ALGEBRAIC STRUCTURE OF AUTOMATA

By

Arthur C. Fleck

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1964

ABSTRACT

ALGEBRAIC STRUCTURE OF AUTOMATA

by Arthur C. Fleck

In order to give a description of the contribution of the thesis under consideration it is necessary to sketch a brief history of this subject. For purposes of this discussion there are two natural reference points. These will be indicated in what follows and we will orient this discussion around them.

The first reference point which we indicate occurs in conjunction with the appearance of the papers of Huffman [1], Mealy [2] and Moore [3]. These were the pioneering works for the area of investigation under consideration here. Prior to the appearance of these papers the mathematical model of a computing device proposed by Turing [4] was widely studied. While this model is of considerable theoretical importance it was not directly applicable to the physical devices and associated problems which began to appear in the early 1950's. In order that the reader understand the full significance of the remarks to follow we will digress to indicate the essential properties of the Moore type model. However, we do this in the more precise and formal language of Ginsburg [5] rather than as it originally appeared. A <u>sequential machine</u>, C, is a quintuple, C = (S,I,O,M,N), where S (states) is a

finite nonempty set, I (inputs) and O (outputs) are (nonempty) semigroups, M is a (next state) function $M: S \times I \longrightarrow S$ such that $M(s,xy) = M(M(s,x),y)$ and N is a (output) function $N: S \times I \longrightarrow O$ such that $N(s,xy) = N(s,x) N(M(s,x),y)$. Briefly then, if a sequential machine is in a given state and an input is applied, an output and a transition to a new state occur. Notice that for two distinct elements $x,y \in I$, the same transitions may be defined by x and y but these inputs may still be distinguished by the output function. The main interest in such a model, as with Turing machines, is in its behavioral properties. That is in the properties of the (presumably observable) inputs and outputs. The reason for distinguishing the works mentioned above is the viewpoint taken by them. Besides establishing the definition of the model, the main concept thich is studied by these authors is that of (behavioral) equivalence of machines. Briefly, the meaning taken for equivalence here is that if two machines are presented with the same sequence of inputs they will produce the identical sequences of outputs (with approiate choices of states). The results of these authors concerning this concept consists of construction and investigation of reduction algorithms. That is, given a machine construct an equivalent machine in which the number of states is minimized. Thus the basic motivation here was the (behavioral) comparison of devices with the idea in mind of finding the 'simplest' device (behaviorally) equivalent to a given one. Investigation of these algorithms usually revolved about structure and uniqueness properties of the 'reduced' machine.

The second set of papers which will be singled out for reference are characterized by a basic change in approach to investigation of this model. Briefly we can class these investigations as efforts to solve questions of the general form, 'Given a device, what work can it do?' That is, how can the output behavior be influenced by choices of inputs and state? This viewpoint is perhaps best exemplified in the works of Rabin and Scott [6] and Ginsburg and Spanier [5],[7].

Before getting on to the job at hand several points should be made. First of all, there is little agreement on exactly how the output association should be defined. Thus each of the authors previously mentioned is in disagreement with the others on this point. In specific, the definition of sequential machine put forth earlier does not exactly agree with those of the mentioned authors but is what Ginsburg has termed a quasimachine [8] . The difference of detail sometimes produces subtle or unexpected results. For instance the uniqueness(of reduced machine) result of Moore ([3] , Theorem 4) requires strong connectedness while that of Ginsburg ([8] , Theorem 1.3) does not. On the other hand another classic ([6] , Theorem 15) shows, roughly speaking, that every two-way automaton is equivalent to a one-way automaton. Never the less a common ground is found in the way the internal transformations are treated. Thus an increase in knowledge in this area should be of general value.

We will now indicate how the results of this thesis relate to these earlier investigations. In Part I the following is accomplished: (1) the basic definitions, including that of the model, are introduced and their interrelations noted (2) the concepts of open set and continuous function are investigated.

In regards to (1) it is clear that a work which studies the relationship of structure to algebraic properties and as function invariants must make a perfunctory mention of the structures to be discussed and their interrelationships. We will concentrate therefore on a discussion of the model. As indicated earlier, it is the belief that a better understanding of structure properties will aid in analysis of behavioral problems which motivated the model here. Apart from this consideration, the model here presents a rich mathematical system. As to particulars, in the definition the semigroup of inputs is assumed to have an existance apart from the automaton in which it is imbedded. Two distinct inputs are not identified because they define the same operator on the set of states. It is clear that this cannot be done if one hopes to make use of this analysis in a system where such inputs may be distinguished by the outputs which they cause. Also, from a mathematical point of view, this is not an unusual consideration. On this point, there is a direct analogy to the definition of a group with operators [9] .

While, due to special restrictions, the concept of open set produces an uninteresting topology, it serves two useful purposes. First, it eliminates the previous dependence of the definition of connectedness on an associated graph. Second, it naturally suggests the investigation of continuous functions in this setting. It can be observed that all of the reduction algorithms mentioned earlier can be thought of as defining a function from one machine to another. While these different algorithms were produced for different models, the transition (structure) was uniform. Thus the study of structure invariants of (continuous) functions provides a generalized and uniform treatment for several previously seperated results and partial results (see, for example, [3] , [8] , [10]). This general investigation was carried out without the usual assumption of the so called 'sequential' property. However, the force of this property was found to be necessary in the results on structure invariants of functions.

The remainder of this thesis has a less direct bearing on existing results. The remarks made above concerning the model are all that will be made in this regard. The techniques applied here are familiar. In several cases the problems attacked are analogous to problems in other disciplines, while in general the methods of solution are not.

In Part II a class of functions analogous to the homomorphisms is introduced. After a brief investigation of the structure invariants of these functions, we are lead to what may be thought of as the automorphism group of an automaton. The motivation is then to find the relationships that exist between the properties of the group and those of the automaton. In this investigation the frequency of the necessity of the force of the sequential property is sufficient to impel this assumption. Then, in certain cases, we are able to identify the action of the inputs with that of the group elements. This shows, to some extent, how the structures considered restrict the actions of the inputs. Roughly, this is similiar to determining inner automorphisms, but there is no direct connection. The main results here indicate under what circumstances a complete or partial description of the automorphism group can be so obtained. At this point another semigroup is introduced by means of a natural equivalence relation on the inputs. This semigroup seems to reflect the structure of both the input semigroup and the automaton, and hence its automorphism group, in rather subtle ways. We show here a reflection of the automorphisms in this semigroup.

In Part III a particular structure, that of the direct product, is investigated. This structure, as presented here, was introduced by Rabin and Scott [6] in their study of acceptable sets of tapes. However, the problem of producing sufficient conditions for realising this structure has not been considered. Perhaps this is because it is not yet clear how to incorporate this concept in a model with outputs. At any rate this is a worthwhile problem to which a reasonable contribution is made by means of the devices introduced earlier. The main results give, in one case, necessary and sufficient conditions and, in another, sufficient conditions for the presence of the structure.

Arthur C. Fleck

LIST OF REFERENCES (ABSTRACT)

1. Huffman,D. A., "The synthesis of sequential switching circuits", Jour. Franklin Inst., 257,1954.

2. Mealy, G. H., "A method for synthesizing sequential circuits", Bell Systems Tech. Jour., Vol. 34, 1955.

3. Moore, E. F., "Gedanken experiments on sequential machines", Automata Studies, Princeton, 1956.

4. Turing, A. M., "On computable numbers with an application to the entscheidungs problem", Proc. London Math. Soc., Vol. 41, 1936.

5. Ginsburg, S., "Some remarks on abstract machines", Trans. Amer. Math. Soc., 96, 1960.

6. Rabin, M. O. and D. Scott, "Finite automata and their decision problems", IBM Jour. of Res. and Dev., Vol. 3, 1959.

7. Ginsburg, S. and E. H. Spanier, "Distinguishability of a semigroup by a machine", Proc. Amer. Math. Soc., 12, 1961.

8. Ginsburg, S., An Introduction to Mathematical Machine Theory, Addison-Wesley Pub. Co., 1962.

9. Jacobson, N., Lectures in Abstract Algebra, Van Nostrand Co., 1951.

10. Ginsburg, S., "Connective properties preserved in minimal state machines", Jour. Assoc. Computing Mach., 7, 1960.

ACKNOWLEDGEMENTS

The author is indebted to G. P. Weeg for his direction, encouragement and enthusiasm as regards this thesis. Perhaps, since it affects the whole of this dissertation, it should be mentioned that the idea for the model taken here is due to him.

The author also wishes to acknowledge his appreciation to the Division of Engineering Research of Michigan State University since a considerable portion of this research was conducted under its support.

TABLE OF CONTENTS

List of Tables

List of Figures

INTRODUCTION

While this work studies an abstract algebraic system, the character of this system obligates us to make a brief historical mention of mathematical models for computing devices. The most notable such model is that of A. M. Turing[1]. Although Turing's model is a useful theoretical concept, it is perhaps of no practical value. This fact has caused another model, the so called 'sequential machine', recently to become the object of a considerable amount of study. Early investigations of this model were directed toward its application to computer design. Prominent among these investigations are papers by Mealy[2], Moore[3] and Ginsburg[4]. Studies of more abstract properties of this model then followed from Rabin and Scott[5], Ginsburg[6], Weeg[7] and others.

The sequential machine model includes two essentially distinct components. The first is that of 'inputs' and internal transformation; the second is that of 'output'. The object in what follows is to study the structure (internal transformation) of such systems in isolation. Thus the model here contains no reference to the concept of output and, as is usual in this case, the term automaton is applied. We first ascertain restrictions on functions on automata which indicate two general classes of functions with desirable structure properties as invariants. This leads to the association of several algebraic entities with each automaton. At the core of the work are the results which relate the structures of these algebraic systems to the structure of the automaton itself.

The following results are dealt with in three parts. In Part I some structures and their interrelationships are introduced. The invariance of these structures under continuous functions is then examined. We are able to show that the class of continuous functions is the largest class under which the strongly connected property is invariant.

In Part II we examine the properties of operation preserving functions which play a role analagous to homomorphisms in the usual algebraic studies. This leads to the association of an 'automorphism' group with each automaton and finally a characterization of the input semigroup. The relationships between the structures of these systems and those of the automaton itself are then investigated. For the class of perfect automata a description of the group and semigroup is given.

In Part III we seek structure conditions on the automaton and its associated algebraic systems which will insure its representation as a direct product. For the class of perfect automata we are able to give a complete solution and for the class of strongly connected automata, a partial solution.

PART I

STRUCTURE PRESERVING PROPERTIES OF CONTINUOUS FUNCTIONS

Introductory Concepts

Most of the results of Part I concerning the interrelations of structures on automata follow easily. However to pursue a discussion of structure preserving properties of functions it is necessary to have these structures and their interactions formally set down. The bearing of the open set concept on structure is also evident. However, the open set concept leads to an interesting new property to require of functions. Judging from the results concerning these (continuous) functions and the manner in which they are obtained, continuity defined by the open set concept is both a worthwhile and natural concept. Many of these results (some of which were reported in[8]) are both surprising and apparent.

The definition of an automaton taken here parallels that of Rabin and Scott [5] and more exactly that of Ginsburg[6] (except for outputs). Occasionally a display of a weighted, directed graph (state or transition diagram) will be used but only to specify an example. The explanation of this device is delayed until that time.

Definition 1.1. An automaton, A = (S, I, M) is a triple where S is a non-empty set (the set of states), I is a non-empty semigroup (the set of inputs), M is a function (the next state function) taking S x I (Cartesian product) into S.

It should be pointed out that while such models historically arose to study sequential switching circuits, the model here allows far greater applicability. For instance we could consider S (together with an operation) to be a group and I to be the semigroup of endomorphisms (or group of automorphisms) of S. Another interesting specialization occurs when $S = \{1, 2, \cdots, n\}$ and I is taken as a subgroup of S_n (the symmetric group). Finally we might identify S and I and consider that M defines a binary operation on this set. It is frequently interesting to apply one or more of these specializations to what follows but this will be left to the reader.

