1974

Algebraic Properties Of Some Classes Of Automata And Languages

Mu-lo Wang

ALGEBRAIC PROPERTIES OF SOME CLASSES OF AUTOMATA AND LANGUAGES

by

Mu-Lo Wang
Department of Mathematics

Submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Graduate Studies
The University of Western Ontario
London, Canada
May 1974

ABSTRACT

The object of this thesis is to study the algebraic properties of some classes of automata and languages.

The following classes of automata are investigated:

(i) right prime automata,

(ii) left prime automata,

(iii) duo automata,

(iv) globally abelian automata.

(i) is a generalization of permutation automata, while (ii) generalizes the concept of a strongly connected automaton. Both (iii) and (iv) are generalizations of abelian automata. Chapter 2 is devoted to the study of these classes. It is shown that the transition monoids of right prime automata are dual to those of left prime automata.

The structure of the transition monoids of various automata is studied in Chapter 3. It is shown that a finite monoid M is the transition monoid of a left prime automaton if and only if the automaton $A_M = (M, M)$ is a subdirect product of strongly connected M-automata, and that the transition monoid of a finite duo automaton is a subdirect product of a finite number of monoids, each of which is either a group or a group union a nilpotent ideal.

Also proved are some properties of the transition monoids of finite globally abelian automata.

In Chapter 4, the families of languages accepted by right prime and left prime acceptors are studied. Some algebraic properties are obtained for these families of languages.

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to my research advisor Professor Gabriel Thierrin for suggesting the topic of this research and for his supervision and encouragement.

I avail myself of this opportunity to thank Dr. Clive M. Reis and Dr. Allan G. Heinicke for reading the manuscript and for their valuable suggestions which improved the present thesis considerably.

Last, I express my sincere gratitude and thanks to Mrs. Lai-Yee K. Cha for her devotion of considerable personal time and effort to the seemingly endless task of typing.

TABLE OF CONTENTS

INTRODUCTION

The point of view adopted in this thesis is that automata can be considered as algebraic systems. In fact, they can be considered as a generalization of monoids. Thus we may take an algebraic approach to the study of automata.

We adopt the following definition: Let M be a monoid with identity 1. An automaton over M (or an M-automaton) is a triple $A = (S, M, \eta)$ where S is a nonempty set of states and η is a homomorphism of M into the transformation monoid T_S of S, such that $1\eta = 1_S$, the identity mapping on S. The image of M under η is a submonoid of T_S, called the transition monoid of A and denoted by T(A). For simplicity, we write

$$(s)a\eta = (s)a = sa \quad \text{for } s \in S.$$

When there is no possibility of ambiguity, we denote A by $A = (S, M)$. A particular but important example of M-automata is the automaton $A_M = (M, M, \eta)$ where, for each $a \in M$, $a\eta = \rho_a$, the inner right translation of M corresponding to a. In this case, we have $T(A_M) \cong M$.

An M-automaton $A = (S, M)$ is (i) a permutation automaton if every $a \in M$ is a permutation on S, (ii) strongly connected if M, and therefore T(A), acts transitively on S, i.e., for any $s, t \in S$, there exists $a \in M$ such that $sa = t$ and (iii) abelian if $sab = sba$ for all $s \in S$ and $a, b \in M$.

Generalizations of the above three classes of automata are the objects of study in this thesis.

Chapter 1 contains a review of some basic concepts and properties of semigroups and automata, which are to be used throughout this thesis.

In sections 2.1 and 2.2, right prime and left prime automata are introduced and studied. They are shown to be generalizations of permutation automata and strongly connected automata respectively. Moreover, it is shown that the transition monoids of right prime automata are dual to those of left prime automata. Two generalizations of abelian automata, namely duo automata and globally abelian automata, are studied in Section 2.3, while in Section 2.4, relations among the previously defined automata are investigated.

The structure of the transition monoids of left prime automata, duo automata and globally abelian automata is studied in Chapter 3. It is shown that a finite monoid M is the transition monoid of a finite left prime automaton if and only if the automaton $A_M = (M, M)$ is a subdirect product of strongly connected M-automata, and that the transition monoid of a finite duo automaton is a subdirect product of a finite number of monoids, each of which is either a group or a group union a nilpotent ideal. Also proved are some properties of the transition monoids of finite globally abelian automata.

In Chapter 4, we consider the families of languages accepted by right prime and left prime acceptors. They are called RP-regular languages and LP-regular languages respectively. It is shown that they are both boolean algebras.

CHAPTER 1

BASIC CONCEPTS

The purpose of this chapter is two-fold: first, to introduce basic concepts to be used throughout this thesis and to establish some fundamental theorems derived from them; secondly, to introduce some special classes of automata, based upon which generalizations will be made in later chapters.

1.1. Semigroups and Related Concepts

A *semigroup* is a set with an associative binary operation. By a *nontrivial semigroup* we mean a semigroup T with $|T| > 1$, where $|T|$ denotes the number of elements of T. A *monoid* is a semigroup with identity.

Let X be any set. A *transformation* on X is a single-valued mapping of X into itself. We shall denote the image of an element x of X under a transformation α by $(x)\alpha$ or $x\alpha$. The set T_X of all transformations on X forms a monoid under composition of mappings.

Let θ be a mapping of a set X into a set Y. Then the relation $\theta\circ\theta^{-1}$ defined on X by $x \equiv y \pmod{\theta\circ\theta^{-1}}$ if $x\theta = y\theta$ is an equivalence relation on X.

Let T be a semigroup. An equivalence relation ρ on

T is a *right congruence* if for any $a, b, c \in T$, $a \equiv b \pmod{\rho}$ implies $ac \equiv bc \pmod{\rho}$. A *left congruence* is defined dually and a *congruence* is a relation which is a right congruence and a left congruence. Thus an equivalence relation ρ on T is a congruence if and only if for any $a, b, c, d \in T$, $a \equiv b \pmod{\rho}$ and $c \equiv d \pmod{\rho}$ imply $ac \equiv bd \pmod{\rho}$. Let ρ be a congruence on T and let T/ρ be the quotient set modulo ρ: $T/\rho = \{\bar{a} \mid a \in T\}$ where $\bar{a}$ is the ρ-class containing a. If we define $\bar{a}\cdot\bar{b} = \overline{ab}$, then T/ρ becomes a semigroup called the *quotient* or *factor semigroup* of T modulo ρ. The mapping $\rho^{\#}$ of T onto T/ρ defined by $a\rho^{\#} = \bar{a}$, is the *natural* or *canonical homomorphism* of T upon T/ρ. Thus every quotient semigroup of a semigroup T is a homomorphic image of T.

Conversely, let ϕ be a homomorphism of a semigroup T into a semigroup N. It can be shown that the relation $\phi\circ\phi^{-1}$ is a congruence on T and $T/\phi\circ\phi^{-1} \cong T\phi$. Therefore every homomorphic image of T is isomorphic to a quotient semigroup of T.

Let X be a nonempty set and X^{+} be the set of all nonempty finite sequences of elements of X. If $x_1x_2\dots x_n$ and $y_1y_2\dots y_m$ are two elements of X^{+}, we define their product by concatenation

$$(x_1\dots x_n)\cdot(y_1\dots y_m) = x_1\dots x_n y_1\dots y_m$$

Then X^{+} becomes a semigroup called the *free semigroup* generated by X. The elements of X are called *letters* and the elements of X^+ are called *words* over X. The *length* $|w|$ of a word $w \in X^+$ is the number of elements of X occurring in w. A word with zero length is called the *empty word* and denoted by Λ. Let $X^* = X^+ \cup \{\Lambda\}$. Then $w\Lambda = \Lambda w = w$ for all $w \in X^*$ and X^* is a monoid called the *free monoid* generated by X.

A nonempty finite set is called an *alphabet*. If X is an alphabet, then X^* is called the free monoid generated by the alphabet X.

1.2. *Automata and Their Transition Monoids*

Let M be a monoid with identity 1. An *automaton* over M (or an *M-automaton*) is a triple $A = (S, M, \eta)$ where S is a nonempty set of states and η is a homomorphism of M into the transformation monoid T_S of S, such that $1\eta = 1_S$ the identity mapping on S. If $A = (S, M, \eta)$ is an automaton over M then M is the *input monoid* of the automaton A. For simplicity, we shall identify the element $a \in M$ with its image $a\eta$ and write $(s)a\eta = (s)a = sa$, for $s \in S$. Thus for all $s \in S$ and $a, b \in M$, $s \cdot 1 = s$ and $s(ab) = (sa)b$. When no ambiguity will arise, we denote A by $A = (S, M)$ leaving η to be understood.

An automaton $A = (S, M)$ is *finite* if S is finite; *trivial* if $|S| = 1$.

In particular, if A is an automaton over a free monoid X^* generated by an alphabet X, then we write

$A = (S, X)$ and call A a free input automaton (abbreviated as f.i. automaton) over the alphabet X. The class of f.i. automata is an important class of automata, which plays a prominent role in Automata Theory.

One particular and important M-automaton is the automaton $A_M = (M, M) = (M, M, \eta)$ where for each $a \in M$, $a\eta = \rho_a$ the right inner translation of M corresponding to a. By the use of this special case, many properties of semigroups can be reduced to properties of M-automata and conversely, the results concerning M-automata can be applied to give results concerning semigroups.

Let $A = (S, M, \eta)$ be an automaton. The image of M under η is a submonoid of T_S, called the transition monoid of A and denoted by $T(A)$, the identity of $T(A)$ being 1_S. Therefore we have

$$T(A) = M\eta \cong M/\eta\circ\eta^{-1}.$$

For every $s \in S$, we define a relation E_s on M by $a \equiv b \pmod{E_s}$ if $sa = sb$. Clearly, E_s is a right congruence on M. Let $E_S = \bigcap_{s \in S} E_s$. Then E_S is a congruence on M. For any $a, b \in M$, we have $a \equiv b \pmod{E_S}$ if and only if $sa = sb$ for all $s \in S$ if and only if $a = b$ if and only if $a \equiv b \pmod{\eta\circ\eta^{-1}}$. Hence

$$M/E_S \cong M/\eta\circ\eta^{-1} \cong T(A).$$

If S is finite, then E_S is of finite index. Consequently the transition monoid of a finite automaton is finite.

For the automaton $A_M = (M, M)$, the congruence

E_M is the equality congruence since M is a monoid. Thus $T(A_M) = M$.

A finite automaton A = (S, M) is often described by means of a table; the transition or next state table:

A	... a ...
⋮	⋮
s	... sa
⋮	

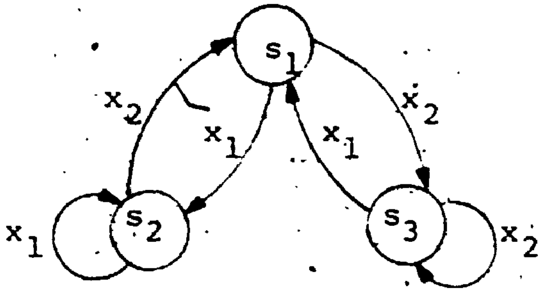
where $s \in S$ and $a \in M$.

For a finite f.i. automaton A = (S, X) over an alphabet X, we merely put the elements of X and the corresponding sa for $a \in X$ on the table. For example, let $A = (S, X, \eta)$ be an f.i. automaton over $X = \{x_1, x_2\}$ with $S = \{s_1, s_2, s_3\}$ and

$x_1\eta = \begin{pmatrix} s_1, & s_2, & s_3 \\ s_2, & s_2, & s_1 \end{pmatrix}$, $x_2\eta = \begin{pmatrix} s_1, & s_2, & s_3 \\ s_3, & s_1, & s_3 \end{pmatrix}$. Then A can be represented by the following transition table:

A	x_1	x_2
s_1	s_2	s_3
s_2	s_2	s_1
s_3	s_1	s_3

Another representation of a finite automaton A = (S, M) is the representation using a directed graph. The vertices of the graph represent the states of A and for every $s, t \in S$ such that $sa = t$, $a \in M$, an arrow labelled a leads from s to t. For the above example, we have



1.3. Homomorphisms and Congruences

Let $A = (S, M, \eta)$ and $B = (S', M, \delta)$ be M-automata. A mapping h(written on the left of the argument)of S into S' is an M-homomorphism (or a homomorphism) of A into B if for every $a \varepsilon M$ and $s \varepsilon S$, we have $(h(s))a\delta = h((s)a\eta)$. If h is one-to-one, then h is an M-monomorphism of A into B. If there is an M-homomorphism of A onto B, then B is a homomorphic image of A; further, A and B are isomorphic if there exists an M-monomorphism of A onto B; if so, we write $A \cong B$.

Let $B = (S', M, \delta)$ be a homomorphic image of an automaton $A = (S, M, \eta)$ under the homomorphism h. Define a mapping ϕ of T(A) into T(B) by $(a\eta)\phi = a\delta$ where $a \varepsilon M$. If $a\eta = b\eta$, then $s(a\eta) = s(b\eta)$ for all $s \varepsilon S$ and $h((s)a\eta) = h((s)b\eta)$ for all $s \varepsilon S$, i.e., $(hs)(a\delta) = (hs)(b\delta)$ for all $s \varepsilon S$. Since h is onto, the above implies $(t)a\delta = (t)b\delta$ for all $t \varepsilon S'$. Hence $a\delta = b\delta$ and ϕ is well-defined. Moreover, ϕ is a homomorphism. For $(a\eta)(b\eta)\phi = ((ab)\eta)\phi = (ab)\delta = (a\delta)(b\delta) = (a\eta)\phi\cdot(b\eta)\phi$.

Clearly, Φ is onto. Therefore Φ is a homomorphism of T(A) onto T(B). This proves the following proposition (cf.[11]).

Proposition 1.3.1.. If the automaton B = (S', M) is a homomorphic image of the automaton A = (S, M), then the transition monoid T(B) of B is homomorphic to the transition monoid T(A) of A. #

Let A = (S, M) be an automaton. An equivalence relation π on the state set S of A is an S-congruence (or a congruence) of A if $s \equiv t \pmod{\pi}$ implies $sa \equiv ta \pmod{\pi}$ for all $a \in M$. It is obvious that the equality relation on S is an S-congruence of A, which will be denoted by 0; and that the universal relation on S is also an S-congruence on S, which will be denoted by ω.

Let π be a congruence of A = (S, M) and $\overline{S} = S/\pi$ be the quotient set of S modulo π. The pair $\overline{A} = (\overline{S}, M)$ becomes an automaton if we define

$$\overline{s}a = \overline{sa} \qquad \text{for } a \in M$$

where $\overline{s}$ denotes the π-class containing s, and $\overline{A}$ is called the quotient or factor automaton of A modulo π, denoted by A/π. The mapping $\pi^{\#}$ of S onto $\overline{S}$ such that $\pi^{\#}s = \overline{s}$ is the natural or canonical homomorphism of A upon A/π. Thus every quotient automaton of an automaton A is a homomorphic image of A.

For the converse, we have the following version (see [3]) of the Main Homomorphism Theorem valid for semigroups (see [2]).

Theorem 1.3.2. (Main Homomorphism Theorem). Let h be an S-homomorphism of an M-automaton $A = (S, M)$ upon an M-automaton $A' = (S', M)$. Let $\pi = h \circ h^{-1}$. Then π is an S-congruence on A and there exists an M-isomorphism f of A/π upon A' such that $f\pi^{\natural} = h$. #

The generalized version of the Induced Homomorphism Theorem for semigroups (see [2]) is as follows (see [3]).

Theorem 1.3.3. (Induced Homomorphism Theorem). Let h_1 and h_2 be M-homomorphisms of an M-automaton $A = (S, M, \eta)$ upon M-automata $A_1 = (S_1, M, \eta_1)$ and $A_2 = (S_2, M, \eta_2)$ respectively and such that $h_1 \circ h_1^{-1} \leq h_2 \circ h_2^{-1}$. Then there exists a unique M-homomorphism f of A_1 upon A_2 such that $fh_1 = h_2$. #

Corollary. If ρ_1 and ρ_2 are S-congruences on an automaton $A = (S, M)$ such that $\rho_1 \leq \rho_2$, then A/ρ_2 is a homomorphic image of A/ρ_1. #

Let $A = (S, M, \eta)$ be an automaton. A subautomaton (or an M-subautomaton) of A is an automaton $B = (S', M, \eta')$ where S' is a nonempty subset of S and for each $a \in M$, $a\eta' = a\eta|_{S'}$.

An S-ideal (or ideal) of A is a nonempty subset I of S such that $I(M\eta) = IM \subseteq I$. Any subset of the form sM where $s \in M$ is an S-ideal of A. It can be shown that an M-automaton $B = (S', M, \eta')$ is a subautomaton of an

M-automaton $A = (S, M, \eta)$ if and only if S' is an S-ideal of A.

Let $A = (S, M)$ be an automaton. A state $s \varepsilon S$ is called *zero* or *null* if $sa = s$ for all $a \varepsilon M$. Clearly, the set $Z(A) = \{s \varepsilon S | sa = s \text{ for all } a \varepsilon M\}$ of all zero states of A is an S-ideal of A. An automaton $A = (S, M)$ is *null* if $S = Z(A)$. Every trivial automaton is a null automaton.

Let I be an S-ideal of A. The relation $\rho(I)$ defined on S by

$$s \equiv t \ (\text{mod } \rho(I)) \text{ if either } s, t \varepsilon I \text{ or } s = t,$$

is an S-congruence called the *Rees congruence* modulo I. The quotient automaton $A/\rho(I)$ is the *Rees quotient automaton* modulo I, often denoted by A/I. Evidently, I is a zero state of A/I.

For an ideal I with $|I| > 1$, the corresponding Rees congruence $\rho(I) \neq 0$ and I is the only nonsingleton class of $\rho(I)$.

Let $A_1 = (S_1, M), \ldots, A_n = (S_n, M)$ be M-automata. By the *direct product* $A = A_1 \times \ldots \times A_n = \prod_{i=1}^{n} A_i$ of $A_1, \ldots, A_n$, we mean the automaton $A = (S, M)$ where $S = \prod_{i=1}^{n} S_i$ and $(s_1, \ldots, s_n)a = (s_1a, \ldots, s_na)$ for $a \varepsilon M$. If $s = (s_1, \ldots, s_i, \ldots, s_n)$, then s_i is the ith component of s. The mapping π_i of S onto S_i, defined by $\pi_i(s) = s_i$, is the ith *projection homomorphism* of A onto the component A_i. Any automaton isomorphic to A is also called the direct product of the automata $A_1, \ldots, A_n$.

An automaton C is a *subdirect product* of the automata $A_1, \ldots, A_n$ if C is isomorphic to a subautomaton $B = (S', M)$ of $\prod_{i=1}^{n} A_i$, which has the property that $\pi_i S' = S_i$ for all $i = 1, \ldots, n$.

An automaton A is *irreducible* if it has the property: When A is expressed as a subdirect product, then at least one of the components is isomorphic to A.

An S-congruence μ of an automaton A is the *least proper congruence* of A if (i) $\mu \neq 0$, (ii) for every S-congruence μ' of A, $\mu' \neq 0$, we have $\mu \leq \mu'$.

The following theorems are special versions of two theorems valid for universal algebra (see [1]). For the proofs of these theorems, the reader is referred to [11].

The first theorem gives the relation between subdirect products and S-congruences.

Theorem 1.3.4. An automaton A is a subdirect product of automata $A_1, \ldots, A_n$ if and only if A contains a family of S-congruences $\rho_1, \ldots, \rho_n$ such that $\bigcap_{i=1}^{n} \rho_i = 0$ and A/ρ_i is isomorphic to A_i for each i. #

In view of this theorem, the following conditions on a nontrivial finite automaton A are equivalent (see [12]).

(i) A is irreducible.

(ii) The intersection of nonequality congruences of A is nonequality.

(iii) A has a least proper congruence.

The second is the following fundamental theorem.

Theorem 1.3.5. Every finite automaton is a subdirect product of irreducible automata. #

Recall that for an M-automaton $A = (S, M)$, the congruence E_S induced by A on M is defined as $a \equiv b \pmod{E_S}$ if $sa = sb$ for all $s \in S$.

