generated by an idempotent of W.

Proof: The splitting sequence

$$M_W(u) \overset{j}{\to} M_W \overset{e_u}{\longrightarrow} M_W(u)$$

implies that $M_W(u) \overset{j}{\to} j(M_W(u))$ is an isomorphism. But obviously

$$j(M_W(u)) = M_W(j(u)) \quad .$$

2.5.2 REMARK: Thus, even though the class of the projective elements in W may be larger than the class of the idempotents of W, the latter class is sufficient for the characterization of the projective elements of W and of the projective monogenic automata.

2.6 The characterization of monogenic projective automata by means of splitting sequences through M_W yields Theorem 2.5.1 directly by considering the idempotents of $\mathrm{End}(M_W)$ as follows.

An automaton P is monogenic and projective iff it has a splitting sequence $P \overset{j}{\to} M_W \overset{e}{\to} P$ through M_W. Hence, if P is monogenic and projective, there exists an endomorphism $M_W \xrightarrow{je} M_W$ which is an idempotent of $End(M_W)$,

$$jeje = j(ej)e = je \quad ,$$

and P is isomorphic to $M_W(je(1_W))$. From the idempotence of je follows

$$je(1_W) = je(je(1_W)) = je(1_W)\ je(1_W) \quad ,$$

i.e., $je(1_W)$ is idempotent in W.

On the other hand, if $M_W \overset{\sigma}{\to} M_W$ is an idempotent endomorphism of M_W and $P = M_W(\sigma(1_W))$, then

$$P \overset{j}{\to} M_W \xrightarrow{\sigma'} P$$

for the inclusion morphism j and for

$$\sigma' : W \to \sigma(1_W)\ W : w \to \sigma(1_W)\cdot w = \sigma(w) \quad ,$$

is a splitting sequence of P through M_W.

The relationship between the idempotents of W and of $End(M_W)$ was established by the representation theorem for $\mathcal{A}_W$ (Give'on 1964) since W is isomorphic to $End(M_W)$.

3. THE CHARACTERIZATIONS OF M_W FOR A FINITE W

3.1 In our first paper in this series (Give'on 1964) we showed that if M_W can be identified (up to an isomorphism) by means of categorical predicates then $\mathcal{A}_W$ is categorically complete. There we succeeded to characterize M_W for the case where W is a unit-commutative monoid (i.e., where $w_1w_2 = 1_W$ always implies $w_1w_2 = w_2w_1$).

3.2 Our results in this paper enable us to characterize M_W for the case where W is any finite monoid. Thus one can hope to apply the categorical study of $\mathcal{A}_W$ to the theory of finite monoids.

3.2.1 THEOREM: If W is a finite monoid then an object X of $\mathcal{A}_W$ is isomorphic to M_W iff X satisfies the following two conditions:

(i) X is monogenic;

(ii) for any monogenic projective automaton P there exists a monic $P \overset{j}{\rightarrow} X$.

Proof: By our previous results we know that M_W satisfies these conditions. Assume now that X is an automaton which satisfies them as well.

Since X is monogenic there exists an epic $M_W \overset{e}{\rightarrow} X$ and therefore the cardinality of S_X is not larger than that of W. Since M_W is projective we have a monic $M_W \overset{j}{\rightarrow} X$ and therefore j is surjective and it determines an isomorphism of M_W and X.

3.2.2 <u>COROLLARY</u>: If W is finite then $\mathcal{A}_W$ is categorically complete.

BIBLIOGRAPHY

Give'on, Y., "Toward a Homological Algebra of Automata, I, II & III," Tech. Reports in process, ORA, The University of Michigan (1964-1965).