For completeness it should be noted that the system described by Definition 1.1 can be considered as a set together with a semigroup of operators on the set. However, this view point will not be taken in what follows.

We now examine some structure properties (i.e. properties of the next state function) of automata. Many of the structures defined below are discussed briefly in the literature but in most cases the properties have never been formally set down and their interrelations examined.

Definition 1.2. A set of states, $T \subset S$, of an automaton A = (S, I, M) is <u>open</u> if given any $s \in T$ and any $x \in I$, $M(s,x) \in T$.

Such a set is defined elsewhere in the literature as a stable set [6] or a submachine, but the term "open" is used here due to the topological nature and interpretation of the definitions and results to follow.

Lemma 1.1. The union of arbitrarily many open sets of states of an automaton A = (S,I,M) is an open set of states of A.

Lemma 1.2. The intersection of arbitrarily many open sets of states of an automaton A = (S,I,M) is an open set of states of A.

Lemmas 1.1 and 1.2 follow from a direct application of the definitions. Thus, as suggested by the terminology, we have

Proposition 1.1. For any automaton A = (S,I,M) the collection of open sets of states of A yields a topology on S, the set of states.

Proof: Obviously the null set, ϕ , and the set S are open. This together with Lemmas 1.1 and 1.2 establishes a topology [9].

We apply the term proposition here, and in what follows, to a more or less self contained result which is of somewhat lesser importance.

In the light of Lemma 1.2 it is not anticipated that topological structures will be of interest here. Our investigation is rather oriented toward automata structures.

Definition 1.3. An automaton A = (S,I,M) is <u>sequential</u> if M(s,xy) = M(M(s,x),y) for all $s \in S$ and $x,y \in I$.

It should be noted that under the definition of an automaton by Rabin and Scott[5] (and similar considerations due to Moore[3], etc.) where the input composition is taken to be juxtaposition, the next state function is usually defined on a set of generators and then extended to the entire (free) semigroup by means of the relation in Definition 1.3. Thus a "finite automaton" is usually considered to be sequential by definition. Definition 1.3 deserves one more comment. It will be seen that not only is sequentialness a natural concept, but for many of the results of this section it is indeed necessary.

Definition 1.4. An automaton $A = (S,I,M)$ is strongly connected if given any s_1, $s_2 \in S$, there exists an $x \in I$ such that $M(s_1,x) = s_2$.

In this context, the concept of strongly connectedness was first defined and investigated by Moore [3].

Proposition 1.2. If an automaton $A = (S,I,M)$ is strongly connected, then there is no proper open subset of S.

Proof: Assume $U \subset S$ is a proper open subset. Then $S - U \neq \phi$. If $s_1 \in U$ and $s_2 \in S - U$, then $M(s_1,x) \in U$ for all $x \in I$.since U is open. But $s_2 \notin U$, hence $M(s_1,x) \neq s_2$ for all $x \in I$. Thus A is not strongly connected, a contradiction. Hence there is no proper open subset of S.

Lemma 1.3. If an automaton $A = (S,I,M)$ is sequential, then for each $s \in S$, $T_s = \{s_1 | s_1 \in S, M(s,x) = s_1\}$(i.e., the set of all s_1 such that $M(s,x) = s_1$ for some $x \in I$) is an open set.

Proof: Assume T_s is not open. Then there exists $s_1 \in T_s$ and $x \in I$ such that $M(s_1,x) = s_2 \notin T_s$. Now since $s_1 \in T_s$, $s_1 = M(s,y)$ for some $y \in I$. But then $M(s,yx) = M(M(s,y),x) = M(s_1,x) = s_2 \in T_s$, a contradiction. Thus T_s is open.

Theorem 1.3. If $A = (S,I,M)$ is a sequential automaton with no proper open subset of S, then A is strongly connected.

Proof: Assume A is not strongly connected. Then there exist s_1, $s_2 \in S$ such that $M(s_1,x) \neq s_2$ for all $x \in I$. Now by Lemma 1.3, $T_{s_1} = \{s | s \in S, M(s_1,x) = s\}$ is open. But $s_2 \notin T_{s_1}$. Hence T_{s_1} is a proper open subset (T_{s_1} is not empty since I is not empty), a contradiction. Thus A is strongly connected.

Two remarks are appropriate at this point: first, Proposition 1.2 and Theorem 1.3 can be stated as a necessary and sufficient condition for strongly connectedness when the definition of an automaton assumes the property of sequentialness [6]. However, for our purposes it will be necessary to use Proposition 1.2 without the sequential property. Second, Theorem 1.3 and Lemma 1.3 are false if the sequential property is omitted as can be seen by the following example.

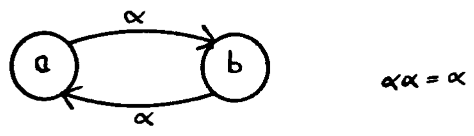

Figure 1

The device used to specify the automaton of Figure 1 is called a state (or transition) diagram. Its meaning is: the set of states, $S = \{a,b\}$, is the set of vertices of the graph; the set of inputs, $I = \{\alpha\}$, is the set of weights of the directed edges; the next state function, $M(a,\alpha)=b$, $M(b,\alpha) = a$, is specified by the directed edges and their weights; the input combination is specified in the margin (if not understood).

Notice that the automaton Figure 1 is not strongly connected, but there is no proper open subset of states. This is possible since the property of sequentialness is not present. Also T_a is not open, so that sequentialness is needed for Lemma 1.3.

Definition 1.5. An automaton $A = (S,I,M)$ is <u>triangular</u> if given any s_1, $s_2 \in S$, there exists $x,y \in I$ and $s \in S$ such that $M(s_1,x) = s = M(s_2,y)$.

Definition 1.6. An automaton $A = (S,I,M)$ is <u>separated</u> if there exist non-void, open sets $U,V \subset S$ such that $U \cup V = S$ and $U \cap V = \phi$; otherwise A is <u>connected</u>.

We mention that an automaton is connected if and only if its state diagram constitutes a connected graph. The open set concept seems to be the simplest way to put forth this concept.

Proposition 1.4. If an automaton $A = (S,I,M)$ is triangular, then A is connected.

Proof: Assume A is not connected. Then there exist non-void, open $U, V \subset S$ such that $U \cup V = S$ and $U \cap V = \phi$. Now let $s_1 \in U$ and $s_2 \in V$. Then since A is triangular there exist $x,y \in I$ and $s \in S$ such that $M(s_1,x) = s = M(s_2,y)$. But then $s \in U$ and $s \in V$ for the desired contradiction. Thus A is connected.

We now introduce one more structure concept and conclude the discussion of the interrelations arising.

Definition 1.7. An automaton $A = (S,I,M)$ is <u>reversible</u> if whenever there exists an $x \in I$ such that $M(s_1,x) = s_2$, then there exists a $y \in I$ such that $M(s_2,y) = s_1$, where s_1, $s_2 \in S$.

This concept resembles closely that of strongly connectedness except that it is not assumed that a transition exists between every pair of states. However, we have the following:

Theorem 1.5. If $A = (S,I,M)$ is a sequential automaton, then a necessary and sufficient condition that A be strongly connected is that A be connected and reversible.

Proof: (Sufficiency)

Suppose that A is not strongly connected. Then there exist s_1, $s_2 \in S$ such that $M(s_1,x) \neq s_2$ for all $x \in I$. Now by Lemma 1.3 $T_{s_1} = \{s | s \in S, M(s_1,x) = s\}$ is open.

But since A is reversible $S - T_{s_1}$ is also open. For suppose there exists $s \in (S - T_{s_1})$ such that $M(s,z) = t \in T_{s_1}$ for some $z \in I$. Then by reversibility there exists $w \in I$ such that $M(t,w) = s$. But then T_{s_1} is not open, a contradiction. Now T_{s_1} and $S - T_{s_1}$ are both open and T_{s_1} is not empty since I is not empty. Also $s_2 \in (S - T_{s_1})$ so $S - T_{s_1}$ is not empty. But we have $T_{s_1} \cup (S - T_{s_1}) = S$ and $T_{s_1} \cap (S - T_{s_1}) = \phi$. Thus A is not connected, a contradiction. Thus A is strongly connected.

The necessity of the condition is entirely obvious in the light of Proposition 1.2 and follows without the sequential property.

Corollary 1.5.1. If $A = (S,I,M)$ is a sequential automaton, then a necessary and sufficient condition that A be strongly connected is that A be triangular and reversible.

Proof: Apply Proposition 1.4, Theorem 1.5 and the definitions.

Corollary 1.5.2. If $A = (S,I,M)$ is a sequential, reversible automaton, then the complement of every open set is open.

Proof: The proof of this fact is essentially the proof given in Theorem 1.5 to show T_{s_1} being open implies $S - T_{s_1}$ is open.

Also as was pointed out by R. Brown, if A is sequential and the complement of every open set is open, then A is reversible. It is also interesting to note that sequentialness cannot be removed from the hypotheses of Theorem 1.5 for Figure 1 provides a counterexample in this case.

Continuous Functions

In this section the structure invariants of transformations on automata are studied. In particular the concept of a continuous function of one automaton into another is defined and its structure preserving properties studied.

Definition 1.8. For two automata, $A = (S,I,M)$ and $B = (T,J,N)$, by function, h, of A into B, written $h:A \rightarrow B$, is meant a function of S into T.

That is a function on an automaton is merely a function on its set of states. For h, A and B as in Definition 1.8, the following usual notation will be used: by the image, $h(X)$, of a set $X \subset S$ under h is meant the set $h(X) = \{t \mid h(x) = t, x \in X\}$ and by inverse image $h^{-1}(Y)$, of a set $Y \subset T$ is meant the set $h^{-1}(Y) = \{s \mid s \in S, h(s) \in Y\}$.

Definition 1.9. A function $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,J,N)$, is continuous if for any open $Y \subset T$, $h^{-1}(Y) \subset S$ is open.

The term continuous is chosen since Definition 1.9 is precisely the topological definition of a continuous function when A and B are topological spaces [9].

Theorem 1.6. Let $A = (S,I,M)$ be a strongly connected automaton and $B = (T,J,N)$ be a sequential automaton. Then if $h:A \longrightarrow B$ is a continuous, onto function, B is strongly connected.

Proof: Assume B is not strongly connected. Then there exist $t_1,t_2 \in T$ such that $N(t_1,x) \neq t_2$ for all $x \in J$. Now by Lemma 1.3 $T_{t_1} = \{t | t \in T, N(t_1,x) = t\}$ is an open set. Then since h is continuous $h^{-1}(T_{t_1}) \subset S$ is open. Then by Proposition 1.2, $h^{-1}(T_{t_1}) = S$, since A is strongly connected. Thus we have $h(S) = T_{t_1}$ and $t_2 \notin T_{t_1}$. But h was assumed to be onto, a contradiction. Hence B is strongly connected.

Before the next theorem is stated we must make reference to the following well-known set equality which holds for functions in general: Let $f:S \longrightarrow T$ be a function. Then the following statement holds

$$(1)\ f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B);\ A,\ B \subset T.$$

Theorem 1.7. Let $A = (S,I,M)$ be a triangular automaton and $B = (T,J,N)$ be a sequential automaton. Then if $h:A \longrightarrow B$ is a continuous, onto function, B is triangular.