Lemma 1.3.6. If an automaton $A = (S, M)$ is a subdirect product of automata $A_1 = (S_1, M), \ldots, A_n = (S_n, M)$, then

$$E_S = \bigcap_{i=1}^{n} E_{S_i}.$$

Proof. Let $a, b \in M$ and $a \equiv b \pmod{E_S}$. Then $ta = tb$ for all $t \in S$. Since A is a subdirect product of $A_1, \ldots, A_n$, it follows that for each $i = 1, \ldots, n$, $\pi_i S = S_i$ where π_i is the ith projection homomorphism. Therefore for each $i = 1, \ldots, n$, if $s_i \in S_i$, then there exists $s \in S$ such that $\pi_i(s) = s_i$. But $sa = sb$ so that

$$s_i a = \pi_i(s)a = \pi_i(sa) = \pi_i(sb) = \pi_i(s)b = s_i b;$$

hence $a \equiv b \pmod{E_{S_i}}$. Consequently, $E_S \leq \bigcap_{i=1}^{n} E_{S_i}$.

Conversely, if $a \equiv b \pmod{\bigcap_{i=1}^{n} E_{S_i}}$, then for each $i = 1, \ldots, n$, $s_i a = s_i b$ for all $s_i \in S_i$. Let $s \in S$. Then $s = (s_1, \ldots, s_n)$ where $s_i \in S_i$, $i = 1, \ldots, n$. We have

$$sa = (s_1, \ldots, s_n)a = (s_1 a, \ldots, s_n a) = (s_1 b, \ldots, s_n b)$$
$$= (s_1, \ldots, s_n)b = sb.$$

Thus $a \equiv b \pmod{E_S}$ and $E_S \geq \bigcap_{i=1}^{n} E_{S_i}$. Therefore $E_S = \bigcap_{i=1}^{n} E_{S_i}$. #

Theorem 1.3.7. If an automaton $A = (S, M)$ is a subdirect product of automata $A_1 = (S_1, M), \ldots, A_n = (S_n, M)$, then the transition monoid $T(A)$ of A is a subdirect product of the transition monoids $T(A_i)$ of A_i, $i = 1, \ldots, n$.

Proof. Let $T = T(A)$ and $T_i = T(A_i)$, $i = 1, \ldots, n$. For every $a \in M$ and each $i = 1, \ldots, n$, let $\bar{a}$ and $\bar{a}^{(i)}$ be, respectively, the E_S-class and E_{S_i}-class containing a. Then

$$T = \{\bar{a} | a \in M\} \text{ and } T_i = \{\bar{a}^{(i)} | a \in M\} \quad i = 1, \ldots, n.$$

Define a mapping $\phi: T \to \prod_{i=1}^{n} T_i$ by $\phi(\bar{a}) = (\bar{a}^{(1)}, \ldots, \bar{a}^{(n)})$. Then we have the following:

1. ϕ is well-defined.

For if $\bar{a} = \bar{b}$, then $a \equiv b \pmod{E_S}$. By Lemma 1.3.6, $a \equiv b \pmod{E_{S_i}}$ for all $i = 1, \ldots, n$. This implies $\bar{a}^{(i)} = \bar{b}^{(i)}$ for all $i = 1, \ldots, n$. Hence $\phi(a) = \phi(b)$.

2. ϕ is a semigroup homomorphism.

Since $\phi(\bar{a}\bar{b}) = \phi(\overline{ab}) = (\overline{ab}^{(1)}, \ldots, \overline{ab}^{(n)})$ and

$$\begin{aligned} \phi(a)\phi(b) &= (\bar{a}^{(1)}, \ldots, \bar{a}^{(n)})(\bar{b}^{(1)}, \ldots, \bar{b}^{(n)}) \\ &= (\bar{a}^{(1)}\bar{b}^{(1)}, \ldots, \bar{a}^{(n)}\bar{b}^{(n)}) \\ &= (\overline{ab}^{(1)}, \ldots, \overline{ab}^{(n)}). \end{aligned}$$

Therefore $\phi(\bar{a}\bar{b}) = \phi(\bar{a})\phi(\bar{b})$.

3. ϕ is one to one.

If $\bar{a} \neq \bar{b}$, then $a \not\equiv b \pmod{E_S}$. But $E_S = \bigcap_{i=1}^{n} E_{S_i}$ by

Lemmma 1.3.6. Therefore $a \not\equiv b \pmod{E_{S_i}}$ for some $i = 1, \ldots, n$. Thus $\bar{a}^{(i)} \neq \bar{b}^{(i)}$ and $\phi(\bar{a}) \neq \phi(\bar{b})$.

4. For each $i = 1, \ldots, n$, the composition $\pi_i\phi$ is onto.

For if $\bar{a}^{(i)} \in T_i$, then $a \in M$. Evidently, $\bar{a} \in T$ and $\pi_i\phi(a) = \bar{a}^{(i)}$.

Therefore T is a subdirect product of $T_1, \ldots, T_n$. #

1.4. Permutation Automata and Strongly Connected Automata

An automaton $A = (S, M)$ is a permutation automaton if every $a \in M$ is a permutation on S.

If $A = (S, M)$ is a finite automaton, then it is obvious that the following conditions on A are equivalent.

(i) A is a permutation automaton.

(ii) For $s, t \in S$, $sa = ta$ where $a \in M$, implies $s = t$.

(iii) For every $a \in M$, we have $Sa = S$.

In general, we have the following result.

Proposition 1.4.1. Let $A = (S, M)$ be an automaton with transition monoid $T = T(A)$. If A is a permutation automaton, then T is cancellative. Conversely if T is a group, then A is a permutation automaton.

Proof. The first statement follows from the fact that in this case, T is a submonoid of the permutation group on S.

Conversely, if T is a group, then the identity of T must be 1_S. Thus for every $a \in M$, $a\eta \in T$ and there exists $(a\eta)^{-1} \in T$ such that

$$(a\eta)(a\eta)^{-1} = (a\eta)^{-1}(a\eta) = 1_S.$$

Since 1_S is bijective so is $a\eta$. Hence $a\eta$ is a permutation on S and A is a permutation automatom. #

The following corollary is a well-known result in finite automata theory.

Corollary. A finite automaton A is a permutation automaton if and only if its transition monoid T(A) is a group. #

Let A be a finite permutation automaton. Then T(A) is a group. If π is an S-congruence of A, then the quotient automaton A/π is a homomorphic image of A. By Proposition 1.3.1, the transition monoid $T(A/\pi)$ is a homomorphic image of T(A) which is a group. Hence $T(A/\pi)$ is also a group. This implies that A/π is a permutation automaton. We conclude in the following.

Proposition 1.4.2. A finite automaton A is a permutation automaton if and only if every quotient automaton of A is a permutation automaton. #

A state s of an automaton A = (S, M) is a generator of A if sM = S.

An automaton A = (S, M) is

(i) cyclic or connected if A contains a generator;

(ii) strongly connected or transitive if M, and therefore T(A), acts transitively on S; or equivalently, for every $s, t \in S$, there exists $x \in M$ such that $sx = t$;

(iii) locally transitive if for each $s \in S$ and $a \in M$ there exists $x \in M$ such that $sax = s$.

It can be easily seen that every strongly connected automaton is locally transitive but not conversely. Moreover, the following three conditions are equivalent.

(i) $A = (S, M)$ is strongly connected.

(ii) A is cyclic and every state is a generator.

(iii) S is the only S-ideal of A.

Let τ be an S-congruence of a strongly connected automaton $A = (S, M)$. Let $\bar{s}, \bar{t} \in \bar{S} = S/\tau$. Then $s, t \in S$ and there exists $a \in M$ such that $sa = t$ which implies $\bar{s}a = \bar{t}$. Therefore $\bar{A} = A/\tau$ is also strongly connected and we have thus proved the following proposition.

Proposition 1.4.3. An automaton A is strongly connected if and only if every quotient automaton of A is strongly connected. #

An S-ideal I of an automaton $A = (S, M)$ is minimal if $J \subseteq I$ where J is an S-ideal, implies $J = I$. Two distinct minimal S-ideals are disjoint.

Thierrin has shown in [13] that a finite automaton $A = (S, M)$ is locally transitive if and only if the state set S is the union of the minimal S-ideals.

On the other hand, every finite permutation automaton is locally transitive since its transition monoid is a group. Consequently, if $A = (S, M)$ is a finite permutation automaton, then S is the union of minimal S-ideals of A.

An automaton $A = (S, M)$ is <u>abelian</u> if for all $s \in S$ and $a, b \in M$ we have $sab = sba$. It is immediate that the transition monoid of an abelian automaton is abelian and that every f.i. automaton $A = (S, X)$ with $|X| = 1$ is abelian.

<u>Proposition 1.4.4</u>. Every strongly connected and abelian automaton is a permutation automaton.

<u>Proof</u>. Let $A = (S, M)$ be a strongly connected and abelian automaton. Using Proposition 1.4.1, it suffices to show that $T(A)$ is a group.

Let $a \in T(A)$ and fix $s_0 \in S$. Then $s_0 a \in S$ and there exists $x \in T(A)$ such that $s_0ax = s_0$ since A is strongly connected. Similarly if $s \in S$, then there exists $b \in T(A)$ such that $s = s_0b$. Since A is abelian, we obtain

$$sax = (s_0b)ax = (s_0ax)b = s_0b = s.$$

Thus $ax = 1_S$ the identity in $T(A)$ and $T(A)$ is a group. #

<u>Proposition 1.4.5</u>. Every finite cyclic permutation automaton is strongly connected.

<u>Proof</u>. Let $A = (S, M)$ be a finite cyclic permutation automaton with generator s_0. Then $s_0M = S$. To show that A is strongly connected, it suffices to show $s_0 \in sM$ for all $s \in S$. For then we have $sM \supseteq s_0M = S$ and $sM = S$ for

all $s \in S$. Let $s \in S$. Since s_0 is a generator, there exists $a \in M$ such that $s = s_0 a = (s_0)a\eta$. By the Corollary to Proposition 1.4.1, $T(A)$ is a group. Therefore $(a\eta)^{-1}$ exists and hence $s_0 = (s_0)(a\eta)(a\eta)^{-1} = s(a\eta)^{-1}$. Let $b \in M$ such that $b\eta = (a\eta)^{-1}$. Then we have $s_0 = sb$. This completes the proof. #

Proposition 1.4.6. Let M be a monoid. Then the following statements are equivalent.

(i) $A_M = (M, M)$ is a strongly connected automaton.

(ii) $A_M = (M, M)$ is a permutation automaton.

(iii) M is a group.

Proof. The automaton A_M is strongly connected if and only if $sM = M$ for all $s \in M$. This is equivalent to M being right simple. But every right simple monoid is a group. This proves the equivalence of (i) and (iii).

On the other hand, A_M is a permutation automaton if and only if M is right cancellative and $Ma = M$ for all $a \in M$. This is equivalent to M being right cancellative and left simple. By duality, the equivalence of (ii) and (iii) is established. #

1.5. Acceptors and Regular Languages

Let X be an alphabet and X^* be the free monoid generated by X. Then every subset L of X^* is called a (formal) language over the alphabet X.

An *acceptor* or *recognizer* over an alphabet X is a quintuple $\hat{A} = (S, X, \delta, s_0, F)$ where $A = (S, X, \delta)$ is a finite f.i. automaton over X; $s_0 \in S$ is the *initial state* and $F \subseteq S$ is the *set of final states*.

A word $x \in X^*$ is *accepted* or *recognized* by $\hat{A}$ if $(s_0)x\delta \in F$. The set $L(\hat{A}) = \{x \mid x \in X^*, (s_0)x\delta \in F\}$ of all words over X accepted by $\hat{A}$ is called the *language accepted or recognized by $\hat{A}$*.

A language U over an alphabet X is *regular* if there exists an acceptor $\hat{A} = (S, X, \delta, s_0, F)$ over X such that $U = L(\hat{A})$.

An acceptor $\hat{A} = (S, X, \delta, s_0, F)$ is *cyclic* or *connected* if the initial state s_0 is a generator of the automaton $A = (S, X, \delta)$.

Two acceptors $\hat{A}$ and $\hat{B}$ over the same alphabet X are *equivalent* if $L(\hat{A}) = L(\hat{B})$.

Proposition 1.5.1. For every regular language U over an alphabet X, there exists a connected acceptor accepting U.

Proof. Let $U = L(\hat{A})$ where $\hat{A} = (S, X, \delta, s_0, F)$. Take $\hat{B} = (S', X, \delta', s_0, F')$ where $S' = s_0X^*$, $\delta' = \delta|_{S'}$ and $F' = F \cap S'$, then clearly $\hat{B}$ is connected and $U = L(\hat{B})$. #

Corollary. Every acceptor is equivalent to a connected acceptor. #

For any language U over an alphabet X, we define a relation P_U on X^* by $a \equiv b \pmod{P_U}$ if $uav \in U$ if and only if $ubv \in U$ where $u, v \in X^*$. It is immediate that P_U is a congruence on X^*. The quotient monoid X^*/P_U is called the <u>syntactic monoid</u> of U and denoted by S(U). Syntactic monoids play an important role in Formal Language Theory, as many languages are characterized by the structure of their syntactic monoids. For example, we have the following fundamental characterization of regular languages.

<u>Theorem 1.5.2</u>. Let X be an alphabet. A language U over X is regular if and only if its syntactic monoid S(U) is finite. #

For the proof of the above theorem, the reader is referred to [6].

CHAPTER 2

GENERALIZATIONS OF SOME AUTOMATA

In this chapter, we consider generalizations of permutation automata, strongly connected automata and abelian automata.

Section 1 is devoted to a generalization of permutation automata, which we call right prime automata; in Section 2 we study left prime automata, a generalization of strongly connected automata. In Section 3, we consider two different generalizations of abelian automata, which we call duo automata and globally abelian automata respectively. Finally, in Section 4, we investigate some relations among these special classes of automata. In each case, particular results are mentioned for finite automata; and possible applications to semigroup theory are also indicated.

Throughout this chapter, we shall adopt the following notation: for any M-automaton A = (S, M, η), denote $a\eta = \bar{a}$ where $a \in M$. Thus elements of T(A) are of the form $\bar{a}$ where $a \in M$.

2.1. Right Prime Automata

An M-automaton A = (S, M) is a right prime automaton if for any s, t ε S and a ε M, sxa = txa for all x ε M implies s = t. This is equivalent to saying that if s, t ε S with s $\neq$ t, then for every a ε M, there exists x_a ε M such that $sx_aa \neq tx_aa$. Every trivial automaton is trivially right prime.

Recall that if A = (S, M) is a permutation automaton, then for any s, t ε S and a ε M, sa = ta implies s = t. Therefore the following is obvious.

Lemma 2.1.1. Every permutation automaton is right prime. #

Let A = (S, M) be an automaton. An input a ε M is a reset input if $|Sa| = 1$. The set of all reset inputs of A is denoted by R(A) = {a ε M | $|Sa| = 1$}. For the automaton A_M = (M, M), R(A_M) is the set of right zeros of M.

Proposition 2.1.2. Let A = (S, M) be a nontrivial right prime automaton. Then R(A) = Ø.

Proof. Suppose R(A) $\neq$ Ø and a ε R(A), then $|Sa| = 1$. Since $|S| > 1$, there exist s, t ε S such that s $\neq$ t. But sxa = txa for all x ε M, contrary to A being right prime. #

An f.i. automaton A = (S, X) over an alphabet X is k-definite for some positive integer k, if every word w ε X* with length $|w| \geq k$ is a reset input. An f.i. automaton is definite if it is k-definite for some positive integer k.

As an immediate corollary to the above proposition, we have the following.

Corollary. A definite automaton cannot be right prime. #

Let $A = (S, M)$ be an automaton and N a left ideal of the monoid M. Define a relation $\pi(N)$ on S by

$$s \equiv t \ (\text{mod } \pi(N)) \text{ if } sx = tx \text{ for all } x \in N.$$

Since N is a left ideal of M, it can be shown that $\pi(N)$ is an S-congruence of A called the S-congruence induced by N and the corresponding $A/\pi(N)$ is called the quotient automaton of A induced by N.

The following proposition concerns a characterization of right prime automata.

Proposition 2.1.3. The following conditions on an automaton $A = (S, M)$ are equivalent.

(i) A is right prime.

(ii) For every left ideal N of M, the induced congruence $\pi(N)$ is the equality.

Proof. (i) implies (ii). Let N be a left ideal of M. Suppose $s \equiv t \ (\text{mod } \pi(N))$, then $sx = tx$ for all $x \in N$. If $a \in N$, then $Ma \subseteq N$. Hence $sya = tya$ for all $y \in M$ so that $s = t$ since A is right prime, proving $\pi(N) = 0$.

(ii) implies (i). Suppose for some $s, t \in S$ and $a \in M$, $sxa = txa$ for all $x \in M$. Let $N = Ma$. The above implies $s \equiv t \ (\text{mod } \pi(N))$. Since N is a left ideal of M, by hypothesis $\pi(N) = 0$. Thus $s = t$ and A is right prime. #

Corollary. The following conditions on a finite automaton

$A = (S, M)$ are equivalent.

(i) A is right prime.

(ii) For every left ideal N of M, the induced congruence $\pi(N)$ is the equality.

(iii) For every left ideal N of M, the quotient automaton $A/\pi(N)$ induced by N is isomorphic to A. #

If the monoid M contains minimal left ideals, then we have the following.

Proposition 2.1.4. Let M be a monoid with minimal left ideals and $A = (S, M)$ be an M-automaton. Then the following are equivalent.

(i) A is right prime.

(ii) For every minimal left ideal N of M, the induced congruence $\pi(N)$ is the equality.

Proof. (i) implies (ii) by Proposition 2.1.3.

(ii) implies (i). Suppose N is a minimal left ideal of M and suppose $sxa = txa$ for all $x \in M$. Let $b \in N$. Then $sxab = txab$ for all $x \in M$. But $N = \{xab | x \in M\} = Mab$ since N is a minimal left ideal of M. Therefore $sy = ty$ for all $y \in N$. Hence $s \equiv t \pmod{\pi(N)}$ and $s = t$ since $\pi(N) = 0$. #

Corollary. Let $A = (S, M)$ be a finite automaton with transition monoid $T(A)$. Then the following are equivalent.

(i) A is right prime.

(ii) For every minimal left ideal N of $T(A)$, the induced congruence $\pi(N)$ is the equality.

(iii) For every minimal left ideal N of T(A), the quotient automaton $A/\pi(N)$ induced by N is isomorphic to A. #

We now consider an example of right prime automaton.

Example 2.1.5. Let A = (S, X) be the f.i. automaton over X = {a, b} with S = {1, 2, 3} and the following transition table:

A	a	b
1	2	1
2	1	2
3	1	1

Straighforward calculation gives the transition monoid $T(A) = \{\bar{\Lambda}, \bar{a}, \bar{b}, \bar{a}^2, \overline{ba}\}$ with the following multiplication table:

T(A)	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$	$\bar{a}^2$	$\overline{ba}$
$\bar{\Lambda}$	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$	$\bar{a}^2$	$\overline{ba}$
$\bar{a}$	$\bar{a}$	$\bar{a}^2$	$\bar{a}$	$\bar{a}$	$\bar{a}^2$
$\bar{b}$	$\bar{b}$	$\overline{ba}$	$\bar{b}$	$\bar{b}$	$\overline{ba}$
$\bar{a}^2$	$\bar{a}^2$	$\bar{a}$	$\bar{a}^2$	$\bar{a}^2$	$\bar{a}$
$\overline{ba}$	$\overline{ba}$	$\bar{b}$	$\overline{ba}$	$\overline{ba}$	$\bar{b}$

The only minimal left ideal of T(A) is $N = \{\bar{a}, \bar{b}, \bar{a}^2, \overline{ba}\}$. From the following table,

	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$	$\bar{a}^2$	$\overline{ba}$
1	1	2	1	1	2
2	2	1	2	2	1
3	3	1	1	2	2

it is easily seen that $\pi(N) = 0$. Therefore A is right prime. #

It is clear that the above automaton is not a permutation automaton. Thus, *right prime automata properly generalize permutation automata*.

Let T be a semigroup. If T has an identity, set $T^1 = T$, and if T has no identity, let T^1 be the semigroup T with an identity, usually denoted by 1, adjoined.

By a *right prime semigroup* we mean a semigroup T in which for any $a, b, c \in T$, $axc = bxc$ for all $x \in T^1$ implies $a = b$; or equivalently, if $a, b \in T$ with $a \neq b$, then for every $c \in T$ there exists $x_c \in T^1$ such that $ax_cc \neq bx_cc$. It is obvious that every right cancellative semigroup is right prime.

An equivalence relation π on a semigroup T is *right prime* if for any $a, b, c \in T$, $axc \equiv bxc \pmod{\pi}$ for all $x \in T^1$ implies $a \equiv b \pmod{\pi}$. Thus a congruence π on a semigroup T is right prime if and only if the corresponding quotient semigroup T/π is a right prime semigroup.

Proposition 2.1.6. Let $A = (S, M)$ be a right prime automaton. Then the transition monoid $T(A)$ of A is right prime.

Proof. Recall that there is a congruence E_S defined on M by $a \equiv b \pmod{E_S}$ if $sa = sb$ for all $s \in S$ and that

$T(A) \simeq M/E_S$. Therefore in view of the above remark, it suffices to show that E_S is a right prime congruence on M.

Let $a, b, c \in M$ and $axc \equiv bxc \pmod{E_S}$ for all $x \in M$. Then for all $s \in S$, $saxc = sbxc$ for all $x \in M$, i.e., for all $s \in S$, $(sa)xc = (sb)xc$ for all $x \in M$. Hence for all $s \in S$, $sa = sb$ since A is right prime. Therefore $a \equiv b \pmod{E_S}$ and E_S is right prime. #

Corollary 1. Let M be a monoid. The automaton $A_M = (M, M)$ is right prime if and only if the monoid M is right prime.

Proof. The sufficiency is obvious, while the necessity follows from the fact that $T(A_M) = M$. #

Corollary 2. Any nontrivial right prime monoid contains no right zeros.

Proof. This follows from the Proposition and Proposition 2.1.2. #

Proposition 2.1.7. If T is a right cancellative semigroup, then T^1 is right prime.

Proof. If $T^1 = T$, then it is trivial.

If $T^1 = T \cup \{1\}$, we shall show that if $a, b \in T^1$ with $a \neq b$, then for every $c \in T^1$ there exists $x_c \in T^1$ such that $ax_c c \neq bx_c c$. We consider the following two cases.

case i. If $a \neq 1$ and $b = 1$, then there exists $x \in T$ such that $ax \neq x$. For otherwise $ay = y$ for all $y \in T$. Moreover, $yay = y^2$ so that $ya = y$ since T is right cancellative. This implies that a is an identity in T, a contradiction.

Therefore $ax \neq x$ for some $x \in T$ and $axc \neq 1xc$ for all $c \in T^1$.

case ii. If $a, b \in T$, then $ac \neq bc$ for all $c \in T^1$ since T is right cancellative. #.

Remark. Any semigroup obtained from a group with an identity adjoined is not right prime. e.g. $T = \{e, a\} \cup \{1\}$ where $\{e, a\}$ is a group, then $1xe = exe$ for all $x \in T^1$ but $1 \neq e$.

Let M be a monoid and A_R be the family of right prime M-automata. We now consider some closure properties of this family A_R. Clearly, every subautomaton of a right prime automaton is right prime. However, a homomorphic image of a right prime automaton need not be right prime, as the following example shows.

Example 2.1.8. Let A be the right prime automaton of Example 2.1.5. Let $\pi = \{\overline{1,2}, \overline{3}\}$. Then π is an S-congruence of A. The quotient automaton $A/\pi = (\overline{S}, X)$ where $\overline{S} = \{\overline{1}, \overline{3}\}$ and $X = \{a, b\}$ has the following transition table:

A/π	a	b
$\overline{1}$	$\overline{1}$	$\overline{1}$
$\overline{3}$	$\overline{1}$	$\overline{1}$

Thus $a, b \in R(A/\pi)$ and $R(A/\pi) \neq \emptyset$. By Proposition 2.1.2, the automaton A/π is not right prime. #

However, A_R is closed under taking subdirect products. To show this, we need the following definition and lemma.

An S-congruence π of an automaton $A = (S, M)$ is right prime if the quotient automaton A/π is right prime. Thus an automaton is right prime if and only if the equality, considered as an S-congruence, is right prime.

Proposition 2.1.9. The intersection of right prime S-congruences of an automaton $A = (S, M)$ is right prime.

Proof. Let $\pi = \bigcap_{\alpha \varepsilon I} \pi_\alpha$ where π_α is a right prime S-congruence of A for all $\alpha \varepsilon I$. It is clear that π is an S-congruence of A. Suppose for some $s, t \varepsilon S$ and $a \varepsilon M$ we have $sxa \equiv txa \pmod{\pi}$ for all $x \varepsilon M$. Then for all $\alpha \varepsilon I$, $sxa \equiv txa \pmod{\pi_\alpha}$ for all $x \varepsilon M$. Since π_α is right prime for all $\alpha \varepsilon I$, hence $s \equiv t \pmod{\pi_\alpha}$ for all $\alpha \varepsilon I$. Therefore $s \equiv t \pmod{\pi}$ and π is right prime. #

Corollary. Every subdirect product of right prime automata is right prime.

Proof. This follows immediately from the Proposition and Theorem 1.3.4. #

We conclude with the following.

Proposition 2.1.10. The family A_R contains trivial automata, is closed under taking subautomata and subdirect products. But A_R is not closed under taking homomorphic images. #

In the following let $A = (S, M)$ be an arbitrary automaton and ρ be the intersection of right prime S-congruences of A. Then by Proposition 2.1.9, ρ is right prime. Moreover, ρ has the following universal property.

Proposition 2.1.11. Let $A = (S, M)$ be an automaton, $B = (S', M)$ be a right prime automaton and h be an M-homomorphism of A into B. Then there exists a unique M-homomorphism f of A/ρ into B such that $f\rho^{\natural} = h$.

Proof. Since h is an M-homomorphism of A into B, $h \circ h^{-1}$ is an S-congruence on A such that $A/h \circ h^{-1} \cong h(A)$, which is a subautomaton of B. By hypothesis, B is right prime so that $h(A)$ is right prime and $h \circ h^{-1}$ is a right prime S-congruence of A. This implies $\rho \leq h \circ h^{-1}$. Applying Theorem 1.3.3, we obtain the desired homomorphism f. #

The above S-congruence ρ is called the least right prime congruence of A and A/ρ is the greatest right prime homomorphic image of A. Moreover, A is right prime if and only if $\rho = 0$.

2.2. Left Prime Automata

An automaton $A = (S, M)$ is a left prime automaton if for any $a, b \in M$ and $s_0 \in S$, $s_0xa = s_0xb$ for all $x \in M$ implies $sa = sb$ for all $s \in S$, i.e., $a \equiv b \pmod{E_S}$.

In general, left prime automata ~~are not~~, in the strict sense, dual to right prime automata. They do, however, give rise to transition monoids dual to the transition monoids of right prime automata. Only in the case $A_M = (M, M)$, where M is a monoid, the notions of left and right prime-ness are dual to each other.

First, we shall show that left prime automata generalize strongly connected automata.

Lemma 2.2.1. Every strongly connected automaton is left prime.

Proof. Let $A = (S, M)$ be a strongly connected automaton. Then $sM = S$ for all $s \varepsilon S$. Suppose for some $a, b \varepsilon M$ and $s_0 \varepsilon S$, $s_0xa = s_0xb$ for all $x \varepsilon M$. Then $sa = sb$ for all $s \varepsilon S$ since $s_0M = S$. Therefore A is right prime. #

Recall that for an automaton $A = (S, M)$, $Z(A) = \{s \varepsilon S | sa = s$ for all $a \varepsilon M\}$ denotes the set of zero states of A.

Proposition 2.2.2. Let $A = (S, M)$ be a nonnull left prime automaton. Then $Z(A) = \emptyset$.

Proof. Suppose $Z(A) \neq \emptyset$ and $s_0 \varepsilon Z(A)$. Then $s_0m = s_0$ for all $m \varepsilon M$. By hypothesis, $S \neq Z(A)$. Let $t \varepsilon S - Z(A)$. Then there exist $a, b \varepsilon M$ such that $ta \neq tb$. But $s_0xa = s_0 = s_0xb$ for all $x \varepsilon M$ so that $sa = sb$ for all $s \varepsilon S$ since A is left prime. In particular, $ta = tb$, a contradiction. #

Let H be a nonempty set of states of an automaton $A = (S, M)$. The quotient $H : s$ of H by $s \varepsilon S$ is defined by

$$H : s = \{x \varepsilon M | sx \varepsilon H\},$$

and the *residue* W_H of H is defined by

$$W_H = \{s \in S\ H : s = \emptyset\}.$$

If $s \in W_H$, then $H : s = \emptyset$. Further, $H : sx = \emptyset$ for all $x \in M$. For otherwise, $H : sa \neq \emptyset$ for some $a \in M$ implies the existence of $b \in M$ such that $sab \in H$ so $ab \in H : s$ and $H : s \neq \emptyset$, contrary to $s \in W_H$. Consequently, $sx \in W_H$ for all $x \in M$ and W_H is an S-ideal.

A nonempty subset H of S is *disjunctive* if $H : s = H : t$ implies $s = t$; *neat* if $H : s \neq \emptyset$ for all $s \in S$. A state $s \in S$ is *disjunctive* if $\{s\}$ is a disjunctive set; *neat* if $\{s\}$ is a neat set.

Lemma 2.2.3. Let $A = (S, M)$ be a nonnull left prime automaton. If H is a disjunctive set, then H is neat and every S-ideal of A meets H.

Proof. Since A is nonnull and left prime, hence $Z(A) = \emptyset$ by Proposition 2.2.2.

Let W_H be the residue of H. Then $|W_H| \leq 1$. For if $s, t \in W_H$, then $H : s = \emptyset = H : t$ so that $s = t$ since H is disjunctive.

Suppose H is not neat and $H : s = \emptyset$ for some $s \in S$, then $s \in W_H$. Thus $W_H = \{s\}$. But W_H is an S-ideal, therefore $sx = s$ for all $x \in M$. This implies $s \in Z(A)$, a contradiction. Thus H is neat.

Finally, let I be an S-ideal of A and $s \in I$. Then $sM \subseteq I$. On the other hand, H is neat hence $H : s \neq \emptyset$.

Thus there exists $a \in M$ such that $sa \in H$. But $sa \in sM \subseteq I$. Therefore $I \cap H \neq \emptyset$. #

Proposition 2.2.4. Let $A = (S, M)$ be a nonnull automaton. If A is left prime and has disjunctive states, then every disjunctive state is neat. Moreover, there is a unique minimal S-ideal and every disjunctive state is contained in the minimal S-ideal.

Proof. Let s be a disjunctive state. By Lemma 2.2.3, s is neat and every S-ideal meets $\{s\}$. Thus s is contained in every S-ideal, and the intersection of all S-ideals of A is not empty. Clearly, this intersection is the unique minimal S-ideal which contains every disjunctive state. #

Corollary. If $A = (S, M)$ is a nonnull left prime automaton such that every state is disjunctive, then A is strongly connected.

Proof. By the Proposition, every state is neat. Thus for every $s, t \in S$, $s : t \neq \emptyset$. This implies that for every $s, t \in S$ there exists $x \in M$ such that $tx = s$. Therefore A is strongly connected. #

Let $A = (S, M)$ be an automaton and $B = (I, M)$ a subautomaton of A. Then $I \subseteq S$ and the following relation holds.

$$E_S = \bigcap_{s \in S} E_s \leq \bigcap_{t \in I} E_t = E_I.$$

Consequently, M/E_I is homomorphic to M/E_S, hence the transition monoid $T(B)$ is homomorphic to the transition monoid T(A).

We now characterize left prime automata.

Proposition 2.2.5. The following conditions on an automaton $A = (S, M)$ are equivalent.

(i) A is left prime.

(ii) For every S-ideal I of A, $E_I = E_S$.

Proof. (i) implies (ii). In view of the above remark, it suffices to show $E_I \leq E_S$. Suppose $a \equiv b \pmod{E_I}$, we have $ta = tb$ for all $t \in I$. Let $t_0 \in I$. Then $t_0M \subseteq I$. Thus the above yields $t_0xa = t_0xb$ for all $x \in M$ so that $a \equiv b \pmod{E_S}$ since A is left prime.

(ii) implies (i). Suppose for some $a, b \in M$ and $s_0 \in S$, $s_0xa = s_0xb$ for all $x \in M$. Let $I = s_0M$. Then I is an S-ideal of A and $a \equiv b \pmod{E_I}$. But $E_I = E_S$. Hence $a \equiv b \pmod{E_S}$ and A is left prime. #

Corollary. The following conditions on a finite automaton $A = (S, M)$ are equivalent.

(i) A is left prime.

(ii) For every S-ideal I of A, $E_I = E_S$.

(iii) For every subautomaton $B = (I, M)$ of A, the transition monoid T(B) of B is isomorphic to the transition monoid T(A) of A.

Proof. The equivalence of (i) and (ii) follows from the Proposition. Moreover, we observe that $B = (I, M)$ is a subautomaton of A if and only if I is an S-ideal of A, and that $T(A) \simeq M/E_S$ and $T(B) \simeq M/E_I$. If A is finite, then

$M/E_S \cong M/E_I$ is equivalent to saying that $E_S = E_I$. Thus the equivalence of (ii) and (iii) follows. #

The following is an example of a left prime automaton.

Example 2.2.6. Let $A = (S, X)$ be the f.i. automaton over $X = \{a, b, c\}$ with $S = \{1, 2, 3, 4\}$ and the following transition table:

A	a	b	c
1	1	4	4
2	1	3	4
3	1	2	4
4	1	1	4

Then $I = \{1, 4\}$ is the only proper S-ideal of A. It is easy to check that $E_I = E_S$. Therefore A is left prime. #

Clearly, the above automaton is not strongly connected. Thus left prime automata properly generalize strongly connected automata.

The dual concept of a right prime semigroup is provided below.

A semigroup T is left prime if for any $a, b, c \in T$, $cxa = cxb$ for all $x \in T^1$ implies $a = b$. Or equivalently, if $a, b \in T$ with $a \neq b$, then for all $c \in T$ there exists $x_c \in T^1$ such that $cx_ca \neq cx_cb$. It is obvious that every left cancellative semigroup is left prime.

Remark. A concept slightly different from a left prime semigroup, called a weakly left cancelling semigroup, is defined by Hoehnke [5] as a semigroup T in which for all a, b_1, b_2 ε T, if $asb_1 = asb_2$ for all s ε T^1 and if $b_1 \neq b_2$, then a is a left zero of T. It is evident that a weakly left cancelling semigroup without left zeros is precisely what a left prime semigroup is.

An equivalence relation π on a semigroup T is left prime if for any a, b, c ε T, cxa ≡ cxb (mod π) for all x ε T^I implies a ≡ b (mod π). Thus a congruence π on a semigroup T is left prime if and only if the corresponding quotient semigroup T/π is a left prime semigroup.

In the discussion of the duality of the notions of right prime semigroup and left prime semigroup, the following concept will be useful.

Let (T, ∘) be a semigroup with operation ∘. Define a new operation * on T by a*b = b∘a. It is clear that (T, *) is also a semigroup. Moreover, the dual of any expression or concept which holds in (T, ∘) will hold in (T, *). For convenience we shall call (T, *) the dual semigroup of (T, ∘).

Thus a semigroup is left prime if and only if its dual semigroup is right prime; and vice versa. However, this kind of duality does not extend to the notions of right prime and left prime automata, except for the special automaton A_M as we have mentioned before.

Clearly the dual of Proposition 2.1.7 holds and has the following form.

defined by Hoehnke [5] as a semigroup T in which for all a, b_1, $b_2 \varepsilon T$, if $asb_1 = asb_2$ for all $s \varepsilon T^1$ and if $b_1 \neq b_2$, then a is a left zero of T. It is evident that a weakly left cancelling semigroup without left zeros is precisely what a left prime semigroup is.

An equivalence relation π on a semigroup T is left prime if for any a, b, c ε T, cxa $\equiv$ cxb (mod π) for all $x \varepsilon T^1$ implies a $\equiv$ b (mod π). Thus a congruence π on a semigroup T is left prime if and only if the corresponding quotient semigroup T/π is a left prime semigroup.

In the discussion of the duality of the notions of right prime semigroup and left prime semigroup, the following concept will be useful.

Let (T, $\circ$) be a semigroup with operation $\circ$. Define a new operation * on T by a*b = b$\circ$a. It is clear that (T, *) is also a semigroup. Moreover, the dual of any expression or concept which holds in (T, $\circ$) will hold in (T, *). For convenience we shall call (T, *) the dual semigroup of (T, $\circ$).

Thus a semigroup is left prime if and only if its dual semigroup is right prime, and vice versa. However, this kind of duality does not extend to the notions of right prime and left prime automata, except for the special automaton A_M as we have mentioned before.

Clearly the dual of Proposition 2.1.7 holds and has the following form.

Proposition 2.2.7. If T is a left cancellative semigroup, then T^1 is left prime. #

Proposition 2.2.8. Let $A = (S, M)$ be a left prime automaton. Then the transition monoid $T(A)$ is left prime.

Proof. Suppose for some $\bar{a}, \bar{b}, \bar{c} \in T = T(A)$, $\bar{c}\bar{x}\bar{a} = \bar{c}\bar{x}\bar{b}$ for all $\bar{x} \in T$. Then for any $s_0 \in S$, $s_0\bar{c}\bar{x}\bar{a} = s_0\bar{c}\bar{x}\bar{b}$ for all $\bar{x} \in T$. This implies $s_0cya = s_0cyb$, i.e., $(s_0c)ya = (s_0c)yb$ for all $y \in M$. Since $s_0c \in S$ and A is left prime, it follows that $sa = sb$ for all $s \in S$ and $\bar{a} = \bar{b}$. Therefore $T(A)$ is left prime. #

Corollary 1. The congruence E_S on a monoid M induced be a left prime M-automaton $A = (S, M)$ is left prime. #

Corollary 2. The transition monoid of a strongly connected automaton is left prime. #

Corollary 3. Let M be a monoid. Then $A_M = (M, M)$ is left prime if and only if M is left prime. #

Corollary 4. Every nontrivial left prime monoid contains no left zeros.

Proof. This follows from Propositions 2.2.8 and 2.2.2. #

The following is an example of a left prime monoid.

Lemma 2.2.9. Let U be a set with $|U| > 1$ and T_U the transformation monoid on U. Then T_U is a left prime monoid.

Proof. Suppose for some $a, b, c \in T_U$, $cxa = cxb$ for all $x \in T_U$. Then for every $u \in U$, $(u)cxa = (u)cxb$ for all $x \in T_U$. For each $u \in U$, let x_u be the constant transformation such that $(v)x_u = u$ for all $v \in U$. Then for every $u \in U$, $(u)a = (ucx_u)a = (u)(cx_ua) = (u)(cx_ub) = (ucx_u)b = (u)b$. Therefore $a = b$ and T_U is left prime. #

Corollary. Every semigroup can be embedded in a left prime semigroup.

Proof. Let T be any semigroup. It is well-known (see [2]) that T can be embedded in T_T1. Moreover T_T1 is left prime by the lemma. #

By this lemma and the Corollary 3 to Proposition 2.2.8, the automaton $A_T = (T, T)$ where $T = T_U$ for some U with $|U| > 1$ is left prime. Moreover, T_U is not a group, thus A_T is not a strongly connected automaton (see Proposition 1.4.6). Dually, the automaton A_T, where T' is the dual semigroup of T is right prime and not a permutation automaton.

Let M be a monoid and A_L be the family of left prime automata over M. This family A_L possesses the same closure properties as A_R. Clearly, every subautomaton of a left prime automaton is left prime. But homomorphic images of left prime automata need not be left prime as verified below.