Proof: Assume B is not triangular. Then there exists $t_1,t_2 \in T$ such that $N(t_1,x) \neq N(t_2,y)$ for all $x,y \in J$. Certainly $t_1 \neq t_2$ or else $N(t_1,x) = N(t_2,x)$ for all $x \in I$. Now by Lemma 1.3 the sets $T_{t_1} = \{t | N(t_1,x) = t\}$ and $T_{t_2} = \{t | N(t_2,x) = t\}$ are open and $T_{t_1} \cap T_{t_2} = \phi$. Now by Statement (1)

$$\begin{aligned} \phi &= h^{-1}(\phi) = h^{-1}(T_{t_1} \cap T_{t_2}) \\ &= h^{-1}(T_{t_1}) \cap h^{-1}(T_{t_2}). \end{aligned}$$

Let $T_1 = h^{-1}(T_{t_1})$ and $T_2 = h^{-1}(T_{t_2})$. Then we have $T_1 \cap T_2 = \phi$. Also since h is continuous T_1 and T_2 are open sets. Now T_{t_1} and T_{t_2} are not empty, since J is not empty. Also h is onto so T_1 and T_2 are not empty. Let $s_1 \in T_1$ and $s_2 \in T_2$. Then since A is triangular, there exist $s \in S$ and $w, z \in I$ such that $M(s_1, w) = s = M(s_2, z)$. Now either $s \in T_1$, $s \in T_2$ or $s \in (S -(T_1 \quad T_2))$. In the first case T_2 is not open, in the second T_1 is not open and in the last case neither T_1 nor T_2 is open, a contradiction in any circumstance. Thus B is triangular.

Proposition 1.8. Let A = (S,I,M) and B = (T,J,N) be two automata and let A be connected. Then if $h: A \longrightarrow B$ is a continuous, onto function, B is connected.

Proof: No proof of this theorem need be given here since all the concepts involved are topological in nature and the topological counterpart of this theorem is valid.

Theorem 1.9. If A = (S,I,M) is a strongly connected automaton and h is any function onto A, then h is continuous.

The proof of Theorem 1.9 is trivial in the light of Proposition 1.2 but we have the following interesting corollary

Corollary 1.9.1. If h is any function of one automaton onto another which preserves strongly connectedness, then h is continuous.

Thus we have that the set of all functions on automata which preserve strongly connectedness is contained in the set of all onto, continuous functions. Moreover if we combine Corollary 1.9.1 with Theorem 1.6 we can make the following important and desirable statement: For the set of all sequential automata, a necessary and sufficient condition that a function preserve strongly connectedness is that it be continuous.

We have seen that continuous functions on automata have several desirable structure preserving properties. We also point out that for almost all the results where a continuous function preserves a structure it is necessary to the proof that the image automaton be sequential. It is easy to construct examples which show that with this restriction removed those theorems are in fact false. For instance, any function from a strongly connected (in fact any) automaton onto the automaton of Figure 1 is necessarily continuous. However, recall that this automaton is not strongly connected. Also if our ideas were extended to models with outputs, both the reduction processes of Mealy [2] and Moore [3] would be continuous.

To conclude this section, we state an example which shows that the reversible property is not necessarily preserved by continuous functions.

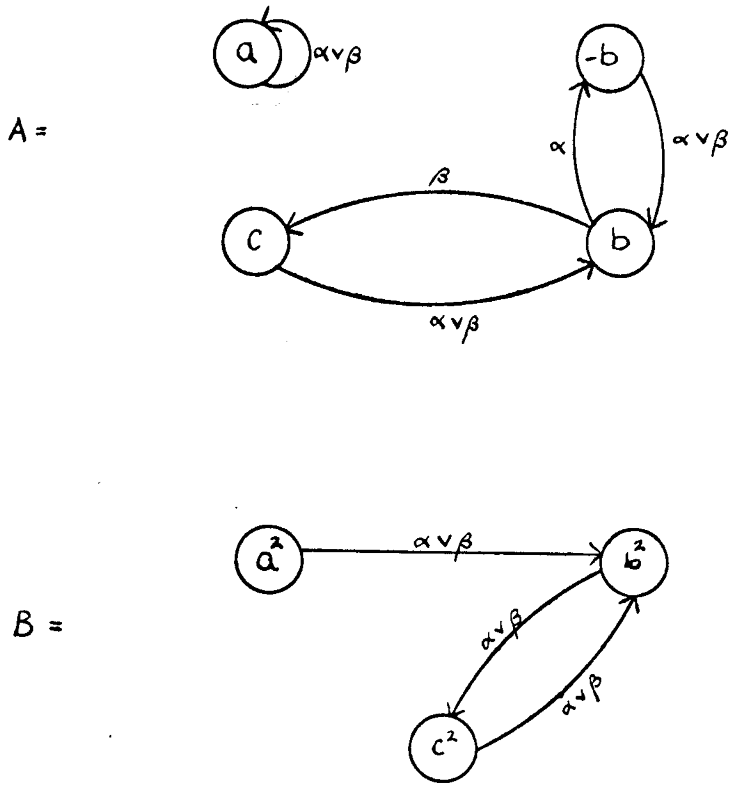

Figure 2

In figure 2 the input composition is the usual juxtaposition (generators α, β) in both cases and the sequential property is assumed for products of generators in both A and B. Of course the transitions are not completely labeled and not all transitions are depicted. For instance in A, $M(-b,\beta\alpha) = -b$ and in B, $M(a^2,\alpha\alpha) = c^2$.

Now we define $h:A \longrightarrow B$ by $h(x) = x^2$ for $x \in \{a,b, -b,c\}$. Then it is easily checked that h is continuous and onto. However, A is reversible but B is not.

PART II

THE GROUP AND SEMI-GROUP OF AN AUTOMATON

Operation Preserving Functions

In this section we leave the general concept of continuous functions on automata and introduce a more specialized class of functions, the class of operation preserving functions on automata, and investigate its properties. In this part, the restriction put on the functions studied is algebraic, rather than topological, in nature. The discussion thus leads to the association of a group with each automaton. Some investigation is then given to the relationship between the structure of an automaton and the structure of its group. This investigation leads us to the concept of a perfect automaton. We are then able to give a description of the group for a perfect automaton and this in turn leads to a convenient method for the calculation of the group of an automaton in this class. The association of a group with an automaton seems to be an extremely helpful(and perhaps necessary) device in some studies of automata (see Part III).

Definition 2.1. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$, satisfies $h[M(s,x)] = N(h(s),x)$ for all $s \in S$ and $x \in I$, then h is operation preserving. If h is also one-to-one and onto, we say h is an isomorphism.

A concept similar to this, but for machines with outputs, has been briefly discussed by Ginsburg [6].

We notice that Definition 2.1 applies only when A and B have semigroups of inputs which are identified. This restriction could be removed by establishing a correspondence between the input set of A and the input set of B (if they were different), but this complicates the discussion unnecessarily while yielding no significant refinement in the results.

Proposition 2.1. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$, is operation preserving, then h is continuous.

Proof: Let $T_1 \subset T$ be open and let $s_1 \in h^{-1}(T_1) \subset S$. Then for each $x \in I$ consider $s_2 = M(s_1,x)$. $h(s_2) = h\left[M(s_1,x)\right] = N\left[h(s_1),x\right] = t_1$. Now since $h(s_1) \in T_1$ and T_1 is open, $h(s_2) = t_1 \in T_1$. But then $s_2 \in h^{-1}(T_1)$ and thus $h^{-1}(T_1)$ is open and h is continuous.

Proposition 2.1 shows that the class of all operation preserving functions is a subclass of the class of continuous functions, possessing therefore all the properties developed for continuous functions.

The following three results show that operation preserving functions have a much stronger structure preserving nature than continuous functions. In particular, Propositions 2.2 and 2.3 show that the restriction of sequentialness can be removed from the image machine for operation preserving functions and Proposition 2.4 shows that reversibility is preserved by operation preserving functions.

Proposition 2.2. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$, is an operation preserving, onto function and

A is triangular, then B is triangular.

Proof: Let $t_1, t_2 \in T$. Then since h is onto there exists $s_1, s_2 \in S$ such that $h(s_1) = t_1$ and $h(s_2) = t_2$. Now since A is triangular there exists $x, y \in I$ and $s \in S$ such that $M(s_1, x) = s = M(s_2, y)$. But then $h[M(s_1,x)] = N(h(s_1),x) = N(t_1,x) = h(s) = h[M(s_2,y)] = N(h(s_2),y) = N(t_2,y)$. Hence B is triangular.

Proposition 2.3. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$, is an onto, operation preserving function and A is strongly connected, then B is strongly connected.

Proof: Let $t_1, t_2 \in T$. Then since h is onto there exists $s_1, s_2 \in S$ such that $h(s_1) = t_1$ and $h(s_2) = t_2$. Since A is strongly connected there exists $x \in I$ such that $M(s_1,x) = s_2$, hence $N(t_1,x) = t_2$ and B is strongly connected.

Proposition 2.4. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$ is an onto, operation preserving function and A is reversible, then B is reversible.

Proof: Let $t_1, t_2 \in T$ such that $N(t_1,x) = t_2$ for some $x \in I$. Then since h is onto there exists $s_1 \in S$ such that $h(s_1) = t_1$. But then for $s_2 = M(s_1,x)$, $h(s_2) = h[M(s_1,x)] = N(h(s_1),x) = N(t_1,x) = t_2$. Thus $h(s_2) = t_2$. Now A is reversible so there exists $y \in I$ such that $M(s_2,y) = s_1$ and then $t_1 = h(s_1) = h[M(s_2,y)] = N(h(s_2),y) = N(t_2,y)$. Thus B is reversible.

In view of the example in Figure 2 and Theorems 1.6 and 1.7 we see that operation preserving functions have a much stronger structure preserving nature than continuous functions. This idea is further emphasized by the following proposition which has no counterpart for continuous functions.

Proposition 2.5. If $h:A \longrightarrow B$, where $A = (S,I,M)$ and $B = (T,I,N)$, is an onto, operation preserving function and A is sequential, then B is sequential.

Proof: Since h is onto, for each $t \in T$ there exists $s \in S$ such that $h(s) = t$. Then

$$\begin{aligned} N(t,xy) &= N(h(s),xy) = h[M(s,xy)] \\ &= h[M(M(s,x),y)] = N(h[M(s,x)],y) \\ &= N(N(h(s),x),y) = N(N(t,x),y) \end{aligned}$$

since h is operation preserving and A is sequential. Thus B is sequential.

It is interesting to notice that Proposition 2.5 is not true if the input compositions are distinct. The example below shows an operation preserving function carrying a sequential automaton onto a non-sequential automaton. Notice that the only thing that distinguishes the two automata is the input composition.

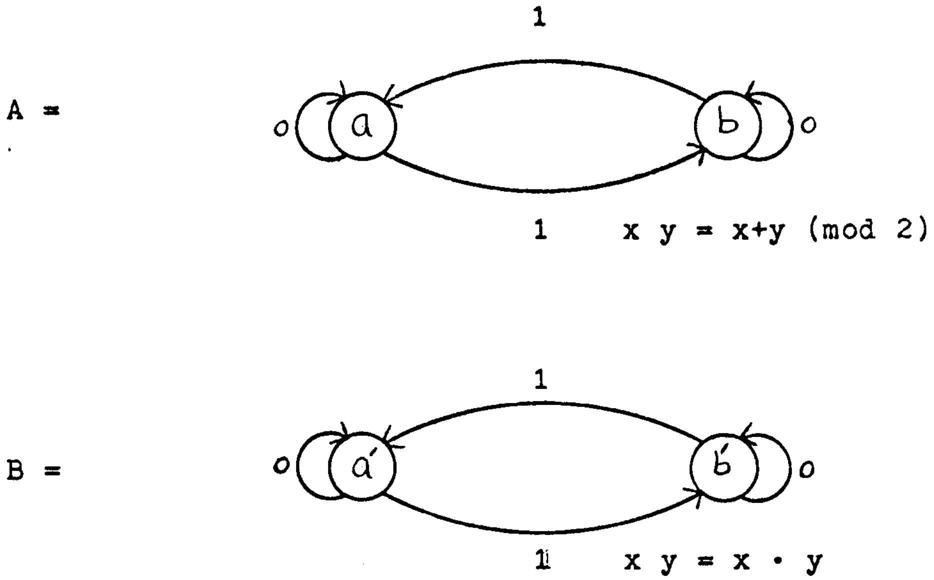

Figure 3

In Figure 3 define h(x) by h(x) = x' for x $\in \{a,b\}$ and h is operation preserving.