Example 2.2.10. Let $A = (S, X)$ be the f.i. automaton over $X = \{a, b\}$ with $S = \{1, 2, 3, 4, 5, 6\}$ and the following transition table:

A	a	b
1	1	3
2	3	1
3	2	2
4	4	6
5	6	4
6	5	5

It can be checked that $T(A) = \{\overline{\Lambda}, \overline{a}, \overline{b}, \overline{ab}, \overline{ba}, \overline{b}^2\}$. There are two S-ideals, namely $I_1 = \{1, 2, 3\}$ and $I_2 = \{4, 5, 6\}$. From the following table,

	$\overline{\Lambda}$	$\overline{a}$	$\overline{b}$	$\overline{ab}$	$\overline{ba}$	$\overline{b}^2$
1	1	1	3	3	2	2
2	2	3	1	2	1	3
3	3	2	2	1	3	1
4	4	4	6	6	5	5
5	5	6	4	5	4	6
6	6	5	5	4	6	4

it is easily seen that $E_{I_1} = E_{I_2} = E_S$. By Proposition 2.2.4, A is left prime. But the Rees quotient A/I_1 which is a homomorphic image of A is not left prime since I_1 is a zero state of A/I_1 (see Proposition 2.2.2). #

We now show that A_L is closed under taking subdirect products. First, we consider the following definition.

An S-congruence π of an automaton $A = (S, M)$ is <u>left prime</u> if the quotient automaton A/π is left prime. Thus an automaton A is left prime if and only if the equality congruence of A is left prime.

<u>Proposition 2.2.11</u>. The intersection of left prime S-congruences of an automaton $A = (S, M)$ is left prime.

<u>Proof</u>. Let $\pi = \bigcap_{\alpha\in I} \pi_\alpha$ where π_α is a left prime congruence

of A for each $\alpha \in I$. Clearly, π is an S-congruence of A. We shall show that π is also left prime.

Suppose for some a, b $\in$ M and $s_0 \in S$, $s_0xa \equiv s_0xb \pmod{\pi}$ for all x $\in$ M, then for all $\alpha \in I$, $s_0xa \equiv s_0xb \pmod{\pi_\alpha}$ for all x $\in$ M. Since π_α is left prime for all $\alpha \in I$, therefore for all $\alpha \in I$, sa $\equiv$ sb $(\text{mod } \pi_\alpha)$ for all s $\in$ S. This implies sa $\equiv$ sb $(\text{mod } \pi)$ for all s $\in$ S, and π is left prime. #

<u>Corollary</u>. Every subdirect product of left prime automata is left prime.

<u>Proof</u>. This follows immediately from the Proposition and Theorem 1.3.4. #

We conclude with the following.

<u>Proposition 2.2.12</u>. The family A_L contains trivial automata; is closed under taking subautomata and subdirect products; but not closed under taking hombmorphic images. #

Now let A = (S, M) be an arbitrary automaton and σ be the intersection of left prime S-congruences of A. Then by Proposition 2.2.11, σ is left prime. Moreover, σ has the following universal property, which is analogous to Proposition 2.1.11.

<u>Proposition 2.2.13</u>. Let A = (S, M) be an automaton, B = (S', M) be a left prime automaton and h be an M-homomorphism of A into B. Then there exists a unique

M-homomorphism f of A/σ into B such that $f\sigma^{\natural} = h$.

Proof. Since h is an M-homomorphism of A into B, $h \circ h^{-1}$ is an S-congruence on A such that $A/h \circ h^{-1} \cong h(A)$, which is a subautomaton of B. By hypothesis, B is left prime so that $h(A)$ is left prime and $h \circ h^{-1}$ is a left prime S-congruence of A. This implies $\sigma \leq h \circ h^{-1}$. Applying Theorem 1.3.3, we obtain the desired homomorphism f. #

The above S-congruence σ is called the least left prime congruence of A and A/σ the greatest left prime homomorphic image of A. Moreover, A is left prime if and only if $\sigma = 0$.

2.3. Duo Automata and Globally Abelian Automata

Recall that an automaton $A = (S, M)$ is abelian if $sab = sba$ for all $s \in S$ and $a, b \in M$.

A generalization of abelian automata is provided below.

An automaton $A = (S, M)$ is duo if for $a, b \in M$, there exist $x, y \in M$ such that $sab = sxa = sby$ for all $s \in S$. This is equivalent to saying that for every $\bar{a}, \bar{b} \in T(A)$, there exist $\bar{x}, \bar{y} \in T(A)$ such that $\bar{a}\bar{b} = \bar{x}\bar{a} = \bar{b}\bar{y}$. Thus the transition monoid $T = T(A)$ of a duo automaton A has the property: $\bar{a}T = T\bar{a}$ for all $\bar{a} \in T$. This suggests the following concept. A semigroup T is a duo semigroup if $aT = Ta$ for every $a \in T$. Clearly, every group is duo.

The following is obvious.

Proposition 2.3.1. An automaton $A = (S, M)$ is a duo automaton if and only if its transition monoid $T(A)$ is a duo monoid. #

Corollary. The automaton $A_M = (M, M)$ is duo if and only if the monoid M is duo. #

It is clear that every abelian automaton is duo. The following shows another example of duo automata.

Proposition 2.3.2. Every finite permutation automaton is duo.

Proof. Let A be a finite permutation automaton. Then by the Corollary to Proposition 1.4.1, its transition monoid $T(A)$ is a group which is duo. Therefore by Proposition 2.3.1, A is duo. #

Proposition 2.3.3. Let T be a duo monoid. If e is an idempotent element of T, then e is in the center of T.

Proof. Since T is duo, $eT = Te$. Thus for each $x \in T$ there exists $y \in T$ such that $ex = ye$. Hence $exe = yee = ye = ex$. By symmetry, $exe = xe$. Therefore $xe = ex$ for all $x \in T$ and e is in the center of T. #

Corollary. Any automaton which contains two distinct resets cannot be duo.

Proof. Let $A = (S, M)$ be an automaton. If $z \in M$ is a reset, then $|Sz| = 1$ and $\bar{z}$ is an idempotent in $T = T(A)$.

Moreover, $\bar{a}\bar{z} = \bar{z}$ for all $\bar{a} \varepsilon T$. Thus if $z_1, z_2 \varepsilon M$ are two distinct resets, then

$$\bar{z}_1\bar{z}_2 = \bar{z}_2 \neq \bar{z}_1 = \bar{z}_2\bar{z}_1$$

so that $\bar{z}_1$ and $\bar{z}_2$ are not in the center of T. Therefore T is not duo by the above Proposition. Consequently A is not duo by Proposition 2.3.1. #

Proposition 2.3.4. Let A = (S, M) be a duo automaton. Then the set Sa is an S-ideal for all a ε M.

Proof. Let s ε Sa and x ε M. Then s = ta for some t ε S. Since A is duo, there exists y ε M such that sx = tax = tya ε Sa. Therefore Sa is an S-ideal. #

We now consider another generalization of abelian automata.

An automaton A = (S, M) is globally abelian if Sab = Sba for all a, b ε M. It is obvious that every abelian automaton is globally abelian and that the automaton A_M = (M, M) is globally abelian if and only if M satisfies the property: Mab = Mba for all a, b ε M.

If A = (S, M) is a permutation automaton, then Sa = S for all a ε M. This implies Sab = Sba for all a, b ε M, so that A is globally abelian. Thus we have proved the following:

Proposition 2.3.5. Every permutation automaton is globally abelian. #

Proposition 2.3.6. If A = (S, M) is a globally abelian automaton, then $\bar{e}\bar{a} = \bar{e}\bar{a}\bar{e}$ for every idempotent $\bar{e} \in T(A)$ and every $\bar{a} \in T(A)$.

Proof. Let $\bar{e} \in T(A)$ be an idempotent and $\bar{a} \in T(A)$ be arbitrary. By hypothesis, Sea = Sae. Therefore for each $s \in S$, there exists $t \in S$ such that sea = tae. But then seae = tae and sea = seae. Thus $\bar{e}\bar{a} = \bar{e}\bar{a}\bar{e}$. #

Proposition 2.3.7. Let A = (S, M) be a globally abelian automaton. Then the set Sa is an S-ideal for all $a \in M$.

Proof. Let $s \in Sa$. Then s = ta for some $t \in S$. If $x \in M$, we have $sx = tax \in Sax = Sxa \subseteq Sa$. Therefore $sx \in Sa$ and Sa is an S-ideal. #

The notion of globally abelian automaton is different from that of duo automaton as we can see in the following example.

Example 2.3.8. Let A = (S, X) be the f.i. automaton over X = {a, b} with S = {1, 2, 3, 4} and the following transition table:

	a	b
1	3	3
2	3	1
3	4	1
4	1	4

It can be checked that Sx = {1, 3, 4} for all $x \in X^*$. Thus Sxy = Syx for all $x, y \in X^+$ and A is globally abelian. On the other hand, $\bar{b}^2 \in T(A)$ is an idempotent and $\bar{b}^2 \cdot \bar{a} \neq \bar{a} \cdot \bar{b}^2$. This implies that $\bar{b}^2$ is not in the center of T(A). By Proposition 2.3.3, T(A) is not duo. Hence A is not duo by Proposition 2.3.1.

2.4. Relations Among Some Classes of Finite Automata

We shall now investigate some relations among the following classes of finite automata:

1. permutation automata,
2. strongly connected automata,
3. locally transitive automata,
4. right prime automata,
5. left prime automata,
6. abelian automata,
7. duo automata,
8. globally abelian automata.

Before doing so, we need the following concept.

A semigroup T is left(right) simple if Ta = T (aT = T) for all a ε T. It is known (see [2]) that every left(right) simple monoid is a group.

Lemma 2.4.1. Let T be a finite semigroup. If Te = T (eT = T) for every idempotent e ε T, then T is left(right) simple.

Proof. Since T is finite, for every a ε T there exists a positive integer n such that $a^n = e$ is an idempotent. Thus $Ta \supseteq Ta^n = Te = T$. Therefore Ta = T and T is left simple. #

Corollary. Let T be a finite monoid. If Te = T(eT = T) for every idempotent $e \in T$, then T is a group. #

Proposition 2.4.2. Every finite, duo, right prime monoid is a group.

Proof. Let T be a finite, duo, right prime monoid. If $e \in T$ is an idempotent, then e is in the center of T by Proposition 2.3.3. Hence xeye = xye for all $x, y \in T$. But T is right prime so that xe = x for all $x \in T$ and Te = T. Since T is a finite monoid, it follows by the Corollary to Lemma 2.4.1, that T is a group. #

Corollary 1. A finite automaton A = (S, M) is a permutation automaton if and only if it is duo and right prime.

Proof. The necessity follows from Propositions 2.1.1 and 2.3.2. Conversely, the transition monoid T(A) of A is a finite, duo, right prime monoid by Propositions 2.3.1 and 2.1.6. Thus T is a group by the proposition and A is a permutation automaton by Proposition 1.4.1. #

Corollary 2. Every finite, abelian, right prime automaton is a permutation automaton. #

Corollary 3. Let A = (X, M) be a finite f.i. automaton with $|X| = 1$. Then A is right prime if and only if A is a permutation automaton.

Proof. The necessity is obvious, while the sufficiency follows from Corollary 2 since A is abelian when $|X| = 1$. #

The following is an example of globally abelian, right prime automaton which is not a permutation automaton.

Example 2.4.3. Let A = (S, M) be the globally abelian f.i. automaton of Example 2.3.8, whose transition table is as follows:

A	a	b
1	3	3
2	3	1
3	4	1
4	1	4

It can be checked that A is right prime. However, A is clearly not a permutation automaton. #

The dual of Proposition 2.4.2 is also true and has the following form.

Proposition 2.4.4. Every finite, duo, left prime monoid is a group. #

Corollary 1. Every finite, duo, left prime automaton is a permutation automaton.

Proof. By Propositions 2.3.1 and 2.2.8, the transition monoid T(A) of a finite, duo, left prime automaton A is a finite, duo, left prime monoid. Thus T(A) is a group by the proposition. It then follows from Proposition 1.4.1 that A is a permutation automaton. #

Corollary 2. Every finite, abelian, left prime automaton is a permutation automaton. #

Corollary 3. Every finite, left prime, f.i. automaton A = (X, M) with |X| = 1 is a permutation automaton.

Proof. This follows from Corollary 1, since A is abelian when $|X| = 1$. #

The following example shows that the converse of the above proposition is not true.

Example 2.4.5. Let $A = (S, X)$ be the f.i. automaton over $X = \{a, b\}$ with $S = \{1, 2, 3, 4\}$ and the following transition table:

A	a	b
1	3	1
2	4	4
3	1	3
4	2	2

Then A is a permutation automaton. But A is not left prime, since $(1)xa = (1)xab$ for all $x \in X^*$ and $(2)a \neq (2)ab$. #

Proposition 2.4.6. Let A be a finite duo cyclic automaton. Then the following are equivalent.

(i) A is a permutation automaton.

(ii) A is right prime.

(iii) A is strongly connected.

(iv) A is left prime.

Proof. The equivalence of (i) and (ii) follows from Proposition 2.4.2; (i) implies (iii) by Proposition 1.4.5; (iii) implies (iv) by Lemma 2.2.1. and (iv) implies (i) by Proposition 2.4.4. #

Corollary. Let A be a finite, abelian, cyclic automaton.

Then the following are equivalent.

(i) A is a permutation automaton.

(ii) A is right prime.

(iii) A is strongly connected.

(iv) A is left prime. #

Proposition 2.4.7. Every finite, left prime, globally abelian automaton is a permutation automaton.

Proof. Let A = (S, M) be a finite, left prime, globally abelian automaton. Then by Proposition 2.2.8, the transition monoid T = T(A) is left prime. Moreover, if $\bar{e} \varepsilon T$ is an idempotent, then $\overline{ex} = \overline{exe}$ for all $\bar{x} \varepsilon T$ by Proposition 2.3.6. Thus we obtain, for every $\bar{x}$, $\bar{y} \varepsilon T$,

$$\overline{exy} = \overline{exey} = \overline{exeye} = \overline{exye}.$$

Therefore $\bar{y} = \overline{ye}$ for all $\bar{y} \varepsilon T$, since T is left prime. That is $T = T\bar{e}$ so that T is a group by the Corollary to Lemma 2.4.1. #

Corollary. Every strongly connected and globally abelian automaton is a permutation automaton. #

Remark. The automaton A of Example 2.4.5 shows that the converse of Proposition 2.4.7 is not true.

Proposition 2.4.8. Let A be a finite, cyclic, globally abelian automaton. Then the following are equivalent.

(i) A is a permutation automaton.

(ii) A is strongly connected.

(iii) A is left prime.

Proof. (i) implies (ii) by Proposition 1.4.5; (ii) implies (iii) by Lemma 2.2.1. and (iii) implies (i) by Proposition 2.4.7. #

Remarks. 1. A finite, cyclic, globally abelian, right prime automaton need not be a permutation automaton; for example, let A = (S, X) be the globally abelian, right prime f.i. automaton of Example 2.4.3. It is clear that A is cyclic with 2 as a generator. But A is not a permutation automaton.

2. A left prime permutation automaton need not be strongly connected. For example, let A = (S, X) be the left prime permutation f.i. automaton of Example 2.2.10, where X = {a, b}, S = {1, 2, 3, 4, 5, 6} and A has the following transition table:

A	a	b
1	1	3
2	3	1
3	2	2
4	4	6
5	6	4
6	5	5

It is clear that A is not strongly connected since $(1)X^* = \{1, 2, 3\} \neq S$.

This example also shows that a duo left prime automaton or a globally abelian left prime automaton need not be strongly connected. #

Proposition 2.4.9. A finite automaton $A = (S, M)$ is a permutation automaton if and only if it is globally abelian and locally transitive.

Proof. Clearly a permutation automaton is globally abelian and locally transitive. Conversely, suppose $A = (S, M)$ is globally abelian and locally transitive. Then for any $a \in M$ and $s \in S$, there exists $b \in M$ such that $sab = s$. Thus $s \in Sab = Sba \subseteq Sa$. Therefore $S \subseteq Sa$ so $S = Sa$. Since S is finite and $\bar{a}$ maps S onto S, $\bar{a}$ is a permutation on S. #

The above proposition suggests the question: when does a finite automaton have a permutation subautomaton? This is not true in general; for example, there are strongly connected automata which are not permutation automata, and these have no proper subautomata. We shall show (Corollary to Lemma 2.4.13) that a finite globally abelian automaton does always contain a permutation subautomaton.

Proposition 2.4.10. Let $A = (S, M)$ be a finite automaton. If $B = (S', M)$ is a permutation subautomaton of A, then S' is the union of the minimal S-ideals contained in S'.

Proof. Let $s \in S'$. Since A is finite, the S-ideal sM contains a minimal S-ideal, I say. Then $sa \in I$ for some $a \in M$. But $\bar{a}$ is a permutation on S', so for some positive integer n, $\bar{a}^n$ is the identity map on S'. Thus $s = (s\bar{a})\bar{a}^{n-1} \in I$. This completes the proof. #

Remark. This proposition generalizes the result that for every finite permutation automaton $A = (S, M)$, the state set S is the union of minimal S-ideals.

Lemma 2.4.11. Let $A = (S, M)$ be a finite automaton with transition monoid $T = T(A)$. Let $a \in M$ and let n be a positive integer such that $\bar{a}^n$ is an idempotent in T. Then $\bar{a}$ is a permutation on $S\bar{e}$.

Proof. Since S is finite, it suffices to show $(S\bar{e})\bar{a} = S\bar{e}$. We may assume $n \neq 1$, for otherwise the assertion is clear. Since $\bar{e} = \bar{a}^n$, we have $S\bar{e}\bar{a} = S\bar{a}^{n+1} = S\bar{a}\bar{e} \subseteq S\bar{e}$. Conversely if $s \in S$, then $s\bar{e} = s\bar{e}\bar{e} = s\bar{a}^n\bar{a}^n = (s\bar{a}^{n-1})\bar{e}\bar{a} \in S\bar{e}\bar{a}$. Hence $S\bar{e} \subseteq S\bar{e}\bar{a}$ and $S\bar{e}\bar{a} = S\bar{e}$. #

Lemma 2.4.12. Let $A = (S, M)$ be a finite globally abelian automaton with transition monoid $T = T(A)$. Let $K = \bigcap_{a \in M} Sa$. Then (i) K is an S-ideal of A;

(ii) K contains every minimal S-ideal of A;

(iii) $Ka = K$ for all $a \in M$.

Proof. (i) Observe that if L is an S-ideal of A, then $L \cap Sa \neq \emptyset$ for all $a \in M$. In fact, we have $La \subseteq Sa$ and $La \subseteq L$ for all $a \in M$. By Proposition 2.3.7, the set Sa is an S-ideal for all $a \in M$. Consequently, $K \neq \emptyset$ and K is an S-ideal since $K = \bigcap_{a \in M} Sa = \bigcap_{\bar{a} \in T} S\bar{a}$ is a finite intersection of S-ideals.

(ii) Let I be a minimal S-ideal. Then $I \cap Sa \neq \emptyset$ for all $a \in M$. But $I \cap Sa$ is an S-ideal contained in I. Therefore the minimality of I implies $I \cap Sa = I$ for all $a \in M$, proving $I \subseteq Sa$ for all $a \in M$. Consequently $I \subseteq K$.

(iii) Let $a \in M$. Then $\bar{a} \in T$ and there exists a positive integer n such that $\bar{a}^n = \bar{e}$ is an idempotent. By Lemma 2.4.11, $\bar{a}$ is a permutation on $S\bar{e} \supseteq K$. Thus $|Ka| = |K|$. Since K is an S-ideal (by (i)), $K\bar{a} = Ka \subseteq K$. This implies $K\bar{a} = Ka = K$. #

Let A = (S, M) be a finite automaton. Then the union H of all minimal S-ideals of A is called the m-kernel of A (see [13]).