The Group of an Automaton

For the remainder of this thesis it will be assumed that all automata under consideration are sequential. Many of the results of the next few sections were indicated in [10].

Proposition 2.6. The set of all functions $h:A \longrightarrow A$, where A = (S,I,M), which are one-to-one, onto and operation preserving form a group.

Proof: The only group property which warrants attention is showing that the system contains inverses. Let $h:A \longrightarrow A$ be one-to-one, onto and operation preserving. Then $h^{-1}:A \longrightarrow A$ defined by $h^{-1}(x) = y$ if and only if $h(y) = x$ is one-to-one and onto and $hh^{-1}(s) = h^{-1}h(s)$

$= s = i(s)$. Now let $M(s,x) = s_1$ and $M(h^{-1}(s),x) = s_2$. Then $h(s_2) = h[M(h^{-1}(s),x)] = M(h\ h^{-1}(s),x) = M(s,x) = s_1$. Thus $h^{-1}(s_1) = s_2$ so that $h^{-1}[M(s,x)] = h^{-1}(s_1) = s_2 = M(h^{-1}(s),x)$. So h^{-1} is also operation preserving and the system is clearly a group.

Proposition 2.6 is an interesting result in that it associates with each automaton a group. In this connection we make

Definition 2.2. For each automaton $A = (S,I,M)$ we denote by $G(A)$ the group associated with it by Proposition 2.6.

The general development to be followed now is suggested by the question: What relationships exist relating the structure of the automaton to the structure of the group associated with it?

Lemma 2.1. If $A = (S,I,M)$ is a strongly connected automaton and h_1, $h_2 : A \longrightarrow A$ are operation preserving with $h_1(s_0) = h_2\ (s_0)$ for some $s_0 \in S$, then $h_1 \equiv h_2$ (i.e., $h_1(s) = h_2(s)$ for all $s \in S$).

Proof: Suppose that h_1 and h_2 are functions satisfying the hypothesis of the lemma and let $s \in S$ be an arbitrary state. Then since A is strongly connected, there exists an $x \in I$ so that $M(s_0,x) = s$. Then $h_1(s) = h_1[M(s_0,x)] = M(h_1(s_0),x) = M(h_2(s_0),x) = h_2[M(s_0,x)] = h_2(s)$. Thus $h_1 \equiv h_2$.

Thus, if A is strongly connected and $h \in G(A)$, h has no fixed points unless h is the identity. Hence G(A) is a group of regular permutations. It follows from this, as pointed out by Weeg [11], that if A has a finite number of states, the order of G(A) divides that number.

Theorem 2.7. If $A = (S,I,M)$ is a strongly connected automaton, then $K[G(A)] \leq K[S]$, where $K[X]$ denotes the cardinality of the set X.

Proof: Assume $K[G(A)] > K[S]$ and let $s_0 \in S$ be any fixed state. Consider the set of states $\{h(s_0)\}$ where h ranges over all of G(A). Since $K[G(A)] > K[S]$, there must be distinct h_1, $h_2 \in G(A)$ so that $h_1(s_0) = h_2(s_0)$ for otherwise there is a one-to-one correspondence between G(A) and a subset of S (i.e., $h \longleftrightarrow h(s_0)$). But then by Lemma 2.1, $h_1 \equiv h_2$, a contradiction since h_1 and h_2 were assumed to be distinct. Thus $K[G(A)] \leq K[S]$.

Representation of the Group Elements

The following results arise from the fact that a group is associated with each automaton. Now each element of the group of an automaton is a function from its set of states to its set of states. If we restrict the next state function to a single input symbol this is precisely the manner in which it maps. With this motivation in mind we now state the question to be answered here: when can the elements of the group of an automaton be expressed in terms of its next state function? To resolve this question we introduce, and give some investigation to, one new concept.

Definition 2.3. Let $A = (S,I,M)$ be an automaton and $h:A \longrightarrow A$. Then h is representable if there exists an $x \in I$ such that $h(s) \equiv M(s,x)$ and $h_x(s) \equiv M(s,x)$ is a representation.

Definition 2.4. Let $A = (S,I,M)$ be an automaton. The middle, $\mathcal{M}$, of I is the set of all $x \in I$ such that $M(s,xy) = M(s,yx)$ for all $y \in I$ and $s \in S$.

Notice that the center of I is contained in the middle and $\mathcal{M}$ is a subsemigroup of I.

Definition 2.5. Let $A = (S,I,M)$ be an automaton. Then A is abelian if $I = \mathcal{M}$ (the middle). Also if A is strongly connected, A is called perfect.

Proposition 2.8. If $A = (S,I,M)$ and $B = (T,I,N)$ are automata and $h:A \longrightarrow B$ is operation preserving and onto, then $\mathcal{M}_A \subset \mathcal{M}_B$, where $\mathcal{M}_A$ and $\mathcal{M}_B$ are the middles for A and B respectively.

Proof: Let $x \in \mathcal{M}_A$, $t \in T$ and $y \in I$, then there exists an $s \in S$ such that $h(s)=t$ and

$N(t,xy)=N(h(s),xy)=h[M(s,xy)]=h[M(s,yx)]=N(h(s),yx)=N(t,yx)$

so $x \in \mathcal{M}_B$ since t and y were arbitrary.

Corollary 2.8.1. If $h:A \longrightarrow B$ is operation preserving and A is abelian, then B is abelian.

The next result shows that for a strongly connected automaton, we can determine if an input is in the middle by the way it acts on a single state.

Proposition 2.9. Let $A = (S,I,M)$ be a strongly connected automaton. Then if $M(s_0,xy)=M(s_0,yx)$ for some $s_0 \in S$ and all $y \in I$, x is in the middle of I.

Proof: Let $s \in S$. Then there exists $z \in I$ such that $M(s_0,z)=s$ and then $M(s,xy)=M(M(s_0,z),xy)=M(s_0,z(xy))=$ $M(s_0,(zx)y)=M(M(s_0,zx),y)=M(M(s_0,xz),y)=M(s_0,(xz)y)=$ $M(s_0,x(zy))=M(s_0,(zy)x)=M(s_0,z(yx))=M(M(s_0,z),yx)=M(s,yx)$. Thus x is in the middle.

The next several results will show when a representation of group elements is possible.

Lemma 2.2. Let $A = (S,I,M)$ be an automaton. Then the representation $h_x(s)=M(s,x)$ is operation preserving if and only if $x \in \mathcal{M}$, the middle.

Proof: Assume $x \in \mathcal{M}$. Then $h_x[M(s,y)]=M(M(s,y),x)=$ $M(s,yx)=M(s,xy)=M(M(s,x),y)=M(h_x(s),y)$. So h_x is operation preserving.

Now assume that h_x is operation preserving. Then $h_x[M(s,y)]=M(h_x(s),y)$ or $M(M(s,y),x)=M(s,yx)=M(M(s,x),y)=$ $M(s,xy)$ so $x \in \mathcal{M}$.

Lemma 2.3. Let $A = (S,I,M)$ be a strongly connected automaton and $x \in \mathcal{M}$, the middle. Then the representation h_x is onto.

Proof: Let $s,t \in S$. Then since A is strongly connected there exists $y \in I$ such that $M(M(s,x),y)=t$. Then $t=M(M(s,x),y)=M(s,xy)=M(s,yx)=M(M(s,y),x)=h_x[M(s,y)]$. Thus h_x is onto.

Theorem 2.10. Let $A =(S,I,M)$ be a strongly connected automaton with n states. Then each representation by an element of the middle is in G(A) and the set of all such elements constitutes a subgroup of the center of G(A).

Proof: The burden of the proof is supplied by Lemma 2.3. Since for $x \in \mathfrak{M}$, h_x maps S onto S and since S is finite, h_x is also one-to-one. But by Lemma 2.2, h_x is operation preserving and so $h_x \in G(A)$. Also for $x,y \in \mathfrak{M}$, $h_x h_y = h_{xy}$ and $xy \in \mathfrak{M}$. Thus the set of representations by elements of the middle is a closed subset of a finite group and hence is a subgroup. Also for $g \in G(A)$ and $x \in \mathfrak{M}$, $h_x g(s) = M(g(s),x) = g[M(s,x)] = gh_x(s)$ so h_x is in the center of G(A).

Corollary 2.10.1. Let A = (S,I,M) be a strongly connected automaton with n states. Then the middle is empty if and only if the identity $i(s) \equiv s$ is not representable.

Lemma 2.4. Let A = (S,I,M) be a perfect automaton. Then h_x is one-to-one and onto for all $x \in I$.

Proof: By Lemma 2.3, h_x is onto. To show h_x is one-to-one assume $h_x(s) = h_x(t) = s_1$ where $s \neq t$ (i.e., h_x is not 1-1). Then since A is strongly connected there exists $y \in I$ such that $M(t,y) = s$. Then $M(s_1,y) = M(h_x(t),y) = M(M(t,x),y) = M(t,xy) = M(t,yx) = M(M(t,y),x) = M(s,x) = h_x(s) = s_1$. Thus $h_y(s_1) = M(s_1,y) = s_1$. But by Lemma 2.2 h_y is operation preserving and $h_y(s_1) = i(s_1) = s_1$. Thus by Lemma 2.1, $h_y(s) \equiv i(s) \equiv s$. So $t = h_y(t) = M(t,y) = s$, a contradiction since $t \neq s$. Thus h_x is one-to-one.

Examples can be constructed to show that Lemma 2.4 is not true for arbitrary strongly connected automata. However, for the class of perfect automata we now see that we have the desired representation.

Theorem 2.11. Let $A = (S,I,M)$ be a perfect automaton. Then a necessary and sufficient condition that $h \in G(A)$ is that h be a representation.

Proof: By Lemmas 2.2 and 2.4 if h is a representation, then $h \in G(A)$.

Now let $g \in G(A)$ and $s_0 \in S$. Then for $s = g(s_0)$ there exists $x \in I$ such that $M(s_0,x) = s$. Then $g(s_0) = h_x(s_0)$ and h_x is operation preserving by Lemma 2.2. Thus by Lemma 2.1, $g \equiv h_x$ and so g is representable.

Corollary 2.11.1. If $A = (S,I,M)$ is a perfect automaton, then $G(A)$ is abelian.

Proof: For h_x, $h_y \in G(A)$ we have $h_x h_y = h_{xy} = h_{yx} = h_y h_x$.

Corollary 2.11.2. If $A = (S,I,M)$ is a perfect automaton, then $K[G(A)] = K[S]$.

Proof: Choose $s_0 \in S$ and for $g \in G(A)$ define $\alpha : G(A) \longrightarrow S$ by $\alpha(g) = g(s_0)$. Then $\alpha(g) = \alpha(h)$ implies $g(s_0) = h(s_0)$ and so by Lemma 2.1, $g = h$. Thus α is one-to-one. Also for $s \in S$, there exists $x \in I$ such that $M(s_0,x) = s$ since A is strongly connected. But then $h_x(s_0) = s$ and $h_x \in G(A)$. Thus $\alpha(h_x) = s$ and so α is onto. Thus $K[S] = K[G(A)]$.

It is natural to ask if the converse of Theorem 2.11 is true. It is not but we have

Proposition 2.12. If for an automaton $A = (S,I,M)$ each element of $G(A)$ is representable and each representation is in $G(A)$, then A is reversible and abelian.

Proof: Let $M(s,x) = t$. Then $h_x \in G(A)$ and so h_x^{-1} exists and h_x^{-1} is representable, say $h_x^{-1}(u) \equiv M(u,y)$. Then $M(t,y) = s$ and so A is reversible. Also $M(s,xy) = M(M(s,x),y) = M(h_x(s),y) = h_x[M(s,y)] = M(M(s,y),x) = M(s,yx)$ since $h_x \in G(A)$. Thus $\mathcal{M} = I$ and A is abelian.