Lemma 2.4.13. Let A = (S, M) be a finite globally abelian automaton. If $K = \bigcap_{a \in M} Sa$ and H is the m-kernel of A, then K = H.

Proof. Since H is the union of minimal S-ideals, it follows by Lemma 2.4.12(ii) that $H \subseteq K$. Conversely, for any x ε M, $\bar{x}$ is a permutation on K by Lemma 2.4.12(iii). Thus by Proposition 2.4.10, $K \subseteq H$ and K = H. #

Corollary. If A = (S, M) is a finite globally abelian automaton, then B = (K, M) is the maximum permutation subautomaton of A.

Proof. By Lemma 2.4.12(iii), B is a permutation subautomaton of A. If C = (S', M) is any permutation subautomaton of A, then $S' \subseteq H = K$ by Proposition 2.4.10 and the lemma. This completes the proof. #

Let A = (S, M) be an automaton. A nonempty subset H of S is a globally abelian subset if Hab = Hba for all a, b ε M.

Lemma 2.4.14. Let $A = (S, M)$ be an automaton. Then

(i) if H_i, $i \in I$, are globally abelian subsets, then so is $\bigcup_{i \in I} H_i$;

(ii) if H is a globally abelian subset, then so is Hx for all $x \in M$.

Proof. (i) This follows from the fact that

$$(\bigcup_{i \in I} H_i)x = \bigcup_{i \in I} (H_i x) \text{ for all } x \in M.$$

(ii) Let $a, b, x \in M$. Since H is globally abelian, it follows that

$$(Hx)ab = H(xa)b = Hb(xa) = (Hbx)a = (Hxb)a = (Hx)ba.$$

Therefore Hx is globally abelian. #

In view of part (i) of Lemma 2.4.14, the union H of all globally abelian subsets of an automaton $A = (S, M)$ is again globally abelian and is called the globally abelian kernel (abbreviated as g.a. kernel) of A. Thus an automaton $A = (S, M)$ is globally abelian if and only if S is the g.a. kernel of A.

Remark. G.a. kernels do not always exist. The following provides us with an example of an automaton with no g.a. subsets. $A = (S, X)$ over $X = \{a, b\}$ with $S = \{1, 2, 3, 4\}$ and transition table as follows:

A	a	b
1	3	2
2	2	3
3	1	2
4	4	4

Lemma 2.4.15. If H is the g.a. kernel of an automaton $A = (S, M)$, then

(i) H is the maximal globally abelian subset of A;

(ii) H is an S-ideal of A.

Proof. (i) is obvious.

(ii) Since H is globally abelian, it follows from Lemma 2.4.14(ii) that Hx is globally abelian for all $x \in M$. Hence $Hx \subseteq H$ for all $x \in M$. Therefore H is an S-ideal of A. #

Corollary 1. Let $A = (S, M)$ be an automaton. If the g.a. kernel H exists, then the subautomaton $A_H = (H, M)$ is the maximum globally abelian subautomaton of A. #

Corollary 2. If a finite strongly connected automaton $A = (S, M)$ has a g.a. kernel H, then $H = S$ and A is a permutation automaton.

Proof. This is a consequence of the Lemma and the Corollary to Proposition 2.4.7. #

Corollary 3. If a finite locally transitive automaton $A = (S, M)$ has a g.a. kernel H, then the subautomaton $A_H = (H, M)$ is the maximum permutation subautomaton of A.

Proof. This is a consequence of the Lemma and Proposition 2.4.13. #

Recall that an S-congruence π of an automaton $A = (S, M)$ is right prime if for any $s, t \in S$ and $a \in M$, $sxa \equiv txa \pmod{\pi}$ for all $x \in M$ implies $s \equiv t \pmod{\pi}$.

Proposition 2.4.16. Let $A = (S, M)$ be an automaton. If every Rees congruence of A is right prime, then for every $s \in S$ and $a \in M$, there exist $x, y \in M$ such that $sxay = s$.

Proof. Let $s \in S$ and $a \in M$. Then $I = s(MaM)$ is an S-ideal of A. If $t \in I$, then $sxa \equiv txa \pmod{\rho(I)}$ for all $x \in M$. By hypothesis, $\rho(I)$ is right prime. Therefore $s \equiv t \pmod{\rho(I)}$. Since $t \in I$, it follows that $s \in I$. Hence there exist $x, y \in M$ such that $sxay = s$. #

Proposition 2.4.17. Let $A = (S, M)$ be a finite automaton. Then the following are equivalent.

(i) A is a permutation automaton.

(ii) A is globally abelian and every S-congruence of A is right prime.

(iii) A is globally abelian and every Rees congruence of A is right prime.

Proof. (i) implies (ii). By Proposition 2.3.5, A is globally abelian. Moreover, by Proposition 1.4.2 and Lemma 2.1.1, every S-congruence of A is right prime.

(ii) implies (iii). Obvious.

(iii) implies (i). Suppose A is not a permutation automaton; then there exists $a \in M$ such that $Sa \neq S$. By Proposition 2.3.7, Sa is an S-ideal. By hypothesis, the associated Rees congruence $\rho(Sa)$ is right prime. Let $s \in Sa$ and $t \in S - Sa$. Then $s \not\equiv t \pmod{\rho(Sa)}$. But $sxa \equiv txa \pmod{\rho(Sa)}$ for all $x \in M$, contrary to $\rho(Sa)$

being right prime. #

The following is an example of a right prime automaton with no nontrivial S-congruence, which is not a permutation automaton. Thus the condition that every S-congruence be right prime is not sufficient to obtain a permutation automaton.

Example 2.4.18. Let A = (S, X) be the f.i. automaton over X = {a, b} with S = {1, 2, 3, 4, 5} and the following transition table:

A	a	b
1	3	4
2	3	5
3	4	5
4	1	2
5	4	4

Clearly A is not a permutation automaton and it can be checked that A is right prime with no nontrivial S-congruence. #

Recall that an S-congruence π of an automaton A = (S, M) is left prime if for any $s_0 \in S$ and $a, b \in M$, $s_0xa \not\equiv s_0xb \pmod{\pi}$ for all $x \in M$ implies $sa \equiv sb \pmod{\pi}$ for all $s \in S$.

Proposition 2.4.19. Let A = (S, M) be an automaton with $Z(A) \neq S$, where Z(A) is the set of null states of A.

Then the following are equivalent.

(i) A is strongly connected.

(ii) Every S-congruence of A is left prime.

(iii) A is left prime and every Rees congruence of A is left prime.

(iv) Every quotient automaton of A is left prime.

Proof. The equivalence of (ii) and (iv) and the implication "(ii) implies (iii)" are obvious.

(i) implies (iv). Assume A is strongly connected. By Proposition 1.4.3, every quotient automaton of A is strongly connected and hence left prime by Lemma 2.2.1.

(iii) implies (i). Let A be left prime with $Z(A) \neq S$. Then $Z(A) = \emptyset$ by Proposition 2.2.2. If A is not strongly connected, there exists a proper S-ideal I of A. By hypothesis, the corresponding Rees quotient A/I is left prime. But $I \in Z(A/I)$ so that $Z(A/I) = S/I$ by Proposition 2.2.2. Therefore, if $s \in S - I$, then $\bar{s}x = \bar{s}$ for all $x \in M$, where $\bar{s}$ denotes the $\rho(I)$-class containing $\bar{s}$. But $\bar{s} = \{s\}$. Hence $sx = s$ for all $x \in M$. This implies $s \in Z(A)$, a contradiction. #

CHAPTER 3

TRANSITION MONOIDS OF SOME CLASSES OF AUTOMATA

In this chapter, the structure of transition monoids of left prime automata, duo automata and globally abelian automata is studied. In particular, a characterization of transition monoids of left prime automata is obtained.

3.1. The Structure of Left Prime Semigroups

We shall start with a representation of left prime semigroups by monomial matrices.

Let T be a semigroup. A nonempty set S together with a mapping: $S \times T \to S$ defined by $(s, a) \to sa$ satisfying $s(ab) = (sa)b$ for all $s \in S$ and $a, b \in T$ is called a right T-system and denoted by S_T. A left T-system is defined dually and denoted by ${}_TS$. A right T-system S_T is unital if T has an identity 1 and $s \cdot 1 = s$ for all $s \in S$. A unital left T-system is defined dually.

Remark. If $\underset{\sim}{A} = (S, M)$ is an automaton over a monoid M, then the state set S of A is a unital right M-system. Thus automata are special cases of right systems.

Any right(left) ideal of T is a right(left)

T-system in the natural way.

For any right T-system S, define a congruence δ_S on T by: a $\equiv$ b (mod δ_S) if sa = sb for all s ε S. A right T-system S is <u>faithful</u> if $\delta_S = 0$.

<u>Remark</u>. For the case of M-automaton A = (S, M) we have $\delta_S = E_S$. Further if the transition monoid of A is T = T(A), then the set S is a right T-system in the natural way. Moreover S_T is a faithful right T-system.

Recall that a semigroup T is left prime if for any a, b, c ε T, cxa = cxb for all x ε T^1 implies a = b.

<u>Lemma 3.1.1</u>. The following conditions on a semigroup T are equivalent.

(i) T is left prime.

(ii) For every a ε T, aT^1 is a faithful right T-system.

(iii) For every a ε T, $\delta_{aT^1} = 0$.

<u>Proof</u>. The equivalence of (ii) and (iii) is obvious.

(i) implies (iii). Suppose b $\equiv$ c (mod δ_{aT^1}), then (ax)b = (ax)c for all x ε T^1. Since T is left prime, hence b = c and $\delta_{aT^1} = 0$.

(ii) implies (i). Let a, b, c ε T. If axb = axc for all x ε T^1 and if S = aT^1, we have b $\equiv$ c (mod δ_S). But S is faithful therefore $\delta_S = 0$ and b = c. This implies that T is left prime. #

<u>Corollary</u>. If T is a left prime semigroup, then every minimal right ideal of T is a faithful right T-system. #

For a right T-system S, let

$$Z(S) = \{s \in S : sa = s \text{ for all } a \in T\}.$$

If T itself is considered as a right T-system, then Z(T) is the set of all left zeros of T.

Lemma 3.1.2. Let T be a nontrivial left prime semigroup. Then $Z(R) = \emptyset$ for every right ideal R of T.

Proof. Since $|T| > 1$, there exist $a, b \in T$ such that $a \neq b$. Let R be a right ideal of T. If $Z(R) \neq \emptyset$ and $z \in Z(R)$, then $zxa = z = zxb$ for all $x \in T^1$. But then $a = b$ since T is left prime, which is a contradiction. #

Remark. A similar but slightly different result holds for automata (cf. Proposition 2.2.2).

Corollary. If T is a nontrivial left prime semigroup, then T contains no left zeros. #

A T-subsystem of a right T-system S is a nonempty subset L of S such that $LT \subseteq L$. By a nontrivial T-subsystem of S we mean a subsystem L such that $L \neq S$ and $|L| > 1$.

Any subset of S of the form sT for some $s \in S$ is a T-subsystem of S.

A right T-system S is irreducible if

(i) $ST \not\subseteq Z(S)$,

(ii) S has no nontrivial T-subsystem.

Thus if S is irreducible and $L \subseteq S$ is a subsystem, then either $L = S$ or $L \subseteq Z(S)$.

A right T-system S is strongly connected if for any

$s, t \in S$, there exists $a \in T$ such that $sa = t$, or equivalently, for all $s \in S$, $sT = S$.

Any strongly connected T-system S is irreducible. For if L is a subsystem of S, then $S = sT \subseteq LT \subseteq L \subseteq S$ where $s \in L$ and hence $S = L$. Further, if S is nontrivial, then $Z(S) = \emptyset$. Conversely, if S is irreducible and $Z(S) = \emptyset$, then for all $s \in S$, sT is a subsystem of S and $sT \not\subseteq Z(S)$. Therefore $sT = S$ and S is strongly connected. Consequently, a nontrivial T-system S is strongly connected if and only if S_T is irreducible and $Z(S) = \emptyset$.

Lemma 3.1.3. Let T be a nontrivial left prime semigroup. Then every minimal right ideal of T, if it exists, is an irreducible T-system.

Proof. Let R be a minimal right ideal of T. By lemma 3.1.2, $Z(R) = \emptyset$ therefore $RT \not\subseteq Z(R)$. Moreover, if L is a subsystem of R and $s \in L$, then $sT \subseteq L \subseteq R$. But sT is a right ideal of T. The minimality of R implies $sT = L = R$. Therefore R is irreducible. #

Following Hoehnke [5], a semigroup T is called right primitive if it has a faithful irreducible right T-system.

Proposition 3.1.4. Let T be a nontrivial semigroup with minimal right ideals. Then the following are equivalent.

(i) T is left prime.

(ii) T is right primitive and $Z(T) = \emptyset$.

Proof. (i) implies (ii). Let R be a minimal right ideal of T. Then R = aT^1 for some $a \varepsilon T$. Since T is left prime, by Lemmas 3.1.1 and 3.1.3, R is a faithful irreducible T-system. Moreover, by the Corollary to Lemma 3.1.2, $Z(T) = \emptyset$.

(ii) implies (i). Let T be right primitive. Then T has a faithful irreducible T-system S. Suppose a, b, c ε T and axb = axc for all $x \varepsilon T^1$, then saxb = saxc for all $s \varepsilon S$ and $x \varepsilon T^1$. We claim that there exists at least one $s_0 \varepsilon S$ such that $s_0aT^1 = S$. For otherwise $saT^1 \subseteq Z(S)$ for all $s \varepsilon S$ since S is irreducible. Thus for all $s \varepsilon S$, sax = sa for all $x \varepsilon T$. But S is faithful hence ax = a for all $x \varepsilon T$. This implies $a \varepsilon Z(T)$, a contradiction. Hence $S = s_0aT^1$ for some $s_0 \varepsilon S$. Also $s_0axb = s_0axc$ for all $x \varepsilon T^1$ so that sb = sc for all $s \varepsilon S$. Consequently b = c since S is faithful. Therefore T is left prime. #

The proof of the above "(ii) implies (i)" is due to Hoehnke (cf. [5], 4.10. p455).

Let T be a semigroup and S_T, S'_T be two right T-systems. A mapping h (written on the left of the argument) of S into S' is a T-homomorphism if (hs)a = h(sa) for all $a \varepsilon T$ and $s \varepsilon S$. The set of all T-homomorphism of S_T into S'_T will be denoted by $\mathrm{Hom}_T[S_T, S'_T]$. If $_TS$ and $_TS'$ are left T-systems, then a T-homomorphism of $_TS$ into $_TS'$ is written on the right of the argument of S and is defined dually.

The set of all T-homomorphisms of $_TS$ into $_TS'$ will be denoted by $\mathrm{Hom}_T[_TS, {}_TS']$.

A T-homomorphism of a right T-system S_T into itself is a T-endomorphism. It is clear that if h_1 and h_2 are two T-endomorphisms of S_T, then the composition h_1h_2 is again a T-endomorphism of S_T. Thus the set $\mathrm{Hom}_T[S_T, S_T]$ of all T-endomorphisms of S_T forms a semigroup. If, in addition, a T=endomorphism is one to one and onto, then it is a T-automorphism. The set of all T-automorphisms of S_T is a subgroup of $\mathrm{Hom}_T[S_T, S_T]$, denoted by $\mathrm{Aut}_T(S_T)$.

If S_T is a right T-system and $H = \mathrm{Hom}_T[S_T, S_T]$, then S can be made into a left H-system by defining the mapping: $H \times S \to S$ by $(h, s) \to hs$. Clearly this mapping is well-defined and satisfies $hf(s) = h(fs)$ for all $h, f \in H$ and $s \in S$. If $G = \mathrm{Aut}_T(S_T)$, then S can also be made into a left G-system in the same way. It is obvious that both $_HS$ and $_GS$ are unital.

Proposition 3.1.5. Let T be a left prime semigroup, let R be a minimal right ideal of T and let $G = \mathrm{Aut}_T(R_T)$. Then T can be embedded in $H = \mathrm{Hom}_G[_GR, {}_GR]$.

Proof. Define a mapping ϕ: $T \to H = \mathrm{Hom}_G[_GR, {}_GR]$ by $\phi(a) = \rho_a$ where ρ_a is a mapping: $R \to R$ defined by $(s)\rho_a = sa$.

We claim that ϕ is the desired embedding. For this purpose, we have to show the following.

1. <u>Φ is well-defined.</u>

$\rho_a \in H$. For if $g \in G$ and $s \in R$, then

$$(gs)\rho_a = (gs)a = g(sa) = g(s\rho_a).$$

2. <u>Φ is a homomorphism.</u>

For every $s \in R$, $s\rho_{ab} = (s)ab = (sa)b = (s\rho_a)\rho_b$ $= (s)\rho_a\rho_b$. Hence $\rho_{ab} = \rho_a\rho_b$ and $\Phi(ab) = \Phi(a)\Phi(b)$.

3. <u>Φ is one to one.</u>

Suppose $\rho_a = \rho_b$ then $s\rho_a = s\rho_b$ for all $s \in R$, i.e., $sa = sb$ for all $s \in R$. This implies $a \equiv b \pmod{\delta_R}$. Since R is a minimal right ideal of T, $R = rT^1$ for every $r \in R$. By Lemma 3.1.1, $\delta_R = 0$. Hence $a = b$. #

A permutation g (written on the left of the argument) of a set X is a <u>regular permutation</u> if $gx = x$ for some $x \in X$ implies $g = 1_X$, the identity mapping on X.

<u>Lemma 3.1.6</u>. Let T be a semigroup and R be a minimal right ideal of T. Then every T-automorphism of R_T is a regular permutation on R.

<u>Proof</u>. Since R is a minimal ideal of T, we have $R = sT$ for every $s \in R$. Let $g \in \mathrm{Aut}_T(R_T)$ and $gr = r$ for some $r \in R$. The minimality of R implies that for every $u \in R$ there exists $a \in T$ such that $u = ra$. Thus

$$gu = g(ra) = (gr)a = ra = u.$$

Therefore $g = 1_R$ and g is a regular permutation on R. #

Let H be a semigroup and ${}_HS$ be a left H-system. I there exists a nonempty subset U of S such that for every $s \in S$, s can be uniquely expressed as $s = hu$ for some $h \in H^1$ and $u \in U$, then S is <u>free</u> or <u>freely generated by U</u> (see [14]) and U is called a <u>base</u> of S. It is clear that in this case S is a disjoint union of H^1u, $u \in U$, i.e., $S = \bigcup_{u \in U} H^1u$.

If S is a free H-system with base U, then every H-endomorphism of S is uniquely determined by its action on U. For if α and β are two H-endomorphisms of S and $u\alpha = u\beta$ for all $u \in U$, then for every $s \in S$ there exist $\bar{u} \in U$ and $h \in H^1$ such that $s = hu$. Thus $s\alpha = (hu)\alpha = h(u\alpha) = h(u\beta) = (hu)\beta = s\beta$.

Moreover, Tully has shown (see [14]) the following result.

<u>Lemma 3.1.7.</u> A unital left system S over a group G is free if and only if G is a group of regular permutations on S. #

<u>Corollary.</u> Let T be a semigroup. Then every minimal right ideal R of T is a free left G-system where $G = \mathrm{Aut}_T(R_T)$.

<u>Proof.</u> It is clear that R is a left G-system. By Lemma 3.1.5, G is a group of regular permutations on R. Thus ${}_GR$ is free by the Lemma. #

Therefore $g = 1_R$ and g is a regular permutation on R. #

Let H be a semigroup and ${}_HS$ be a left H-system. If there exists a nonempty subset U of S such that for every $s \in S$, s can be uniquely expressed as $s = hu$ for some $h \in H^1$ and $u \in U$, then S is free or freely generated by U (see [14]) and U is called a base of S. It is clear that in this case S is a disjoint union of H^1u, $u \in U$, i.e., $S = \bigcup_{u \in U} H^1u$.

If S is a free H-system with base U, then every H-endomorphism of S is uniquely determined by its action on U. For if α and β are two H-endomorphisms of S and $u\alpha = u\beta$ for all $u \in U$, then for every $s \in S$ there exist $u \in U$ and $h \in H^1$ such that $s = hu$. Thus $s\alpha = (hu)\alpha = h(u\alpha) = h(u\beta) = (hu)\beta = s\beta$.

Moreover, Tully has shown (see [14]) the following result.

Lemma 3.1.7. A unital left system S over a group G is free if and only if G is a group of regular permutations on S. #

Corollary. Let T be a semigroup. Then every minimal right ideal R of T is a free left G-system where $G = \mathrm{Aut}_T(R_T)$.

Proof. It is clear that R is a left G-system. By Lemma 3.1.5, G is a group of regular permutations on R. Thus ${}_GR$ is free by the Lemma. #

Let G be a group and G^0 be the group G with zero adjoined, i.e., $G^0 = G \cup \{0\}$. An $m \times n$ matrix (a_{ij}) over G^0 is *strictly row monomial* if for each i there exists exactly one j such that $a_{ij} \neq 0$. It can be verified that the product of two strictly row monomial $n \times n$ matrices is also strictly row monomial. Thus the set of all $n \times n$ strictly row monomial matrices over G^0 is a semigroup denoted by $M_n(G^0)$.

The following result is due to Tully (see [14], Theorem 8, p.103).

Proposition 3.1.8. Let G be a group and S be a free left G-system with base U and $|U| = n$. Then

$$\mathrm{Hom}_G[{}_GS, {}_GS] \cong M_n(G^0).$$

Proof. Let $U = \{u_1, \ldots, u_n\}$. Then $S = \bigcup_{k=1}^{n} Gu_k$ is a disjoint union since S is a free left ~~S~~-system.

Define a mapping [illegible] $\mathrm{Hom}_G[{}_GS, {}_GS] \to M_n(G^0)$ by

$$(h)\phi = (a_{ij}), \text{ where } a_{ij} = \begin{cases} g & \text{if } u_ih = gu_j \text{ and } g \in G, \\ 0 & \text{otherwise.} \end{cases}$$

We claim that ϕ is a semigroup isomorphism.

Since S is a disjoint union of Gu_k, $k = 1, \ldots, n$, hence ϕ is well-defined. Let $h, f \in H = \mathrm{Hom}_G[{}_GS, {}_GS]$ and $h\phi = (a_{ij})$, $f\phi = (b_{ij})$. For each i, let k be the integer such that $a_{ik} \neq 0$ and j be the integer such that $b_{kj} \neq 0$. Then for each $u_i \in U$ we have

$$\begin{aligned} (u_i)hf = (u_ih)f = (a_{ik}u_k)f = a_{ik}(u_kf) &= a_{ik}(b_{kj}u_j) \\ &= (a_{ik}b_{kj})u_j. \end{aligned}$$

Thus $(hf)\phi = (c_{ij})$ where $c_{ij} = a_{ik}b_{kj}$. It follows that $(c_{ij}) = (a_{ij})(b_{ij})$ and $(hf)\phi = (h\phi)(f\phi)$. Therefore ϕ is a semigroup homomorphism.

On the other hand, since ${}_GS$ is free, every G-homomorphism is uniquely determined by its action on U. This implies that ϕ is one to one. It remains to show that ϕ is onto. To this end, let $(a_{ij}) \in M_n(G^0)$. Then for every $i = 1, \ldots, n$, there exists j, $1 \leq j \leq n$ such that $a_{ij} \neq 0$. Let h be the mapping defined for every $u_i \in U$ by $u_ih = a_{ij}u_j$. Extend h to a mapping of S, also denoted by h, by defining for every $s = gu_i \in S$ where $g \in G$ and $u_i \in U$, $sh = (gu_i)h = g(u_ih)$. Then h is a mapping of S into itself and is a G-endomorphism of S. For if $g' \in G$ and $s = gu_i \in S$, then

$$g'(sh) = g'(gu_i)h = g'g(u_ih) = (g'gu_i)h = (g's)h.$$

Therefore $h \in \mathrm{Hom}_G[{}_GS, {}_GS]$. It is obvious that $(h)\phi = (a_{ij})$. This completes the proof. #

As a consequence of the above Proposition, we have the following.

Corollary. Let $s_1, \ldots, s_n$ be arbitrary in S. Then the mapping h of U into S defined by

$$u_ih = s_i \quad i = 1, \ldots, n$$

can be extended uniquely to a G-endomorphism of ${}_GS$.

Proof. For each s_i, $i = 1, \ldots, n$, there exist uniquely $g \in G$ and $u_j \in U$ such that $s_i = gu_j$. Let

$$a_{ij} = \begin{cases} g & \text{if } s_i = gu_j, \\ 0 & \text{otherwise.} \end{cases}$$

Then $(a_{ij}) \in M_n(G^0)$. By the Proposition, h can be extended to a G-endomorphism of ${}_GS$. The uniqueness follows from the freeness of ${}_GS$ as a G-system. #

Another consequence of the above Proposition is the following embedding of a finite left prime semigroup into a monomial matrix semigroup.

Proposition 3.1.9. Every finite left prime semigroup is a subsemigroup of a monomial matrix semigroup.

Proof. Let T be a finite left prime semigroup, R be a minimal right ideal of T and $G = \mathrm{Aut}_T(R_T)$. By Proposition 3.1.5, T is a subsemigroup of $\mathrm{Hom}_G[{}_GR, {}_GR]$. By Lemma 3.1.6, G is a group of regular permutations of R. Thus ${}_GR$ is a free left G-system with base, U say, by Lemma 3.1.7. Since T is finite, R and U are finite. If $|U| = n$, then $\mathrm{Hom}_G[{}_GR, {}_GR]$ is isomorphic to $M_n(G^0)$ by Proposition 3.1.8. Consequently, T is isomorphic to a subsemigroup of $M_n(G^0)$. #

Now we turn to consider some properties of the semigroup $\mathrm{Hom}_G[{}_GR, {}_GR]$. First, we have the following lemma.

Lemma 3.1.10. Let T be a left prime semigroup with minimal right ideal R and $G = \mathrm{Aut}_T(R_T)$. Then the semigroup $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ acts transitively on ${}_GR$.

Proof. It suffices to show $sH = R$ for all $s \in R$. Since R is a minimal right ideal of T, $sT = R$ for all $s \in R$. Thus for all $r \in R$ there exists $a \in T$ such that $sa = r$. But $s\sigma_a = sa = r$ and $\sigma_a \in H$. Thus $sH = R$. #

Remark. The above Lemma also holds if R is a strongly connected right system over T.

Proposition 3.1.11. Let T be a left prime semigroup with a minimal right ideal R and $G = \mathrm{Aut}_T(R_T)$. Then the semigroup $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ is left prime.

Proof. Suppose for some $f, h_1, h_2 \in H$, $fxh_1 = fxh_2$ for all $x \in H$; we shall show $h_1 = h_2$. If $r \in R$, then $(rf)xh_1 = (rf)xh_2$ for all $x \in H$. Further, $rf \in R$ so that $(rf)H = R$ by Lemma 3.1.10. Hence the above implies $sh_1 = sh_2$ for all $s \in R$. Therefore $h_1 = h_2$. #

Remark. The above Proposition also holds if R is a strongly connected right system over T.

Proposition 3.1.12. Let T be a finite left prime semigroup, R a minimal right ideal of T and $G = \mathrm{Aut}_T(R_T)$. If $|G| > 1$, then the semigroup $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ is right prime.

Proof. Suppose for some $f, h_1, h_2 \in H$, $h_1xf = h_2xf$ for all $x \in H$. We shall show $h_1 = h_2$.

By Lemmas 3.1.6 and 3.1.7, R is a free left G-system with base U, say. Since T is finite and $U \subseteq R \subseteq T$, U is finite. Let $U = \{u_1, \ldots, u_n\}$. Then $R = \bigcup_{k=1}^{n} Gu_k$. It suffices to show $u_ih_1 = u_ih_2$ for all

$i = 1, \ldots, n$.

Since $u_i h_1, u_i h_2 \in R$, there exist $g_{ij}, g_{ik} \in G$ such that

$$u_i h_1 = g_{ij} u_j,$$
$$u_i h_2 = g_{ik} u_k.$$

We shall show $g_{ij} = g_{ik}$ and $j = k$. Let x_1 be the mapping of U into R defined by $u_i x_1 = u_1$ for all $i = 1, \ldots, n$. Then by the Corollary to Proposition 3.1.8, x_1 can be extended to a G-endomorphism of R, also denoted by x_1. Thus $x_1 \in H$ and we obtain

$$(u_i h_1) x_1 f = (u_i h_2) x_1 f,$$
$$(g_{ij} u_j) x_1 f = (g_{ik} u_k) x_1 f,$$
$$g_{ij} (u_j x_1) f = g_{ik} (u_k x_1) f,$$
$$g_{ij} (u_1 f) = g_{ik} (u_1 f);$$
$$(g_{ik})^{-1} g_{ij} (u_1 f) = u_1 f.$$

Since $u_1 f \in R$ and $(g_{ik})^{-1} g_{ij} \in G$, which is a group of regular permutations of R, it follows that $(g_{ik})^{-1} g_{ij} = 1$ and thus $g_{ik} = g_{ij}$.

It remains to show $j = k$. Suppose $j \neq k$. Since $|G| > 1$, there exists $g \in G$ such that $1 \neq g$. Let x_2 be the mapping of R defined by

$$u_j x_2 = g u_1,$$
$$u_i x_2 = u_1 \quad \text{for all } i \neq j.$$

Then by the Corollary to Proposition 3.1.8, $x_2 \in H$. Thus the hypothesis yields

$$(u_i h_1) x_2 f = (u_i h_2) x_2 f,$$

$$(g_{ij}u_j)x_2f = (g_{ik}u_k)x_2f,$$
$$g_{ij}(u_jx_2)f = g_{ik}(u_kx_2)f,$$
$$g_{ij}(gu_l)f = g_{ik}(u_l)f,$$
$$g_{ij}g(u_lf) = g_{ik}(u_lf).$$

So $g_{ij}g = g_{ik}$. But $g_{ij} = g_{ik}$. Hence $g = 1$, a contradiction. Therefore $j = k$ and H is right prime.

Remark. If $G = 1$, then $H = T_R$, the transformation monoid on R. Unless $|R| = 1$, H is not right prime since every constant transformation in T_R is a right zero of T_R (see Corollary 2 to Proposition 2.1.6).

A semigroup T is regular if for all $a \in T$ there exists $x \in T$ such that $axa = a$.

Proposition 3.1.13. Let T be a finite left prime semigroup with a minimal right ideal R and $G = \mathrm{Aut}_T(R_T)$. Then the semigroup $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ is regular.

Proof. By the hypothesis, R is a free left G-system with a finite base $U = \{u_1, \ldots, u_n\}$ and $R = \bigcup_{i=1}^{n} Gu_i$. Moreover, every G-endomorphism of ${}_GR$ is uniquely determined by its action on U.

Let $h \in H$. Let f be the mapping of U into R defined as follows. For each $i = 1, \ldots, n$, if $Uh \cap Gu_i \neq \emptyset$ and i_0 is the first integer such that $u_{i_0}h = gu_i \in Gu_i$, then define $u_if = g^{-1}u_{i_0}$; otherwise define $u_if = u_i$. Then by the Corollary to Proposition 3.1.8, f can be extended to a G-endomorphism of R, also denoted by f. We shall show $hfh = h$. To this end, it suffices to show $(u_k)hfh = (u_k)h$ for all $k = 1, \ldots, n$. Suppose $(u_k)h = au_i$, $a \in G$. Then $Uh \cap Gu_i \neq \emptyset$. Hence $u_if = g^{-1}u_{i_0}$ where i_0 is the first integer such that $u_{i_0}h = gu_i$. Thus we have

$$(u_k)hfh = (u_kh)fh = (au_i)fh = a(u_if)h = a(g^{-1}u_{i_0})h$$

$$= ag^{-1}(u_{i_0}h) = ag^{-1}(gu_i) = au_i = (u_k)h.$$

Therefore H is regular. #

In what follows, we shall establish a characterization of finite left prime monoids.

We now fix the notation for the rest of the section. Let T be a finite left prime semigroup with a minimal right ideal R and $G = \mathrm{Aut}_T(R_T)$. Then by Lemmas 3.1.1, 3.1.2 and 3.1.3, R_T is a faithful strongly connected right T-system. Moreover, we have shown that ${}_GR$ is a free left G-system with a finite base $U = \{u_1, \ldots, u_n\}$, say, and $R = \bigcup_{i=1}^{n} Gu_i$.

Let $H = \mathrm{Hom}_G[{}_GR, {}_GR]$. Then H can be made into a right T-system by defining the mapping: $H \times T \to H$ by $(h, a) \to h\circ a = h\rho_a$. Clearly $h\circ a \in H$. Moreover, for any $h \in H$ and $a, b \in T$ we have

$$(h\circ a)\circ b = (h\rho_a)\circ b = h\rho_a\rho_b = h\rho_{ab} = h\circ(ab).$$

Therefore H is a right T-system under this mapping.

On the other hand, it is clear that for each $i = 1, \ldots, n$, the set Gu_i is a left G-subsystem of ${}_GR$.

Thus it makes sense to consider $\mathrm{Hom}_G[{}_G(Gu_i), {}_GR]$ and we have the following:

Lemma 3.1.14. Let $H_i = \mathrm{Hom}_G[{}_G(Gu_i), {}_GR]$. Then

$$H_i = \{h_i \mid h_i = h|_{Gu_i} \text{ for some } h \in H\}.$$

Proof. Let $F = \{h_i \mid h_i = h|_{Gu_i}$ for some $h \in H\}$. Then clearly $F \subseteq H_i$. Suppose $h_i \in H_i$ and let h be the mapping of U into R defined by

$$u_ih = u_ih_i,$$
$$u_jh = u_j \quad \text{for all } j \neq i.$$

By the Corollary to Proposition 3.1.8, h can be extended to a G-endomorphism of R, also denoted by h. Evidently $h_i = h|_{Gu_i}$. This proves $H_i \subseteq F$. Therefore $H_i = F$. #

Similarly, H_i can be made into a right T-system by defining the mapping: $H_i \times T \to H_i$ by

$$(h_i, a) \to h_i * a = h_i\rho_a.$$

Proposition 3.1.15. Let T, R, G, H and $H_1, \ldots, H_n$ be as above. Then for each $i = 1, \ldots, n$, the following conditions hold.

(i) $Z(H_i) = \emptyset$.

(ii) H_i is a faithful right T-system.

(iii) H_i is an irreducible right T-system.

Proof. (i) Recall that

$Z(H_i) = \{h_i \mid h_i * a = h_i$ for all $a \in T\}$. Suppose $Z(H_i) \neq \emptyset$ and $h_i \in Z(H_i)$. If $r \in R$, then $rh_i \in R$. We obtain

$$rh_i = (r)h_i * a = (rh_i)\rho_a = (rh_i)a \quad \text{for all } a \in T.$$

This yields $rh_i \in Z(R)$, a contradiction since $Z(R) = \emptyset$ by Lemma 3.1.2. Therefore $Z(H_i) = \emptyset$.

(ii) By definition, a right T-system S is faithful if the congruence $\delta_S = 0$ on T, where δ_S is defined by $a \equiv b \pmod{\delta_S}$ if $sa = sb$ for all $s \in S$. Since R_T is faithful, $\delta_R = 0$ and it suffices to show $\delta_{H_i} \le \delta_R$.

Suppose $a \equiv b \pmod{\delta_{H_i}}$. Then $h_i * a = h_i * b$ for all $h_i \in H_i$. Let $u_i \in U$. We have

$$(u_i)h_i * a = (u_i)h_i * b \quad \text{for all } h_i \in H_i,$$
$$(u_i h_i)\rho_a = (u_i h_i)\rho_b \quad \text{for all } h_i \in H_i,$$
$$(u_i h_i)a = (u_i h_i)b \quad \text{for all } h_i \in H_i.$$

Since $H_i = \{h_i \mid h_i = h_{Gu_i}$ for some $h \in H\}$ by Lemma 3.1.14, the above implies

$$(u_i h)a = (u_i h)b \quad \text{for all } h \in H.$$

On the other hand, Lemma 3.1.10 yields $u_i H = R$. Thus $ra = rb$ for all $r \in R$. Therefore $a \equiv b \pmod{\delta_R}$ and $\delta_{H_i} \le \delta_R$.

(iii) Recall that a right T-system S is irreducible if $ST \not\subseteq Z(S)$ and S contains no nontrivial T-subsystems. In view of (i), it suffices to show that H_i contains no nontrivial T-subsystems. Let $K \neq \emptyset$ be a T-subsystem of H_i. Let $h \in H_i$ and $k \in K$. Then $u_i h \in R$ and $u_i k \in R$. Since R_T is strongly connected, there exists $a \in T$ such that $u_i h = (u_i k)a = (u_i k)\rho_a = u_i(k*a)$. Hence $h = k*a$ and

$h \in K$. Therefore $K = H_i$. #

Corollary. For each $i = 1, \ldots, n$, H_i is a faithful stringly connected right T-system. #

Proposition 3.1.16. Let T, R, G, $U = \{u_1, \ldots, u_n\}$, $H = \mathrm{Hom}_G[{}_G R, {}_G R]$ and $H_1, \ldots, H_n$ be as above. Then the right T-system H is the direct product of the right T-systems $H_1, \ldots, H_n$, i.e., $H = \prod_{i=1}^{n} H_i$.

Proof. Define a mapping α: $H \to \prod_{i=1}^{n} H_i$ by $\alpha(h) = (h|_{Gu_1}, \ldots, h|_{Gu_n})$.

1. α is well-defined.

   This follows from $h|_{Gu_i} \in H_i$ for every $i = 1, \ldots, n$.

2. α is one to one.

   If $h, g \in H$ and $h \neq g$, then for some $u_i \in U$, $u_i h \neq u_i f$ and hence $h|_{Gu_i} \neq f|_{Gu_i}$ proving $\alpha(h) \neq \alpha(f)$.

3. α is onto.

   Suppose $(h_1, \ldots, h_n) \in \prod_{i=1}^{n} H_i$. Let h be the mapping of U into R defined by

   $$u_i h = u_i h_i \quad \text{for } i = 1, \ldots, n.$$

   Since $h_i u_i \in R$ for all $i = 1, \ldots, n$, by the Corollary to Proposition 3.1.8, h can be extended to a G-endmorphism of R. Thus $h \in H$. Evidently $\alpha(h) = (h_1, \ldots, h_n)$.

4. α is a T-homomorphism.

   Let $h \in H$ and $a \in T$. Then

   $$\alpha(h \circ a) = \alpha(h\rho_a) = (h\rho_a|_{Gu_1}, \ldots, h\rho_a|_{Gu_n})$$

$$= (h_{Gu_1} \cdot a, \ldots, h_{Gu_n} \cdot a)$$

$$= (h_{Gu_1} * a, \ldots, h_{Gu_n} * a)$$

$$= (h_{Gu_1}, \ldots, h_{Gu_n}) * a$$

$$= (\phi h) * a.$$

Therefore H is the direct product of $H_1, \ldots, H_n$. #

Considering H as the direct product of $H_1, \ldots, H_n$, let π_i be the ith projection map for each $i = 1, \ldots, n$. Then $\pi_i(h) = h_{Gu_i}$ for every $h \in H$.

On the other hand, Proposition 3.1.5 says that T can be embedded in $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ under the mapping ϕ defined by $\phi(a) = \rho_a$.

We shall need these facts to prove the following proposition.

<u>Proposition 3.1.17</u>. Let T, R, G, $U = \{u_1, \ldots, u_n\}$, $H = \mathrm{Hom}_G[{}_GR, {}_GR]$ and $H_i = \mathrm{Hom}_G[{}_G(Gu_i), {}_GR]$, $i = 1, \ldots, n$, be as above. Then the right T-system T_T is a subdirect product of $H_1, \ldots, H_n$.

<u>Proof</u>. For each $i = 1, \ldots, n$ we have the following diagram:

$$\begin{tikzcd}
T \arrow[r, "\phi"] \arrow[dr, "\pi_i\phi"'] & H \arrow[d, "\pi_i"] \\
 & H_i
\end{tikzcd}$$

To show that T is a subdirect product it suffices to show that the mapping π_i is onto for every $i = 1, \ldots, n$.