Thus a partial converse to Theorem 2.11 may be stated as

Corollary 2.12.1. If A is connected and if each element of $G(A)$ is representable and each representation is in $G(A)$, then A is perfect.

Proof: This follows immediately from Proposition 2.12 and Theorem 1.5.

Proposition 2.13. Let $A = (S,I,M)$ be a strongly connected automaton with n states. Then if the middle of I is empty, $o(G(A)) < n$.

Proof: Assume $o(G(A)) = n$ and let $s_0 \in S$. Then by Lemma 2.1 for any $s \in S$ there exists $g \in G(A)$ so that $g(s_0) = s$. Now since A is strongly connected there exists an $x \in I$ so that $M(s_0,x) = s_0$. Then for any $s \in S$, $M(s,x) = M(g(s_0),x) = g[M(s_0,x)] = g(s_0) = s$. Thus h_x represents the identity and then by Corollary 2.10.1, $\mathcal{M} \neq \phi$, a contradiction. Thus $o(G(A)) < n$.

Description of the Group of a Perfect Automaton

The next theorem and its implications will lead directly to a description of the group for a perfect automaton.

Theorem 2.14. Let $A = (S,I,M)$ be a perfect automaton. Then $G(A)$ is a homomorphic image of I.

Proof: We define the homomorphism $\alpha : I \longrightarrow G(A)$ by $\alpha(x) = h$ if and only if $h(s) \equiv M(s,x)$, where $x \in I$. To see that α is in fact a homomorphism, suppose that $\alpha(x) = h$, $\alpha(y) = k$ and $\alpha(xy) = g$. Then $g(s) = M(s,xy) = M(s,yx) = M(M(s,y),x) = M(k(s),x) = hk(s)$. Thus $\alpha(xy) = g = hk = \alpha(x)\alpha(y)$ and so α is a homomorphism.

Theorem 2.14 is a result which generalizes to less restrictive classes of automata. By a similar argument, it can be shown that for a strongly connected automaton, $A = (S,I,M)$, there is a homomorphism from a sub-semigroup of I onto $G(A)$. We shall examine this more closely in the section concerning the characteristic semigroup.

The homomorphism α of Theorem 2.14 induces the natural equivalence relation $x \sim y$ if and only if $\alpha(x) = \alpha(y)$, so that I is divided into mutually disjoint and exhaustive (equivalence) classes. We will denote such a class by $\overline{x}$ (i.e., $\overline{x} = \{y \mid y \sim x\}$)and the set of all such classes by $\overline{I}$. Then we have that these equivalence classes, together with a natural operation form a parallel of a quotient group.

Corollary 2.14.1. Let $A = (S,I,M)$ be a perfect automaton. Then $\overline{I}$ forms a group isomorphic to $G(A)$, where $\overline{x}\,\overline{y} = \overline{xy}$ for $x \in \overline{x}$, $y \in \overline{y}$.

Corollary 2.14.1 yields a description of $G(A)$ in terms of certain classes of inputs and the manner in which they combine. However, knowledge of these classes depends on a previous knowledge of $G(A)$. We shall exhibit a way to determine these equivalence classes without knowledge of $G(A)$.

Definition 2.6. 7 Let $A = (S,I,M)$ be an automaton. Then for $x, y \in I$ we say <u>x is equivalent to y modulo s_0</u>, $x \underset{s_0}{\sim} y$, if $M(s_0,x) = M(s_0,y)$, where $s_0 \in S$.

Again, it is easy to verify that Definition 2.6 yields a formal equivalence relation and that, for the case of perfect automata, the classes are independent of the "base" state s_0 and coincide with the classes induced by the homomorphism α. Thus Definition 2.6 provides a means of calculating $G(A)$ for a perfect automaton A.

Theorem 2.15. Let $A = (S,I,M)$ be a strongly connected automaton with n states. Then if $G(A)$ is abelian and of order n, A is perfect.

Proof: Let $s \in S$ be an arbitrary state and $x, y \in I$ be arbitrary inputs. Then let $M(s,x) = s_1$ and $M(s,y) = s_2$. Now since there are n states and n group elements it follows from Lemma 2.1 that there exists $h_1, h_2 \in G(A)$ such that $h_1(s) = s_1$ and $h_2(s) = s_2$. Then we have

$M(s,xy) = M(M(s,x),y) = M(h_1(s),y) = h_1[M(s,y)] = h_1h_2(s).$ Similarly,

$M(s,yx) = h_2h_1(s)$. As $h_1h_2 = h_2h_1$, $M(s,xy) = M(s,yx)$. Thus A is perfect.

We conclude this section with an example of the computation of the group of a perfect automaton.

A =

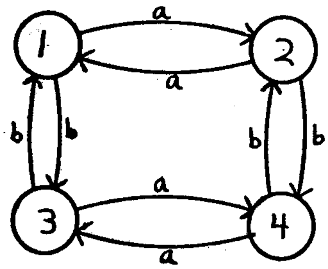

Figure 4

Here the input composition is the usual juxtaposition (generators a ,b). It is easily verified that the automaton A depicted above is perfect. Let us use equivalence modulo state 2 to compute the equivalence (as remarked above the same classes arise for each state).

$$\overline{aa} = \{aa, bb, abab, \cdots\}$$
$$\bar{a} = \{a, abb, bab, \cdots\}$$
$$\bar{b} = \{b, aba, baa, \cdots\}$$
$$\overline{ab} = \{ab, ba, abaa, \cdots\}$$

where, for instance, $\bar{a}$ is as above since $M(2,a) = M(2,abb) = \cdots$.

From these classes we can easily compute Table I as shown below.

	$\overline{aa}$	$\overline{a}$	$\overline{b}$	$\overline{ab}$
$\overline{aa}$	$\overline{aa}$	$\overline{a}$	$\overline{b}$	$\overline{ab}$
$\overline{a}$	$\overline{a}$	$\overline{aa}$	$\overline{ab}$	$\overline{b}$
$\overline{b}$	$\overline{b}$	$\overline{ab}$	$\overline{aa}$	$\overline{a}$
$\overline{ab}$	$\overline{ab}$	$\overline{b}$	$\overline{a}$	$\overline{aa}$

Table I

This is recognized as the "four group". Table I will also serve as the group table for G(A) and it is convenient to specify G(A) by

$$G(A) = \{g_{\overline{aa}}, g_{\overline{a}}, g_{\overline{b}}, g_{\overline{ab}}\}$$

where

$g_{\overline{aa}}(s) = M(s,aa)$, $g_{\overline{b}}(s) = M(s,b)$, $g_{\overline{a}}(s)=M(s,a)$,
$g_{\overline{ab}}(s) = M(s,ab)$.

This of course tells us how the group elements operate on the states and we can use Table I and the subscripts to combine them(i.e., $g_{\overline{a}}g_{\overline{b}} = g_{\overline{ab}}$, etc.).

<u>The Characteristic Semigroup</u>

The equivalence relation established in conjunction with Theorem 2.14 was restricted to perfect automata. The equivalence below agrees with this but applies to arbitrary automata. The structure of the resulting semigroup and of the automaton can then be seen to bear interesting relationships.

Definition 2.7. Let $A = (S,I,M)$ be an automaton and $x,y \in I$. Then <u>x is equivalent to y</u>, $x \sim y$, if $M(s,x) \equiv M(s,y)$. We denote by $\overline{x}$ the set $\overline{x} = \{y | x \sim y\}$ and by $\overline{I}$ the set of all such classes.

Proposition 2.16. The equivalence of Definition 2.7 is an equivalence relation and the classes $\overline{I}$ form a semigroup under the induced operation $\overline{x}\ \overline{y} = \overline{xy}$, where $x \in \overline{x}$ and $y \in \overline{y}$. This semigroup is called the <u>characteristic semigroup of A</u>.

Proof: It is clear that we have an equivalence relation. For $x_1, x_2 \in \overline{x}$ and $y_1, y_2 \in \overline{y}$ we have $M(s,x_1y_1) \equiv M(M(s,x_1),y_1) \equiv M(M(s,x_2),y_1) \equiv M(M(s,x_2),y_2) \equiv M(s,x_2y_2)$. Thus $\overline{x}_1\overline{y}_1 = \overline{x}_2\overline{y}_2$ and so the class multiplication is well-defined and closed. Also it is clear that associativity is inherited. Thus $\overline{I}$ is a semigroup.

It is helpful to notice the following facts: For $A = (S,I,M)$, the distinct $\overline{x}$ classes of $\overline{I}$ correspond to the distinct representations h_x by elements of I. The class $\overline{x}$ will frequently be associated with the representation h_x where $x \in \overline{x}$. Also it is clear that x is in the middle of I if and only if $\overline{x}$ is in the center of $\overline{I}$. Further if A has n states, then $o(\overline{I}) \leq n^n$, the number of functions on n symbols. Finally, the characteristic semigroup possesses a desirable property which does not hold for the group of an automaton. That is, an operation preserving function of the automaton A onto the automaton B induces a homomorphism of the characteristic semigroup of A onto the characteristic semigroup of B(by the obvious identification map) while G(B) is not in general a homomorph of G(A) in this case.

From the way multiplication is defined in $\overline{I}$ the following is obvious.

Proposition 2.17. The function β: $I \longrightarrow \overline{I}$ defined by $\beta(x) = \overline{x}$ is a homomorphism.

The following specialization is of interest.

Corollary 2.17.1. If $A = (S,I,M)$ is an automaton and I is a group with identity e, then $\overline{e}$ is an invariant subgroup of I and $\overline{I}$ is isomorphic to the quotient group $I/\overline{e}$.

Proof: This is an immediate application of the homomorphism theorems of group theory.

In what follows we will notice some reflection of this result when I is an arbitrary semigroup.

The following result partially indicates the nature of the characteristic semigroup for a strongly connected automaton.

Proposition 2.18. Let $A = (S,I,M)$ be a strongly connected automaton. Then if $\overline{I}$ has a right identity it is unique and is a two-sided identity.

Proof: Let $\overline{e} \in \overline{I}$ be such that $\overline{x}\,\overline{e} = \overline{x}$ for all $\overline{x} \in \overline{I}$. Then for $s \in S$, choose $x \in I$ and $t \in S$ such that $M(t,x)=s$. Then for $e \in \overline{e}$, $s = M(t,x) = M(t,xe) = M(M(t,x),e) = M(s,e)$. Thus $M(s,e) \equiv s$. Hence $M(s,xe) \equiv M(s,ex) \equiv M(s,x)$ and so $\overline{e}$ is a two-sided identity and is therefore unique.

Corollary 2.18.1. Let $A = (S,I,M)$ be a strongly connected automaton. Then $\overline{I}$ is a group if and only if the representations defined by the $\overline{x}$ classes form a permutation group.

Proof: The statement of sufficiency is merely a play on words.

Necessity follows from the fact that the identity of $\overline{I}$ represents the function which maps each state to itself. Hence if a class $\overline{x}$ has an inverse relative to this identity the corresponding representation must be one-to-one and onto.

For a strongly connected automaton with n states a bound on the order of the characteristic semigroup can be obtained in terms of the order of the group of the automaton.

Theorem 2.19. If $A = (S,I,M)$ is strongly connected with n states and $o(G(A))=k$, then $o(\overline{I}) \leq n^{n/k}$.

Proof: We pointed out earlier that if A is strongly connected with n states and $o(G(A))=k$, then k divides n, say $kr=n$. Let $G(A)= \{g_1, g_2, \cdots, g_k\}$. It is clear from Lemma 2.1 that we can choose r states, say $s_1, s_2, \cdots, s_r$ so that

$$\bigcup_{j=1}^{r} \bigcup_{i=1}^{k} g_i(s_j) = S \quad \text{and}$$

$$\bigcup_{i=1}^{k} g_i(s_j) \bigcap \bigcup_{i=1}^{k} g_i(s_u) = \phi \qquad \text{for } j \neq u.$$

Thus we can write the representation corresponding to $\overline{x}$ in the classical form as follows:

$$\overline{x}: \begin{pmatrix} g_1(s_1) & g_2(s_1) \cdots g_k(s_1) & g_1(s_2) \cdots g_k(s_2) \cdots g_1(s_r) \cdots g_k(s_r) \\ t_1 & g_2(t_1) \cdots g_k(t_1) & t_2 \cdots g_k(t_2) \cdots g_1(t_r) \cdots g_k(t_r) \end{pmatrix}$$

where the row of images is as above because if we assume t_1 to be arbitrary then (assuming g_1 is the identity)

$$M(g_j(s_1),x) = g_j[M(s_1,x)] = g_j(t_1) \text{ where } x \in \overline{x}.$$

Thus we have n choices for each of the t_i and so $o(\overline{I}) \leq n^r$.

It can be observed that by defining an $\overline{x}$ class of each of the possible forms suggested in the proof of Theorem 2.19, this bound can actually be achieved.

Theorem 2.20. Let $A = (S,I,M)$ be a strongly connected automaton with n states.
Then

(I) For the middle, $\mathcal{M}$, $\mathcal{M} \neq \phi$ if and only if $\overline{I}$ has an identity.

(II) $\overline{I}$ has an identity if and only if its center, $C(\overline{I})$, is a group and is thus a subgroup of $G(A)$.

(III) $\overline{I}$ is isomorphic to $G(A)$ if and only if $o(G(A)) = n$.

Proof: Parts (I) and (II) are restatements of Corollary 2.10.1 and Theorem 2.10 respectively in terms of properties of the characteristic semigroup.

To prove the necessity of (III) notice that since A is strongly connected with n states, $o(\overline{I}) \geq n$. Then since in this case $o(G(A)) \leq n$ and $\overline{I}$ is isomorphic to $G(A)$ we must have $o(\overline{I}) = o(G(A)) = n$.

Now assume $o(G(A)) = n$ and choose $s_0 \in S$. Then by Lemma 2.1, for any $t \in S$ there exists $h \in G(A)$ such that $h(s_0) = t$. Now if $M(s_0,x) = M(s_0,y) = t$, then $M(t,x) = M(h(s_0),x) = h[M(s_0,x)] = h[M(s_0,y)] = M(h(s_0),y) = M(t,y)$. Thus $\overline{x} = \overline{y}$ and $o(\overline{I}) = n$. Now $\alpha : \overline{I} \longrightarrow G(A)$ defined by $\alpha(\overline{x}) = g$ where $M(s_0,x) = g(s_0)$ for $x \in \overline{x}$ is an isomorphism. α is one-to-one and onto in view of Lemma 2.1 and if $\alpha(\overline{x}) = g$ and $\alpha(\overline{y}) = h$, then for $x \in \overline{x}$ and $y \in \overline{y}$,

$M(s_0,xy)=M(M(s_0,x),y)=M(g(s_0),y)=g[M(s_0,y)] = g(h(s_0))$. Thus $\alpha(\bar{x}\ \bar{y}) = gh = \alpha(\bar{x})\ \alpha(\bar{y})$.

For automata satisfying the hypothesis of Theorem 2.20 we find a large amount of structure forced on the characteristic semigroup. At this point it is interesting to point out an immediate application of our results to semigroup theory.

Corollary 2.20.1. Let I be an abelian semigroup of functions on the finite set S and suppose that I is transitive (i.e., for any s, t $\in$ S there is an x $\in$ I such that x(s) = t). Then I is a group of regular permutations on S and is of order n (the order of S).

Proof: Define the automaton A = (S,I,M) where M(s,x) = x(s). Then I and $\bar{I}$ coincide since each class $\bar{x}$ contains only the function x. Now A is strongly connected and sequential by the transitive and associative properties. Also since I is abelian A is abelian. Thus A is perfect and by Corollary 2.11.2, o(G(A)) = o(S). Thus by Theorem 2.20, I is isomorphic to G(A) and is a group of regular permutations.

Before proceeding to the last result of this section we must prove a lemma concerning semigroups.

Definition 2.8. Let I be a semigroup and x $\in$ I. x is said to be periodic if there exists a positive integer t such that $x^{t+1} = x$ and if t is the least such integer, t is the period of x. If an element is of period one it is called idempotent.

This is not the usual [12] definition of 'periodic' for semigroups. However it is a natural generalization of the concept used in group theory and is useful in what follows. Notice that according to this definition even a finite semigroup can have elements which are not periodic.

Lemma 2.5. If I is a semigroup with exactly one idempotent and each element is periodic, then I is a group.

Proof: Let e be the idempotent of I. Then for $x \in I$ and $x \neq e$, we have $x^{t+1} = x$ for the period $t > 1$. Then $(x^t)(x^t) = (x^{t+1})(x^{t-1}) = x\, x^{t-1} = x^t$. Thus $(x^t)^2 = x^t$, so x^t is an idempotent and $x^t = e$. But $x = x^t x = x x^t = ex = xe$, so e is a two-sided identity. Also $xx^{t-1} = x^{t-1}x = e$, so x has a two-sided inverse and thus I is a group.

The last result of this section indicates a fundamental property of the characteristic semigroup for a strongly connected automaton.

Theorem 2.21. Let $A = (S,I,M)$ be a strongly connected automaton with n states. Then there are subgroups J_1 and J_2 of the characteristic semigroup $\overline{I}$ such that J_2 is a normal subgroup of J_1 and the factor group J_1/J_2 is isomorphic to $G(A)$.

Proof: Let us denote by $M(s,\overline{x})$ the unique state determined by $M(s,x)$ where $x \in \overline{x}$. Choose $s_0 \in S$ and let $J = \left\{\overline{x} \mid \overline{x} \in \overline{I} \text{ and } M(s_0,\overline{x}) = g(s_0) \text{ for some } g \in G(A)\right\}$. Then J is a subsemigroup of $\overline{I}$ since if $M(s_0,\overline{x}) = g(s_0)$ and

$M(s_0,\bar{y})= h(s_0)$, then $M(s_0,\bar{x}\ \bar{y})= g(h(s_0))$. Thus $\bar{x}$, $\bar{y} \in J$ implies that $\bar{x}\ \bar{y} \in J$. Also this reasoning shows that the function $\beta : J \longrightarrow G(A)$ defined by $\beta(\bar{x})= g$, where $M(s_0, \bar{x})= g(s_0)$ is a well-defined homomorphism. Since A is strongly connected β is onto.

Now let $\bar{e}$ be any idempotent of J(it is known that any finite semigroup has at least one idempotent [12]). Since β is a homomorphism and $\bar{e}$ is an idempotent, $\beta(\bar{e})$ must be the identity of G(A). Thus

(1) $M(s_0,\bar{e})= s_0$. Also for any state of the form $g(s_0)$ where $g \in G(A)$,

(2) $M(g(s_0),\bar{e})= g[M(s_0,\bar{e})] = g(s_0)$.

Let $\{\bar{e}_1, \bar{e}_2, \cdots , \bar{e}_k\}$ be the (non-empty) set of all distinct idempotents of J. Let $J^1= \bar{e}_1J\bar{e}_1$. Then J^1 is a subsemigroup of J and $\bar{e}_1 \in J^1$. Also $\bar{e}_1$ is a two-sided identity for J^1 since $\bar{e}_1(\bar{e}_1\bar{x}\ \bar{e}_1)= (\bar{e}_1\bar{x}\ \bar{e}_1)\bar{e}_1= \bar{e}_1\bar{x}\ \bar{e}_1$.

Now if $\bar{e}_1$ is the only idempotent of J^1, let $J^1= J_1$. Otherwise there is another idempotent, say $\bar{e}_2$, in J^1 and so define $J^2 = \bar{e}_2J^1\bar{e}_2$. Then J^2 is a subsemigroup of J^1 and $\bar{e}_2 \in J^2$ and $\bar{e}_2$ is a two-sided identity for J^2. Also $\bar{e}_1 \notin J^2$ since then we would have $\bar{e}_1\bar{e}_2= \bar{e}_1= \bar{e}_2$, a contradiction since $\bar{e}_1 \neq \bar{e}_2$. Now if $\bar{e}_2$ is the only idempotent of J^2, let $J^2= J_1$. Otherwise we repeat as above with the new idempotent. Hence in at most k steps we arrive at the subsemigroup J_1 which has exactly one idempotent which is a two-sided identity.

Since J_1 is a subsemigroup of J, β acting on J_1 is again a homomorphism. Also β maps J_1 onto G(A) since

for $\overline{x} \in J$,
$M(s_0,\overline{e}_k \cdots \overline{e}_1 \overline{x}\ \overline{e}_1 \cdots \overline{e}_k) = M(M(s_0,\overline{e}_k),\overline{e}_{k-1} \cdots \overline{e}_1 \overline{x}\ \overline{e}_1 \cdots \overline{e}_k) =$
$M(s_0,\overline{e}_{k-1} \cdots \overline{e}_1 \overline{x}\ \overline{e}_1 \cdots \overline{e}_k) = \cdots =$
$M(M(s_0,\overline{x}),\overline{e}_1 \cdots \overline{e}_k) = M(g(s_0),\overline{e}_1 \cdots \overline{e}_k) =$
$M(M(g(s_0),\overline{e}_1),\overline{e}_2 \cdots \overline{e}_k) = M(g(s_0),\overline{e}_2 \cdots \overline{e}_k) = \cdots = g(s_0)$ by repeated applications of (1) and (2). Thus since β maps J onto $G(A)$, β maps J_1 onto $G(A)$.

Finally we show that every element of J_1 is periodic. First notice that if $M(s_0,\overline{x}) = g(s_0)$, where $g \in G(A)$, then $M(s_0,\overline{x}^m) = g^m(s_0)$. Now let $\overline{x} \in J_1$. Then $M(s_0,\overline{x}) = g(s_0)$ for some $g \in G(A)$. Suppose $g^{t+1} = g$(i.e., g is of period t). Then consider the powers $\overline{x}, \overline{x}^2, \cdots, \overline{x}^u, \cdots$. Since J_1 is finite there must be a repetition, say $\overline{x}^u = \overline{x}^v$ where $u > v$. Then $g^u(s_0) = M(s_0,\overline{x}^u) = M(s_0,\overline{x}^v) = g^v(s_0)$. Thus by Lemma 2.1, $g^u = g^v$ or $g^{u-v+1} = g$. Thus $u-v = mt$ or $u = v+mt$ for some positive integer m. Then we have
$(\overline{x}^v)^{mt+1} = \overline{x}^v \overline{x}^{mt}\ \overline{x}^{(v-1)mt} = \overline{x}^u\ \overline{x}^{(v-1)mt} = \overline{x}^v\ \overline{x}^{(v-1)mt} = \cdots =$
$\overline{x}^v$. Thus $\overline{x}^v$ is periodic. But we noticed in the proof of Lemma 2.5 that if $(\overline{x}^v)^{mt+1} = \overline{x}^v$, then $(\overline{x}^v)^{mt}$ is idempotent. But the only idempotent is a two-sided identity and so $\overline{x}^{vmt} = 1$(the two-sided identity) or $\overline{x}^{vmt+1} = \overline{x}$ and $\overline{x}$ is periodic. Thus by Lemma 2.5, J_1 is a group. Then let J_2 be the kernel of the homomorphism β and then the quotient group J_1/J_2 is isomorphic to $G(A)$.

PART III

THE DIRECT PRODUCT OF AUTOMATA

Strong Relatedness

In this section a particular structure is studied, the direct product. The algebraic devices of the previous sections are applied with considerable success, though many problems are still unsettled. A necessary and sufficient condition for the direct product to be strongly connected is given. The main results of this section concerns the following problem. Given an automaton, when can it be written as a direct product of automata? This seems to be a difficult and, at the same time, important problem. Sufficient conditions for writing a given automaton as a direct product are given here and as a matter of fact the proof of these results show how to construct the "factors". However the condition given here is, no doubt, too strong to be useful in applications. Nevertheless, this is a step in the right direction and it is hoped that the solution here may suggest the proper line of attack under more general circumstances.