Since R_T is strongly connected, $rT = R$ for every $r \in R$.

Let $h_i \in H_i$. Then $u_i h_i \in R = u_i T$. Hence there exists $a \in T$ such that $u_i h_i = u_i a = u_i \rho_a$. Thus we have $(gu_i)h_i = g(u_i h_i) = g(u_i \rho_a) = (gu_i)\rho_a$ for all $g \in G$. This implies $h_i = \rho_a | Gu_i = \pi_i(\rho_a)$. But $\phi(a) = \rho_a$ so that $h_i = \pi_i(\phi(a))$. Therefore π_i is onto. #

Corollary. The right T-system T_T is a subdirect product of faithful strongly connected right T-systems.

Proof. This is a consequence of the Proposition and the Corollary to Proposition 3.1.15. #

We conclude with the following:

Theorem 3.1.18. Let M be a finite monoid. Then M is left prime if and only if the right M-system M_M is a subdirect product of strongly connected right M-systems.

Proof. The necessity follows from the above Corollary to Proposition 3.1.17.

Sufficiency. We remark first that since M is a monoid, the right M-system M_M is the same as the M-automaton $A_M = (M, M)$. Hence results concerning M-automata (in particular $A_M = (M, M)$) can be applied to M_M.

Suppose M_M is a subdirect product of strongly connected right M-systems. Since every strongly connected M-system is left prime, by the Corollary to Proposition 2.2.11, M_M is left prime. Finally by Corollary 3 to Proposition 2.2.8, M is a left prime monoid. #

Example 3.1.19. Let $T(A) = \{\overline{1}, \overline{a}, \overline{b}, \overline{a^2}, \overline{ba}\}$ be the transition monoid of the right prime automaton $A = (S, X)$ of Example 2.1.5. Then T(A) is right prime. Denote $\overline{1}$, $\overline{a}$, $\overline{b}$, $\overline{a^2}$ and $\overline{ba}$ by 1, a, b, c and d respectively and let $M = \{1, a, b, c, d\}$ be the dual semigroup of T(A). Then M is a left prime monoid with the following multiplication table.

M	1	a	b	c	d
1	1	a	b	c	d
a	a	c	d	a	b
b	b	a	b	c	d
c	c	a	b	c	d
d	d	c	d	a	b

It is clear that the minimal right ideal of M is $R = \{a, b, c, d\}$. It can be checked that

$$G = \mathrm{Aut}_M(R_M) = \left\{ e = \begin{pmatrix} a, & b, & c, & d \\ a, & b, & c, & d \end{pmatrix}, \ g = \begin{pmatrix} a, & b, & c, & d \\ c, & d, & a, & b \end{pmatrix} \right\}.$$

The free left G-system ${}_GR$ can be represented by the following table:

σ	e	G^R
c	a	a
d	b	b
a	c	c
b	d	d

Let $\Gamma = \{a, b\}$ be a base for G^R. Then $Ga = \{a, c\}$ and $Gb = \{b, d\}$. We obtain

$$H_1 = \left\{ h_{11} = \begin{pmatrix} a,c \\ a,c \end{pmatrix},\ h_{12} = \begin{pmatrix} a,c \\ c,a \end{pmatrix},\ h_{13} = \begin{pmatrix} a,c \\ b,d \end{pmatrix},\ h_{14} = \begin{pmatrix} a,c \\ d,b \end{pmatrix} \right\},$$

$$H_2 = \left\{ h_{21} = \begin{pmatrix} b,d \\ b,d \end{pmatrix},\ h_{22} = \begin{pmatrix} b,d \\ d,b \end{pmatrix},\ h_{23} = \begin{pmatrix} b,d \\ a,c \end{pmatrix},\ h_{24} = \begin{pmatrix} b,d \\ c,a \end{pmatrix} \right\}.$$

Both H_1 and H_2 are strongly connected right M-systems. The embedding of M into $H_1 \times H_2$ is given by:

$$\begin{aligned} 1 &\to (h_{11}, h_{21}), \\ a &\to (h_{12}, h_{23}), \\ b &\to (h_{14}, h_{21}), \\ c &\to (h_{11}, h_{24}), \\ d &\to (h_{13}, h_{22}). \quad \# \end{aligned}$$

3.2. The Structure of Duo Automata

Recall that an automaton $A = (S; M)$ is duo if for all $a, b \in M$, there exist $x, y \in M$ such that $sab = sxa = sby$ for all $s \in S$, and that a semigroup T is duo if $aT = Ta$.

Let π be an S-congruence of a duo automaton $A = (S; M)$. Then clearly for all $a, b \in M$ there exists $x, y \in M$ such that

$sab \quad sxa \quad sby$ (mod [illegible]), for all s [illegible] S.

Therefore every quotient automaton of A is duo. Thus we have the following.

Proposition 3.2.1. Every duo automaton is a subdirect product of duo irreducible automata.

Proof. Let A be a duo automaton. By Theorem 1.3.5, A is a subdirect product of A_i, $i \in I$. By Theorem 1.3.4, each A_i is a quotient automaton of A. Therefore each A_i is duo by the above observation. The assertion then follows. #

In view of the above Proposition, it will then be sufficient to study the structure of duo irreducible automata. If A is a finite duo irreducible automaton with transition monoid $T = T(A)$, we will show that T is either a group or a union of a group and a nilpotent ideal.

Recall that an automaton $A = (S, M)$ is irreducible if and only if the intersection of nonequality S-congruences is nonequality.

First, we have the following.

Lemma 3.2.2. Let $A = (S, M)$ be a duo irreducible automaton with $T = T(A)$. If $\bar{e} \in T$ is an idempotent, then $\bar{e}$ is either an identity or a reset.

Proof. Let $\bar{e} \in T$ be an idempotent. Then $I = S\bar{e}$ is an S-ideal by Proposition 2.3.4. Suppose $\bar{e}$ is neither an identity nor a reset, then $I \neq S$ and $|I| > 1$. Thus the associated Rees congruence (I) is nonequality.

On the other hand, let - be the equivalence on S defined by s t (mod -) if $s\bar{e} = t\bar{e}$. We shall show that is an S-congruence. To this end, let s t (mod -). Then $s\bar{e} = t\bar{e}$. Since T is duo by Proposition 2.3.1, and by Proposition 2.3.3, every idempotent of T is in the center of T. Thus if a M, then we have

$$s a\bar{e} = s\bar{a}\bar{e} = s\bar{e}\bar{a} = t\bar{e}\bar{a} = t\bar{a}\bar{e} = t a\bar{e}.$$

This implies sa ta (mod -) and - is an S-congruence. Moreover, since $\bar{e}$ is not an identity, there exist s, t S such that $s \neq t$ and $s\bar{e} = t\bar{e}$. Hence is a nonequality S-congruence of A.

It is clear that every class of = contains exactly one element of $I = S\bar{e}$. Hence $\cap$ (I) = 0. This contradicts the irreducibility of A. #

<u>Proposition 3.2.3</u>. Let A = (S, M) be a finite duo irreducible automaton with transition monoid T = T(A). If T is not a group, then T contains a zero element and T is a union of a group and a nilpotent ideal.

<u>Proof</u>. It is clear that the subset G of all permutations of S in T forms a subgroup of T. If $T \neq G$, then there are elements of T, which do not act as permutations on S. Since T is finite, if $\bar{a} \in T - G$, then there exists a positive integer n such that $\bar{a}^n = \bar{z}$ is an idempotent and $\bar{z} \neq 1_S$, so that $\bar{z}$ is a reset by the above Lemma. Moreover,

by Proposition 2.3.1, T is duo and by Proposition 2.3.3, $\bar{z}$ is in the center of T. Therefore for every $\bar{x} \in T$, we obtain

$$s\bar{z}\bar{x} = s\bar{x}\bar{z} = s\bar{z} \text{ for all } s \in S$$

This implies that $\bar{z}$ is a zero in T.

Let $N = \{\bar{a} \mid \bar{a} \in T$ and $\bar{a}^n = \bar{z}$ for some integer $n > 0\}$. Then clearly $T = G \cup N$. It remains to show that N is a nilpotent ideal. Since every element of N is nilpotent and T is finite, it suffices to show that N is an ideal. Let $\bar{a} \in N$ amd $\bar{x} \in T$. Since $\bar{a}$ is not a permutation on S, $S\bar{a} \subsetneq S$. Moreover, $S\bar{a}\bar{x} \subseteq S\bar{a} \subsetneq S$. This implies that $\bar{a}\bar{x}$ is not a permutation on S. Thus $\bar{a}\bar{x} \in N$. Similarly, $\bar{x}\bar{a} \in N$. Hence N is an ideal. #

<u>Corollary 1</u>. If the monoid T is not a group, then A has a unique null state.

<u>Proof</u>. By the Proposition, T contains a zero element $\bar{z}$ which is a reset. Then $S\bar{z} = \{s\}$ and s is a null state. Clearly it is unique. #

<u>Corollary 2</u>. Any finite irreducible automaton which contains two distinct null states cannot be duo.

<u>Proof</u>. This is a consequence of the above Corollary 1. #

<u>Corollary 3</u>. Any finite duo irreducible automaton without null states is a permutation automaton.

<u>Proof</u>. Let A be a finite duo irreducible automaton without null states. By the above Corollary 1, T = T(A) is a

group. Therefore, A is a permutation automaton by Proposition 1.4.1. #

Let Y = {0, 1}. Define 1·1 = 1 and 1·0 = 0·1 = 0·0 = 0. Then (Y, ·) is a lattice called the <u>two-element chain</u>. Any semigroup isomorphic to Y is also called the two-element chain.

<u>Corollary 4</u>. Let A be a finite duo irreducible automaton. Then the set F of all idempotents of T = T(A) is either a singleton or the two-element chain.

<u>Proof</u>. By the Proposition, T is either a group or a union of a group and a nilpotent ideal. If T is a group, then F = {1} is a singleton. If T is not a group, then F = {1, $\bar{z}$} where $\bar{z}$ is the zero in T. Clearly, in this case, F is the two-element chain. #

<u>Example 3.2.4</u>. Let A = (S, X) be the f.i. automaton over X = {a, b, c} with S = {1, 2, 3, 4, 5, 6} and the following transition table:

A	a	b	c
1	1	1	2
2	2	2	2
3	6	3	2
4	4	4	1
5	3	6	2
6	5	5	2

It can be checked that T = T(A) = {$\bar{\Lambda}$, $\bar{a}$, $\bar{b}$, $\bar{a}^2$, $\overline{ab}$, $\overline{ba}$, $\bar{c}$, 2 OF/DE 2

$\bar{c}^2\}$ with following multiplication table:

T	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$	$\bar{a}^2$	$\overline{ab}$	$\overline{ba}$	$\bar{c}$	$\bar{c}^2$
$\bar{\Lambda}$	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$	$\bar{a}^2$	$\overline{ab}$	$\overline{ba}$	$\bar{c}$	$\bar{c}^2$
$\bar{a}$	$\bar{a}$	$\bar{a}^2$	$\overline{ab}$	$\bar{\Lambda}$	$\overline{ba}$	$\bar{b}$	$\bar{c}$	$\bar{c}^2$
$\bar{b}$	$\bar{b}$	$\overline{ba}$	$\bar{\Lambda}$	$\overline{ab}$	$\bar{a}^2$	$\bar{a}$	$\bar{c}$	$\bar{c}^2$
$\bar{a}^2$	$\bar{a}^2$	$\bar{\Lambda}$	$\overline{ba}$	$\bar{a}$	$\bar{b}$	$\overline{ab}$	$\bar{c}$	$\bar{c}^2$
$\overline{ab}$	$\overline{ab}$	$\bar{b}$	$\bar{a}$	$\overline{ba}$	$\bar{\Lambda}$	$\bar{a}^2$	$\bar{c}$	$\bar{c}^2$
$\overline{ba}$	$\overline{ba}$	$\overline{ab}$	$\bar{a}^2$	$\bar{b}$	$\bar{a}$	$\bar{\Lambda}$	$\bar{c}$	$\bar{c}^2$
$\bar{c}$	$\bar{c}$	$\bar{c}$	$\bar{c}$	$\bar{c}$	$\bar{c}$	$\bar{c}$	$\bar{c}^2$	$\bar{c}^2$
$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$	$\bar{c}^2$

Since $\bar{x}T = T\bar{x}$ for all $\bar{x} \in T$, T is duo. Thus by Proposition 2.3.1, A is duo. The subgroup of T is $G = \{\bar{\Lambda}, \bar{a}, \bar{b}, \bar{a}^2, \overline{ab}, \overline{ba}\}$, the zero element of T is $\bar{c}^2$, the nilpotent ideal is $N = \{\bar{c}, \bar{c}^2\}$ and $T = G \cup N$. #

The following theorem concerns the structure of finite duo automata.

<u>Theorem 3.2.5</u>. Let $A = (S, M)$ be a finite duo automaton. Then the transition monoid $T(A)$ of A is a subdirect product of a finite number of monoids, each of which is either a group or a union of a group and a nilpotent ideal.

<u>Proof</u>. By Proposition 3.2.1, A is a subdirect product of duo irreducible automata, say A_i, $i = 1, \ldots, n$. Since A is finite so is every A_i. Let $T_i = T(A_i)$, $i = 1, \ldots, n$. Then by Proposition 3.2.3, each T_i is either a group or a

union of a group and a nilpotent ideal. By Theorem 1.3.7, T(A) is a subdirect product of T_i, i = 1, ..., n. This completes the proof. #

Recall that if an automaton A = (S, M) is a subdirect product of automata $A_i = (S_i, M)$, i = 1, ..., n, then the embedding of T = T(A) into the direct product $\prod_{i=1}^{n} T_i$ of $T_i = T(A_i)$ i = 1, ..., n is defined by $\phi(\bar{a}) = (\bar{a}^{(1)}, \ldots, \bar{a}^{(n)})$ where $a \in M$, $\bar{a} \in T$ is the E_S- class containing a and for each i = 1, ..., n, $\bar{a}^{(i)} \in T_i$ is the E_{S_i}-class containing a (see the proof of Theorem 1.3.7).

Let A = (S, M) be a duo automaton with transition monoid T = T(A). Then by Proposition 2.3.1, T is duo, and by Proposition 2.3.3, every idempotent of T is in the center of T. Thus if $\bar{e}$ and $\bar{f}$ are idempotents of T, then $(\bar{e}\bar{f})(\bar{e}\bar{f}) = \bar{e}\bar{e}\bar{f}\bar{f} = \bar{e}\bar{f}$. This implies that the set F of all idempotents of T forms a subsemigroup; indeed F is a commutative band. Moreover, as a consequence of Theorem 3.2.5, we have the following result.

<u>Corollary</u>. Let A = (S, M) be a finite duo automaton with transition monoid T = T(A). Then the set F of all idempotents of T is a subsemigroup which is either a singleton or a subdirect product of two-element chains.

<u>Proof</u>. As in the proof of the Theorem, T is a subdirect product of T_i, i = 1, ..., n. For each i = 1, ..., n, let

F_i be the set of all idempotents of T_i. Then clearly $\phi(F) \subseteq \prod_{i=1}^{n} F_i$ since ϕ is a semigroup homomorphism. Moreover, for each i = 1, ..., n, $\pi_i\phi|_F$ is onto. For if $\bar{e}^{(i)} \in F_i \subseteq T_i$, then there exists $\bar{x} \in T$ such that $\pi_i\phi(\bar{x}) = \bar{e}^{(i)}$. If $\bar{x} \in F$, then we are done. If $\bar{x} \notin F$, then there exists a positive integer n such that $(\bar{x})^n \in F$. Thus

$$\pi_i\phi(\bar{x}^n) = (\pi_i\phi(\bar{x}))^n = (\bar{e}^{(i)})^n = \bar{e}^{(i)}.$$

Therefore $\pi_i\phi|_F$ is onto and F is a subdirect product of $F_1, \ldots F_n$. The assertion then follows by Corollary 4 to Proposition 3.2.3, which yields that each F_i is either a singleton or the two-element chain. #

3.3. Some Properties of Globally Abelian Automata

Recall that an automaton A = (S, M) is globally abelian if Sab = Sba for all a, b ε M.

Proposition 3.3.1. Let A = (S, M) be a globally abelian automaton and π be an S-congruence of A. Then the quotient automaton A/π = (S/π, M) is also globally abelian.

Proof. Let $\bar{S} = S/\pi$ and $\bar{s}$ be the π-class of S containing s. For any a, b ε M, if $\bar{s} \in \bar{S}ab$, then there exists $t \in \bar{s}$ such that t ε Sab = Sba. This implies $\bar{t} \in \bar{S}ba$. But $\bar{t} = \bar{s}$. Therefore $\bar{s} \in \bar{S}ba$ and $\bar{S}ab \subseteq \bar{S}ba$. By symmetry, $\bar{S}ab = \bar{S}ba$ and A/π is globally abelian. #

Corollary. Every globally abelian automaton is a subdirect product of globally abelian irreducible automata. #

Let X be a nonempty set. The *left zero semigroup* on X is the set X together with the operation $*$ defined by $a*b = a$ for all $a, b \varepsilon X$. It is clear that $*$ is associative and that every element of X is left zero.

For the rest of this section, let $A = (S, M)$ be a finite globally abelian automaton with transition monoid $T = T(A)$.

Proposition 3.3.2. The set F of all idempotents of T is a subsemigroup which is a union of left zero semigroups.

Proof. If $\bar e, \bar f \varepsilon F$, then by Proposition 2.3.6, $\bar e\bar x = \bar e\bar x\bar e$ for all $\bar x \varepsilon T$, so that

$$(\bar e\bar f)(\bar e\bar f) = (\bar e\bar f\bar e)\bar f = (\bar e\bar f)\bar f = \bar e\bar f.$$

Hence $\bar e\bar f \varepsilon F$. Therefore F is a subsemigroup.

Define an equivalence relation π on F by $\bar e \equiv \bar f$ (mod π) if $S\bar e = S\bar f$. Clearly, π is a right congruence. Moreover, since A is globally abelian, π is commutative, i.e., $\bar e\bar f \equiv \bar f\bar e$ (mod π) for all $\bar e, \bar f \varepsilon F$. Thus π is a congruence. Let $[\bar e]$ denote the π-class containing $\bar e$. Then $F = \bigcup_{e \varepsilon F} [\bar e]$. We shall show that every π-class is a left zero semigroup. Let $\bar e, \bar f \varepsilon [\bar e]$ and $s \varepsilon S$. Then $s\bar e \varepsilon S\bar e = S\bar f$. Thus $s\bar e = t\bar f$ for some $t \varepsilon S$. We obtain

$$s\bar e\bar f = (t\bar f)\bar f = t\bar f = s\bar e.$$

Therefore $\bar e\bar f = \bar e$ and $[\bar e]$ is a left zero semigroup. This completes the proof. #

Remark. In fact, F is a semilattice (see [8]) of left zero semigroups.

Proposition 3.3.3. In the monoid $\bar{T}$, the following are true.

(i) Every minimal right ideal of T is a group.

(ii) Every principal right ideal generated by an idempotent is a homomorphic image of T.

Proof. (i) Let R be a minimal right ideal of T. Since T is finite, $R = \bar{e}T$ for some idempotent $\bar{e} \in T$. We claim that $\bar{e}$ is the identity of R. To this end, we let $\bar{a} \in R$. Then $\bar{a} = \bar{e}\bar{b}$ for some $\bar{b} \in T$. It is clear that $\bar{e}\bar{a} = \bar{a}$. Moreover, $\bar{a}\bar{e} = (\bar{e}\bar{b})\bar{e} = \bar{e}\bar{b} = \bar{a}$ since $\bar{e}\bar{b}\bar{e} = \bar{e}\bar{b}$ by Proposition 2.3.6. Therefore $\bar{a}\bar{e} = \bar{e}\bar{a} = \bar{a}$ for all $\bar{a} \in R$ and $\bar{e}$ is the identity of R. This together with the fact that R is a minimal right ideal proves that R is a group.