Definition 3.11. Let $A = (S,I,M)$ and $B = (T,I,N)$ be two automata. The direct product, $A \times B$, is the automaton $A \times B = (S \times T,\ I,\ M \times N)$ where $M \times N\,[(s,t),x] = (M(s,x),\ N(t,x))$.

This definition parallels exactly the definition of

Rabin and Scott 5 .

Definition 3.2. Two automaton $A = (S,I,M)$ and $B = (T,I,N)$ are <u>strongly related</u> if given any s_1, $s_2 \in S$ and any $t_1, t_2 \in T$ there exists an $x \in I$ such that $M(s_1,x) = s_2$ and $N(t_1,x) = t_2$.

Obviously if two automata are strongly related, each automaton is strongly connected. As we shall see, the only desirable property which this relation possesses is symmetry.

Proposition 3.1. Let $A = (S,I,M)$ and $B = (T,I,N)$ be two automata. Then a necessary and sufficient condition that $A \times B$ be strongly connected is that A and B be strongly related.

Proof: Suppose that $A \times B$ is strongly connected. Then given any $(s_1,t_1) \in S \times T$ and $(s_2,t_2) \in S \times T$ there exists an $x \in I$ such that $M \times N\left[(s_1,t_1),x\right] = (s_2,t_2)$. But $M \times N\left[(s_1,t_1),x\right] = (M(s_1,x), N(t_1,x))$. Hence $M(s_1,x) = s_2$ and $N(t_1,x) = t_2$ and so A and B are strongly related.

Now suppose that A and B are strongly related. Then given any $(s_1,t_1) \in S \times T$ and $(s_2,t_2) \in S \times T$ there exists $(s_2,t_2) = (M(s_1,x), N(t_1,x)) = M \times N\left[(s_1,t_1),x\right]$. Thus $A \times B$ is strongly connected.

The object of Proposition 3.1 and Definition 3.2 was to show the relationship which must exist between two automata in order that their direct product be strongly connected.

Proposition 3.2. Let $A = (S,I,M)$ and $B = (T,I,N)$ be two automata which are strongly related. Then if there exists an onto, operation preserving function, $h:A \longrightarrow C$, where C is the automaton $C = (R,I,P)$, C is strongly related to B.

Proof: Let r_1, $r_2 \in R$ and t_1, $t_2 \in T$. Then since h is onto there exist s_1, $s_2 \in S$ such that $h(s_1) = r_1$ and $h(s_2) = r_2$. Then since A is strongly related to B there exists an $x \in I$ such that $M(s_1,x) = s_2$ and $N(t_1,x) = t_2$. But then $r_2 = h(s_2) = h[M(s_1,x)] = P(h(s_1),x) = P(r_1,x)$ since h is operation preserving. Thus C is strongly related to B.

Hence if A x B yields a strongly connected automaton and C is any operation preserving image of A then C xB must yield a strongly connected automaton.

Proposition 3.3. If $A = (S,I,M)$ and $B = (T,I,N)$ are strongly related automata, then there is no operation preserving function between A and B (A and B non-trivial).

Proof: Suppose that there exists an operation preserving function between A and B, say $h:A \longrightarrow B$. Then let $s_1 \in S$ and $t_1 = h(s_1)$ and $t_2 \in T$ be such that $t_2 \neq h(s_1)$. Now since A and B are strongly related there exists an $x \in I$ such that $M(s_1,x) = s_1$ and $N(t_1,x) = t_2$. But then $t_2 = N(t_1,x) = N(h(s_1),x) = h[M(s_1,x)] = h(s_1)$ since h is operation preserving, a contradiction. Thus no such h exists.

Corollary 3.3.1. For any automaton A, A is not strongly related to itself and hence A x A is not strongly connected.

Proof: The identity function is an operation preserving function from any automaton to itself. Thus by Proposition 3.3, A is not strongly related to A.

The Group of A Direct Product

Proposition 3.4. Let $A = (S,I,M)$ and $B = (T,I,N)$ be automata. Then $G(A) \times G(B)$ is isomorphic to a subgroup of $G(A \times B)$.

Proof: Let $g \in G(A)$, $h \in G(B)$ and $(s,t) \in S \times T$. Now consider $(g,h) \in G(A) \times G(B)$. Let $((g,h))(s,t) = (g(s),h(t))$ and then $(g,h)[M \times N((s,t),x)] = (g,h)[(M(s,x),N(t,x))] = (g[M(s,x)], h[N(t,x)]) = (M(g(s),x),N(h(t),x)) = M \times N[(g(s),h(t)),x]$ since g and h are operation preserving on A and B respectively. Thus (g,h) defines an operation preserving function on A x B.

Also the function defined by (g,h) is one-to-one and onto since g and h separately are one-to-one and onto. Thus the function defined by (g,h) is in G(A x B) and so $G(A) \times G(B) \subseteq G(A \times B)$ by means of the obvious identification.

To show that, in general, equality does not hold in Proposition 3.4 we include the following example:

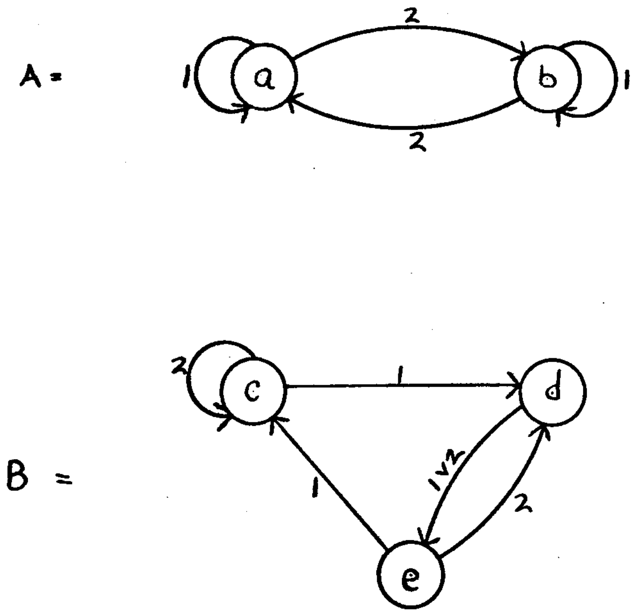

Figure 5

again the input composition is taken to be juxtaposition (generators 1, 2) for both A and B and the next state functions are extended to the entire input semigroup by the sequential property.

Then we have

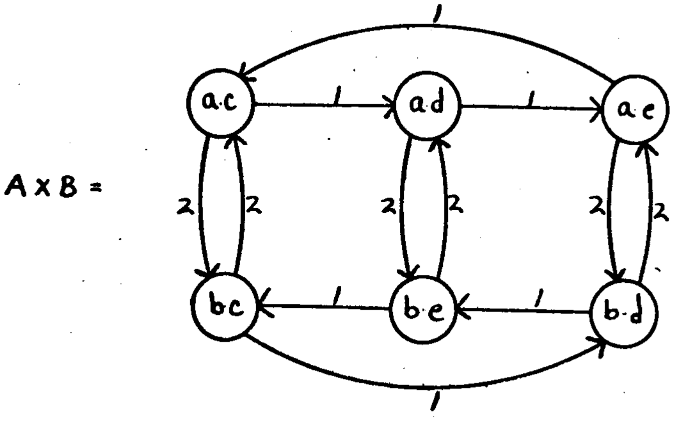

Figure 6

Then, writing the groups as permutations, we have

$$G(A) = \{I,F\} \qquad \text{where } F = (ab)$$

$$G(B) = \{I\}$$

$$G(A \times B) = \{I,H,H^2,K,HK,H^2K\}$$

where

$$H = (ac\ ad\ ae)(bc\ be\ bd)$$

$$K = (ac\ bc)(ad\ bd)(ae\ be)$$

and of course

$$G(A) \times G(B) \approx \{I,K\} .$$

Notice here that A and B are even strongly related.

As would be expected, it is easily verified that an isomorphism between two automata A = (S,I,M) and B = (T,I,N) induces an isomorphism between G(A) and G(B). Unfortunately it is also easy to find counter examples to the converse of this statement, for instance consider automaton A of Figure 3 and the automaton obtained by interchanging 0 and 1.

Automata As Direct Products

We have, thus far, examined briefly the manner in which the direct product affects structure and groups of automata. An interesting question is: under what conditions can a given automaton be written as a direct product of two non-trivial automata? Furthermore if a given automaton can be written as a direct product how can its "factors" be determined? The following result gives at least a partial answer to these questions.

Theorem 3.6. Let A = (S,I,M) be a strongly connected and G(A) be transitive. Then if G(A) is isomorphic to a direct product of groups, A is isomorphic to a direct product of automata.

Proof: Without loss of generality we may identify G(A) with the direct product of groups H X L. We now show that A is isomorphic to B X C, where B = (H,I,N) and C = (L,I,N'), N and N' being defined below. Let ϕ:H X L $\longrightarrow$ S be defined as follows: let $s_0 \in$ S be fixed and define $\phi((h,g)) = (h,g)(s_0)$ for $(h,g) \in$ H X L. By Lemma 2.1, ϕ is one-to-one. By hypothesis, ϕ is onto.

We now define $N(h,x) = h_1$ if and only if $M(\phi((h,g)),x) = \phi((h_1,g_1))$. This definition is not ambiguous since ϕ is one-to-one and onto. However, we must show that this yields a well-defined definition of N. Now $M(\phi((h,g)),x)=M((h,g)(s_0),x)=(h,g)[M(s_0,x)]$. Now suppose $M(s_0,x) = (k,m)(s_0)$(by hypothesis there is such a group element). Then $M(\phi((h,g)),x) =$ $(h,g)(k,m)(s_0) = (hk,gm)(s_0) = \phi(hk,gm)$. But then $M(\phi((h,g_1)),x) = \phi(hk,g_1m)$ so that N is well defined.

Similarly, we define $N'(g,x) = g_1$ if and only if $M(\phi((h,g)),x) = \phi((h_1,g_1))$. Then an argument analogous to the above shows that N' is well defined.

We now have defined the automata B and C and we wish to show that ϕ is the desired isomorphism between A and B X C. We have already shown that ϕ is one-to-one and onto. Strictly from the definitions of ϕ , N and N' we have

$\phi[N \times N'((h,g),x)] = \phi[N(h,x),N'(g,x)] = M(\phi((h,g)),x)$, So ϕ is operation preserving and is thus an isomorphism.

A way to generalize this result will be indicated shortly but we show now that the condition of Theorem 3.6 is both necessary and sufficient in the case of perfect automata.

Theorem 3.7. Let $A = (S,I,M)$ be a perfect automaton. Then a necessary and sufficient condition that A be isomorphic to a direct product of automata is that $G(A)$ be isomorphic to a direct product of groups.

Proof: To show sufficiency we notice that by Theorem 2.11, A satisifies the conditions of Theorem 3.6.

Now suppose A is isomorphic to $B \times C$, where $B=(T,I,N)$ and $C = (R,I,N')$. First, since A is perfect and isomorphic to $B \times C$ and the perfect structure is invariant under operation preserving functions, $B \times C$ is perfect. Also, the projection functions $p_B: B \times C \longrightarrow B$ and $p_C: B \times C \longrightarrow C$ defined by $p_B((t,r)) = t$ and $p_C((t,r)) = r$ are onto and operation preserving. Thus B and C are each perfect. Now by Theorem 2.11, for $g \in G(B \times C)$ we have

$g((t,r)) \equiv N \times N'((t,r),x_0) \equiv (N(t,x_0),N'(r,x_0)) \equiv (h(t),f(r))$.

But also by Theorem 2.11, $h \in G(B)$ and $f \in G(C)$. In view of Theorem 2.11 and the fact that B and C are strongly related, the correspondenbe $g \longleftrightarrow (h,f)$ is one-to-one and onto between $G(B \times C)$ and $G(B) \times G(C)$. Thus it is clearly an isomorphism. But the isomorphism

between A and $B \times C$ induces an isomorphism between

G(A) and G(B X C). Thus G(A) is isomorphic to G(B) X B(C).

The automaton exhibited in Figure 6 shows that for a strongly connected automaton A with n states and $o(G(A)) = n$, even though A is a direct product G(A) need not be. Thus the converse to Theorem 3.6 does not hold. We shall see, however, that in the case described above, the composite nature of G(A X B) that can be observed in the example of Figure 6 will always occur and that this is sufficient to produce a factorization of the automaton.

Definition 3.3. Let $A = (S,I,M)$ be an automaton and G(A) be its group of automorphisms. Then for a subgroup H of G(A), s_1 is equivalent to s_2 modulo H, $s_1 \sim s_2(H)$, if there exists $h \in H$ such that $h(s_1) = s_2$, where s_1, $s_2 \in S$.

Note: Equivalence modulo a subgroup of G(A) is an equivalence relation on the set of states of an automaton A. We denote such a class by $\overline{s}$ and the set of all such classes by $\overline{S}$.

Definition 3.4. Let $A = (S,I,M)$ be an automaton and G(A) be its group of automorphisms. Then for a subgroup H of G(A) we define the automaton A modulo H, A/H, by

$A/H = (\overline{S},I,M^*)$ where $\overline{S}$ is the set of equivalence classes of S modulo H and $M^*(\overline{s},x) = \overline{M(s,x)}$ where $s \in \overline{s}$.

Note: The next state function in A/H is well-defined. For suppose that $M(s_1,x) = t$ and $s_1 \sim s_2(H)$. Then there exists $h \in H$ such that $h(s_1) = s_2$. But then $M(s_2,x) = h(t)$ so that $M(s_1,x) \sim M(s_2,x)\ (H)$. Also notice that $\beta(s) = \overline{s}$ is an onto, operation preserving function from A to A/H so that all the desirable structures of A are imparted to A/H.

Theorem 3.8. Let $A = (S,I,M)$ be a strongly connected automaton and H be a normal subgroup of G(A). Then the factor group G(A)/H is isomorphic to a subgroup of G(A/H).

Proof: Let $\{H\ g_i\}$ be the cosets which constitute G(A)/H. Then for each distinct coset $H\ g_j$ define $G_j\colon A/H \longrightarrow A/H$ by $G_j(\overline{s}) = \overline{g_j(s)}$ where $s \in \overline{s}$. We first show that G_j is well-defined. Let $s,t \in \overline{s}$. Then there is an $h \in H$ with $h(s) = t$. Thus $g_j(t)=g_j(h(s)) =h_1(g_j(s))$ since H is normal. But this means $g_j(t)\sim g_j(s)(H)$ and so $\overline{g_j(s)} = \overline{g_j(t)}$ and G_j is well-defined.

Now suppose that $G_j(\overline{s}) = G_j(\overline{t})$. Then $\overline{g_j(s)}=\overline{g_j(t)}$ or $g_j(s) \sim g_j(t)(H)$. Thus there is an $h \in H$ with $h(g_j(s)) = g_j(t)$ so that $g_j^{-1}hg_j(s) = h_1(s) = t$. But then $s \sim t(H)$ or $\overline{s} = \overline{t}$ and so G_j is one-to-one.

Also given $\overline{t} \in \overline{S}$, choose $\overline{t} \in \overline{t}$. Then there is $s \in S$ so that $g_j(s) = t$ since g_j is onto. Then $G_j(\overline{s})=\overline{g_j(s)}=\overline{t}$ and so G_j is onto. Further we have

$G_j[M^*(\overline{s},x)] =G_j(\overline{M(s,x)}) = \overline{g_j[M(s,x)]} = \overline{M(g_j(s),x)} =$ $M^*(\overline{g_j(s)},x) = M^*(G_j(\overline{s}),x)$ by the definitions of M^* and

G_j. Thus $G_j \in G(A/H)$.

Finally suppose that g_1 and g_2 belong to distinct cosets and that $G_1(\bar{s}) = G_2(\bar{s})$ for some $\bar{s} \in \bar{S}$. Then $g_1(s) \sim g_2(s)(H)$ or $h(g_1(s)) = g_2(s)$ for some $h \in H$. But then by Lemma 2.1, $hg_1 \equiv g_2$ and so g_1 and g_2 are in the same coset, a contradiction. Thus distinct cosets give rise to distinct elements of $G(A/H)$. Thus it is clear that $G_j \longleftrightarrow g_j$ is an isomorphism between $G(A)/H$ and a subgroup of $G(A/H)$.

It is easy to find examples where the subgroup mentioned in the above theorem is, in fact, proper. However we notice

Corollary 3.8.1. Let $A = (S,I,M)$ be a strongly connected automaton with n states and $o(G(A)) = n$. Then if H is a normal subgroup of $G(A)$, $G(A)/H$ is isomorphic to $G(A/H)$.

Proof: Notice that the order of $G(A)/H$ is equal to the number of states of A/H and that A/H is strongly connected.

Theorem 3.9. Let $A = (S,I,M)$ be a strongly connected automaton with n states and $o(G(A)) = n$. Then if there exist subgroups H and K of $G(A)$ such that $H \cap K = 1$ and $H K = G(A)$, A is isomorphic to $A/H \times A/K$.

Proof: Let $H = \{1,h_1,h_2,\dots,h_m\}$ and

$$K = \{1,g_1,g_2,\dots,g_t\} .$$

Then choose $s_0 \in S$ and consider the array

$$\begin{array}{lllll} 1(s_0) & g_1(s_0) & g_2(s_0) & \cdots & g_t(s_0) \\ h_1(s_0) & h_1g_1(s_0) & & \cdots & h_1g_t(s_0) \\ \vdots & \vdots & & & \vdots \\ h_m(s_0) & h_mg_1(s_0) & & \cdots & h_mg_t(s_0). \end{array}$$

First since A is strongly connected with $o(G(A))=n$, $HK = G(A)$, $H \cap K = 1$ it is clear, in view of Lemma 2.1, thateach state of S appears in this array once and only once. Also it is clear that the rows of this array are the equivalence classes of S modulo K and the columns are the equivalence classes of S modulo H.

Thus the intersection of any equivalence class of S modulo H with any one of the classes of S modulo K is exactly one state.

So we make the correspondence $\phi : A/H \times A/K \longrightarrow A$ as follows: $\phi(\overline{s}_H, \overline{t}_K) = \overline{s}_H \cap \overline{t}_K$.

According to the remark immediately preceeding ϕ is one-to-one and onto.

But if in A/H, $M^*(\overline{s}_H, x) = \overline{u}_H$ and in A/K, $M^{**}(\overline{t}_K, x) = \overline{v}_K$ then $\phi[M^* \times M^{**}((\overline{s}_H, \overline{t}_K), x)] = \phi(\overline{u}_H, \overline{v}_K) = \overline{u}_H \cap \overline{v}_K$ and $M(\overline{s}_H \cap \overline{t}_K, x) = \overline{u}_H \cap \overline{v}_K$, so ϕ is operation preserving. ThusA/H X A/K is isomorphic to A.

Now we find that the converse is also true.

Theorem 3.10. Let $A = (S,I,M)$ be a strongly connected automaton with n states and $o(G(A)) = n$. Then if A is isomorphic to $B \times C$, $G(A)$ has subgroups H and K with $HK = G(A)$ and $H \cap K = 1$.

Proof: Let B = (T,I,N) and C = (R,I,P). where $T = \{t_0, t_1, \ldots, t_t\}$ and $R = \{r_0, r_1, \ldots, r_r\}$. Then we can identify S with the set of pairs (t_i, r_j), $i = 0, 1, \ldots, t$; $j = 0, 1, \ldots, r$.

Then let $g_{i,0}$ be the $g \in G(A)$ such that $g(t_0, r_0) = (t_i, r_0)$ and $g_{0,j}$ be the $g \in G(A)$ such that $g(t_0, r_0) = (t_0, r_j)$. Since $O(G(A)) = o(S)$ and A is strongly connected, Lemma 2.1 tells us that these are uniquely defined functions.

Now let

$$H = \{g_{i,0}\} \qquad i = 0, 1, \ldots, t \qquad \text{and}$$
$$K = \{g_{0,j}\} \qquad j = 0, 1, \ldots, r.$$

Then $H \cap K = 1$ and $HK = G(A)$.

SUMMARY

A brief review of what this thesis accomplishes is given here, together with mention of some lines of investigation which remain open. In Part I the scene has been set for what follows by presenting some of the basic automata structures and their interrelationships. Also it was noticed there that several of these structures are invariant under the general class of continuous functions. In Part II, after an introduction to the concept of an operation preserving function, a group was associated with each automaton. We then examined to what extent the structure of the group and of the automaton are interdependent. For perfect automata we were able to give a complete characterization of the associated group. A natural equivalence was then placed on the input semigroup and this gave rise to the characteristic semigroup. The study was thereby enriched by the additional interplay which naturally arises. It could then be observed that the characterization of the group of a perfect automaton had in fact been given in terms of this characteristic semigroup. We then investigated to what extent these results could be carried over for strongly connected automata. Finally, in Part III, we found that under certain circumstances the composite property of the group of an automaton forces the representation of the automaton as a direct product and conversely.

In the area of automata studies, the use of the tools introduced in the text represent a new adventure. As a result many interesting and natural questions at present remain unanswered. We shall mention here only a few which seem to have an important bearing on the concepts introduced. The first question is whether a strongly connected automaton always has a subset of its characteristic semigroup which is isomorphic to the group of the automaton. As indicated by Theorem 2.21 this will at least occur frequently and as mentioned above is always true for a perfect automaton. The next problem is that of determining all automata (to within isomorphism) which are the image of a given automaton under an operation preserving function. This corresponds to the group theory problem of determining all homomorphs of a given group. Unfortunately a device as convenient as the invariant subgroup does not seem to be available for automata. Finally, the resolution of this problem should shed some light on the problem of determining the factors of a given (strongly connected) automaton since the factors will be included in this class.

LIST OF REFERENCES

1. Turing, A. M., "On computable numbers with an application to entscheidungs problem", Preceedings London Math. Soc., Vol. 41, pp. 230-265; Nov. 1936.

2. Mealy, G. H., "A method for synthesizing sequential circuits", Bell Systems Technical Journal, Vol. 34, pp. 1045-1079; Sept. 1955.

3. Moore, E. F., "Gedanken-experiments on sequential machines", Automata Studies, Princeton, pp. 129-153(1956).

4. Ginsburg, S., "On the reduction of superfluous states in sequential machines", Jour. Assoc. Computing Mach., Vol. 6, pp. 259-282 (1959).

5. Rabin, M. O., and Scott, D., "Finite Automata and their decision problems", IBM Journal of Research and development, Vol. 3, pp. 114-125; April 1959.

6. Ginsburg, S., "Some remarks on abstract machines", Trans. Amer. Math. Soc. 96(1960), 400-444.

7. Weeg, G. P., "The structure of an automaton and its operation preserving transformation group", J. ACM 9, 5(July 1962), pp. 345-349.

8. Fleck, A. C., "Structure preserving properties of certain classes of functions on automata", presented at the summer meeting of Amer. Math. Soc., 1961 (582-17).

9. Hocking, J. G. and Young, G. S., Topology, Addison-Wesley Publishing Co., Reading, Mass., 1961.

10. Fleck, A. C., "Isomorphism groups of automata", Jour. Assoc. Computing Mach., Vol. 9, No. 4, pp. 469-476 (1962).

11. Weeg, G. P., "Some group theoretic properties of strongly connected automata", Unpublished research at the Computer Laboratory, Michigan State University; May, 1961.

12. Clifford, A. H., and Preston, G. B., "The algebraic theory of semigroups", Mathematical Surveys, No. 7, Amer. Math. Soc.(1961).