(ii) Let $R = \bar{e}T$ be the principal right ideal generated by an idempotent $\bar{e} \in T$. Define a mapping ϕ of T into $R = \bar{e}T$ by $\bar{t}\phi = \bar{e}\bar{t}$. Clearly ϕ is onto. Moreover, ϕ is a homomorphism, for if $\bar{s}, \bar{t} \in T$, then

$$(\bar{s}\bar{t})\phi = \bar{e}(\bar{s}\bar{t}) = (\bar{e}\bar{s})\bar{t} = (\bar{e}\bar{s}\bar{e})\bar{t} = (\bar{e}\bar{s})(\bar{e}\bar{t}) = (\bar{s}\phi)\cdot(\bar{t}\phi)$$

since $\bar{e}\bar{s}\bar{e} = \bar{e}\bar{s}$ by Proposition 2.3.6. #

Lemma 3.3.4. Every left ideal generated by an idempotent of T is two-sided. Consequently, the minimal ideal I of T is of the form $I = T\bar{e}$ for every idempotent $\bar{e} \in I$.

Proof. Let $\bar{e} \in T$ be an idempotent and $L = T\bar{e}$. If $\bar{a} \in L$, then $\bar{a}\bar{e} = \bar{a}$. Thus for any $\bar{x} \in T$, we have $\bar{a}\bar{x} = (\bar{a}\bar{e})\bar{x} = \bar{a}(\bar{e}\bar{x})$ $= \bar{a}(\bar{e}\bar{x}\bar{e}) \in T\bar{e} = L$ since $\bar{e}\bar{x} = \bar{e}\bar{x}\bar{e}$ by Proposition 2.3.6. Therefore L is a two-sided ideal.

Since T is finite, the last statement follows immediately from the above. #

A semigroup T is a left group if T is left simple and right cancellative. For a finite semigroup T, T is left simple if and only if T is right cancellative. Thus if T is finite, then either condition implies that T is a left group.

Proposition 3.3.5. The minimal ideal of T is a left group.

Proof. Let I be the minimal ideal of T. Since T is finite, so is I. By the above remark, it suffices to show that I is left simple.

Let $\bar{a} \in I$. Then evidently $I\bar{a} \subseteq I$. Conversely, since T is finite, there exists a positive integer n such that $\bar{a}^n = e$ is an idempotent. Clearly $\bar{e} \in I$ and $I\bar{a} \supseteq I\bar{a}^n$, $= I\bar{e}$. But $I\bar{e} = T\bar{e}$ since I is an ideal and $\bar{e} \in I$ is an idempotent. Moreover, $T\bar{e}$ is a two-sided ideal by Lemma 3.3.4. Thus $I\bar{a} \supseteq T\bar{e} \supseteq I$ by the minimality of I. Therefore $I\bar{a} = I$ and I is left simple. #

CHAPTER 4

RP-REGULAR LANGUAGES AND LP-REGULAR LANGUAGES

In this chapter, we shall define two subfamilies of regular languages, namely RP-regular languages and LP-regular languages, and study their algebraic characterizations. Before doing so, we recall some well-known properties of regular languages, which are needed for the subsequent discussion.

4.1. Some Properties of Regular Languages

Let U and V be languages over an alphabet X. The union or sum of U and V is denoted by U + V, their intersection by $U \cap V$ and complement of U by $\overline{U}$.

The product or concatenation of U and V is the language $UV = \{uv | u \in U, v \in V\}$. The star operation or iteration of U is the language $U^* = \sum_{n=0}^{\infty} U^n$ where $U^0 = \{\Lambda\}$ and $U^n = U^{n-1}U$ for $n > 0$. If $U = \{w\}$ where $w \in X^*$, then we write $U^* = w^*$.

The transpose or mirror $\tilde{U}$ of U is the language $\tilde{U} = \{\tilde{u} | u \in U\}$ where $\tilde{u} = x_k x_{k-1} \ldots x_2 x_1$ if $u = x_1 x_2 \ldots x_{k-1} x_k$ and $x_i \in X$ for $i = 1, \ldots, k$. We set $\tilde{\Lambda} = \Lambda$.

Recall that an acceptor over an alphabet X is a quintuple $\hat{A} = (S, X, \delta, s_0, F)$ where $A = (S, X, \delta)$ is a finite f.i. automaton over X, $s_0 \in S$ is the initial state and $F \subseteq S$ is the set of final states. The language accepted by $\hat{A}$ is denoted by $L(\hat{A}) = \{x \mid x \in X^*, (s_0)x\delta \in F\}$. For any acceptor $\hat{A}$, its automaton is always denoted by A.

Let X be an alphabet and $\mathcal{A}$ be a family of f.i. automata over X. If Γ is the family of languages accepted by acceptors whose automata are in $\mathcal{A}$, then we say that Γ is <u>defined by $\mathcal{A}$</u>. Thus Γ is defined by $\mathcal{A}$ if for any $U \subseteq X^*$, $U \in \Gamma$ if and only if there exists an acceptor $\hat{A}$ such that $L(\hat{A}) = U$ and $A \in \mathcal{A}$.

Recall that a trivial automaton is an automaton with only one state.

<u>Lemma 4.1.1.</u> Let $\mathcal{A}$ be a family of f.i. automata over an alphabet X and Γ be the family of languages defined by $\mathcal{A}$. If $\mathcal{A}$ contains trivial automata, then the languages X^* and $\emptyset$ are in Γ.

<u>Proof.</u> Let $C = (S = \{s_0\}, X, \delta)$ be a trivial automaton in $\mathcal{A}$, and $\hat{A} = (S = \{s_0\}, X, \delta, s_0, F = \{s_0\})$. Then $L(\hat{A}) = X^*$ and $A = C \in \mathcal{A}$.

On the other hand, let $\hat{B} = (S = \{s_0\}, X, \delta, s_0, F = \emptyset)$. Then $L(\hat{B}) = \emptyset$ and $B = C \in \mathcal{A}$.

Therefore X^* and $\emptyset$ are in Γ. #

Lemma 4.1.2. Let $\mathcal{A}$ be a family of automata over an alphabet X. Then the family Γ of languages defined by $\mathcal{A}$ is closed under taking complements. Moreover, if $\mathcal{A}$ is closed under taking direct products, then Γ is closed under union and intersection.

Proof. If $U \varepsilon \Gamma$, then there exists an acceptor $\hat{A} = (S, X, \delta, s_0, F)$ such that $U = L(\hat{A})$ and $A \varepsilon \mathcal{A}$. Let $\hat{B} = (S, X, \delta, s_0, \overline{F})$ where $\overline{F} = S - F$. Then it is immediate that $\overline{U} = L(\hat{B})$ and $B = A \varepsilon \mathcal{A}$. This proves $\overline{U} \varepsilon \Gamma$.

Now suppose $\mathcal{A}$ is closed under taking direct products and $U, V \varepsilon \Gamma$. Let $\hat{A} = (S^A, X, \delta^A, s_0^A, F^A)$ ~~and~~ $\hat{B} = (S^B, X, \delta^B, s_0^B, F^B)$ be the acceptors such that $U = L(\hat{A})$ and $V = L(\hat{B})$, and $A, B \varepsilon \mathcal{A}$. Define $\hat{C} = (S^C, X, \delta^C, s_0^C, F^C)$ to be the acceptor whose automaton is the direct product of A and B, i.e., $C = (S^C, X, \delta^C) = (S^A \times S^B, X, \delta^A \times \delta^B) = A \times B$, with $s_0^C = (s_0^A, s_0^B)$ and $F^A = (F^A \times S^B) \cup (S^A \times F^B)$. Then by hypothesis, $C \varepsilon \mathcal{A}$. It can be shown (see [11]) that $U + V = L(\hat{C})$. Therefore $U + V \varepsilon \Gamma$.

On the other hand, if $\hat{D} = (S^D, X, \delta^D, s_0^D, F^D)$ is the acceptor where $D = A \times B$, $s_0^D = (s_0^A, s_0^B)$ and $F^D = F^A \times F^B$, then it can be shown (see [11]) that $U \cap V = L(\hat{D})$. With $D = A \times B \varepsilon \mathcal{A}$, we obtain $U \cap V \varepsilon \Gamma$. #

Combining these two lemmas, we have the following.

Proposition 4.1.3. Let $\mathcal{A}$ be a family of f.i. automata over an alphabet X and Γ be the family of languages defined by

A. If $\mathcal{W}$ contains trivial automata and is closed under taking direct products, then Γ is a boolean algebra. #

Corollary. The family of regular languages over an alphabet X is a boolean algebra. #

Let T be a semigroup. For any subset H of T and any $a \in T$, we define

(i) $H.^{\cdot}a = \{x \mid ax \in H, x \in T\}$.

(ii) $H^{\cdot}.a = \{x \mid xa \in H, x \in T\}$.

(iii) $H..a = \{(x, y) \mid xay \in H, x, y \in T\}$.

(iv) $a \equiv b \pmod{R_H}$ if $H.^{\cdot}a = H.^{\cdot}b$.

(v) $a \equiv b \pmod{{}_H R}$ if $H^{\cdot}.a = H^{\cdot}.b$.

(vi) $a \equiv b \pmod{R_{[H]}}$ if $H..a = H..b$.

It can be shown (see [2]) that R_H is a right congruence on T, ${}_H R$ is a left congruence on T and $R_{[H]}$ is a congruence on T. They are called, respectively, the principal right congruence, the principal left congruence and the principal congruence determined by H. Moreover, if T is a monoid, then H is a union of some classes of R_H, ${}_H R$ and $R_{[H]}$.

Now let X be an alphabet and U be a language over X. Then U is a subset of X^*. Using the relations, R_U, ${}_U R$ and $R_{[U]}$, an algebraic characterization of regular languages can be obtained as follows:

Theorem 4.1.4. Let U be a language over an alphabet X. The following are equivalent.

(i) U is a regular language.

(ii) U is a union of some classes of a congruence of finite index of X*.

(iii) U is a union of some classes of a right congruence of finite index of X*.

(iv) U is a union of some classes of a left congruence of finite index of X*.

(v) The principal congruence $R_{[U]}$ is of finite index.

(vi) The principal right congruence R_U is of finite index.

(vii) The principal left congruence ${}_UR$ is of finite index.

(viii) U is accepted by an acceptor over X. #

For the proof of the above theorem, the reader is referred to [9] and [11].

Let R be an equivalence relation on the free monoid X* generated by an alphabet X. The <u>transpose</u> $\tilde{R}$ of R is defined by

$$x \equiv y \pmod{\tilde{R}} \text{ if } \tilde{x} \equiv \tilde{y} \pmod{R}.$$

It can be easily shown (see [11]) that $\tilde{R}$ is an equivalence relation of same index as R over X* and $\tilde{\tilde{R}} = R$. Moreover, R is a right congruence if and only if $\tilde{R}$ is a left congruence, and vice versa.

<u>Lemma 4.1.5.</u> Let U be a language over an alphabet X and R be an equivalence relation on X*. Then U is a union of

some R-classes if and only if $\tilde{U}$ is a union of some $\tilde{R}$-classes.

<u>Proof</u>. Since $\tilde{\tilde{R}} = R$, it suffices to prove the implication one way.

Suppose U is a union of some R-classes. Let $a \equiv b \pmod{\tilde{R}}$ and $a \in \tilde{U}$. Then $\tilde{b} \in U$ since $\tilde{a} \equiv \tilde{b} \pmod{R}$ and $\tilde{a} \in U$. Therefore $b \in \tilde{U}$ and $\tilde{U}$ is a union of some $\tilde{R}$-classes. #

<u>Proposition 4.1.6</u>. Let U be a language over an alphabet X. Then the transpose $\tilde{R}_U$ of the principal right congruence R_U determined by U is the principal left congruence ${}_{\tilde{U}}R$ determined by the transpose $\tilde{U}$ of U, i.e., $\tilde{R}_U = {}_{\tilde{U}}R$. Dually, ${}_U\tilde{R} = R_{\tilde{U}}$.

<u>Proof</u>. We shall prove $\tilde{R}_U = {}_{\tilde{U}}R$ only, since a dual argument will show ${}_U\tilde{R} = R_{\tilde{U}}$.

Suppose $a \equiv b \pmod{\tilde{R}_U}$ then $\tilde{a} \equiv \tilde{b} \pmod{R_U}$. Let $x \in \tilde{U}\cdot .a$. We have $xa \in \tilde{U}$ hence $\tilde{a}\tilde{x} = \widetilde{xa} \in U$ and $\tilde{x} \in U.\cdot\tilde{a} = U.\cdot\tilde{b}$. Therefore $\widetilde{xb} = \tilde{b}\tilde{x} \in U$ and $xb \in \tilde{U}$ hence $x \in \tilde{U}\cdot .b$. Consequently $\tilde{U}\cdot .a \subseteq \tilde{U}\cdot .b$. By symmetry, $\tilde{U}\cdot .a = \tilde{U}\cdot .b$ and $a \equiv b \pmod{{}_{\tilde{U}}R}$.

Conversely, let $a \equiv b \pmod{{}_{\tilde{U}}R}$ and $x \in U.\cdot\tilde{a}$. Then $\tilde{a}x \in U$ hence $\tilde{x}a = \widetilde{\tilde{a}x} \in \tilde{U}$. This implies $\tilde{x} \in \tilde{U}\cdot .a = \tilde{U}\cdot .b$ therefore $\tilde{x}b \in \tilde{U}$ and $\tilde{b}x \in U$. Thus $x \in U.\cdot\tilde{b}$ and $U.\cdot\tilde{a} \subseteq U.\cdot\tilde{b}$. By symmetry, $U.\cdot\tilde{a} = U.\cdot\tilde{b}$ and $\tilde{a} \equiv \tilde{b} \pmod{R_U}$ which implies $a \equiv b \pmod{\tilde{R}_U}$. #

Let U be a regular language over an alphabet X. By Theorem 4.1.4, the principal right congruence R_U is of finite index and U is a union of R_U-classes. Let $S = \{\overline{a} \mid a \in X^*\}$ where $\overline{a}$ denotes the R_U-class containing a. Then S is finite. Define $\hat{A}(R_U) = (S, X, \delta, s_0, F)$ where $(\overline{a})x\delta = \overline{ax}$ for every $\overline{a} \in S$ and $x \in X$, $s_0 = \overline{\Lambda}$ and $F = \{\overline{u} \mid u \in U\}$. Then $\hat{A}(R_U)$ is an acceptor over X. It can be shown (see [9] and [11]) that $U = L(\hat{A}(R_U))$ and that if $\hat{B} = (S^B, X, \delta^B, s_0^B, F^B)$ is any acceptor equivalent to $\hat{A}(R_U)$, then $|S| \leq |S^B|$. In view of this property, the acceptor $\hat{A}(R_U)$ is called the <u>reduced acceptor</u> accepting U.

The following is a well-known theorem (see [7]) which links the structure of a regular language and the structure of an automaton.

<u>Theorem 4.1.7.</u> Let U be a regular language over an alphabet X, and $\hat{A}(R_U)$ be the reduced acceptor accepting U. Then $S(U) = T(A)$ where A is the automaton of $\hat{A}(R_U)$. #

4.2. <u>RP-Regular Languages</u>

Let X be an alphabet. An acceptor $\hat{A}$ over X is <u>right prime</u> if its automaton A is right prime. Let $\mathcal{A}_R$ be the family of right prime f.i. automata over X and Γ_R be the family of languages defined by $\mathcal{A}_R$. A language U over X is <u>RP-regular</u> if $U \in \Gamma_R$. Thus a language U is RP-regular if and only if it is accepted by a right prime acceptor.

<u>Proposition 4.2.1</u>. The family Γ_R of RP-regular languages over an alphabet X is a boolean algebra.

<u>Proof</u>. This follows from Propositions 2.1.10 and 4.1.3. #

<u>Proposition 4.2.2</u>. For every RP-regular language U over an alphabet X, there exists a connected right prime acceptor accepting U.

<u>Proof</u>. Let $U = L(\hat{A})$ where $\hat{A}$ is a right prime acceptor over X. Then its automaton A is right prime. By Proposition 1.5.1, there exists a connected acceptor $\hat{B}$ over X, whose automaton B is a subautomaton of A such that $U = L(\hat{B})$. By Proposition 2.1.10, B is right prime. Hence $\hat{B}$ is a connected right prime acceptor accepting U. #

Let M be a monoid and R be a right congruence on M. Let $M/R = \{[m] \mid m \in M\}$ be the set of all R-classes [m] of M. Define

$$([m])a\eta = [ma] \text{ for all } [m] \in M/R \text{ and } a \in M.$$

Since R is a right congruence on M, η is well-defined. Hence the triple $(M/R, M, \eta)$ becomes an M-automaton called <u>the M-automaton induced by R</u> and denoted by A(M/R). If R is of finite index, then M/R is finite and A(M/R) is a finite automaton.

Recall that an equivalence relation R on a monoid M is right prime if for any a, b, c $\in$ M, $axc \equiv bxc \pmod R$ for all $x \in M$ implies $a \equiv b \pmod R$.

Theorem 4.2.3. Let U be a language over an alphabet X. Then the following are equivalent.

(i) U is RP-regular.

(ii) U is a union of some classes of a congruence on X^*, which is right prime and of finite index.

(iii) U is a union of some classes of a right congruence on X^*, which is right prime and of finite index.

Proof. (i) implies (ii). Let U be RP-regular. Then there exists a right prime acceptor $\hat{A} = (S, X, \delta, s_0, F)$ such that $U = L(\hat{A})$. It is known (see [9] and [11]) that U is a union of some classes of the congruence E_S on X^*. Since S is finite, E_S is of finite index. Moreover, from the proof of Proposition 2.1.6, we see that E_S is right prime. Therefore (ii) holds.

(ii) implies (iii). Obvious.

(iii) implies (i). Let U be a union of some R-classes of a right prime right congruence R on X^* of finite index. Then the automaton $A(X^*/R)$ induced by R is a finite automaton. Let $\hat{A} = (X^*/R, X, \eta, s_0, F)$ be the acceptor with $A = A(X^*/R)$, $s_0 = [\Lambda]$ and $F = \{[u] | u \in U\}$. Then it can be shown (see [9] and [11]) that $U = L(\hat{A})$.

Moreover, $A(X^*/R)$ is right prime. For suppose $[a]xc = [b]xc$ for all $x \in X^*$; then $[axc] = [bxc]$ for all $x \in X^*$. That is, $axc \equiv bxc \pmod{R}$ for all $x \in X^*$. This implies $a \equiv b \pmod{R}$ since R is right prime. Thus

[a] = [b] and A(X*/R) is right prime. Therefore U is RP-regular. #

We shall give an example in the next section to show that the principal right congruence R_U of an RP-regular language U need not be right prime.

4.3. LP-Regular Languages

An acceptor A over an alphabet X is left prime if its automaton is left prime. Let A_L be the family of left prime f.i. automata over X and Γ_L be the family of languages defined by A_L. A language U over X is LP-regular if $U \in \Gamma_L$. Thus a language U is LP-regular if and only if U is accepted by a left prime acceptor.

Proposition 4.3.1. The family Γ_L of LP-regular languages over an alphabet X is a boolean algebra.

Proof. This follows from Propositions 2.2.12 and 4.1.3. #

Proposition 4.3.2. For every LP-regular language U over an alphabet X, there exists a connected left prime acceptor accepting U.

Proof. This proof is analogous to that of Proposition 4.2.2. Let $U = L(\hat{A})$ where $\hat{A}$ is a left prime acceptor over X. Then its automaton A is left prime. By Proposition 1.5.1, there exists a connected acceptor $\hat{B}$ over X, whose automaton B is a subautomaton of A, such that $U = L(\hat{B})$.

By Proposition 2.2.12, B is left prime. Hence $\hat{B}$ is a connected left prime acceptor accepting U. #

Recall that an equivalence relation R on a monoid M is left prime if for any a, b, c ϵ M, cxa $\equiv$ cxb (mod R) for all x ϵ M implies a $\equiv$ b (mod R).

First, we prove the following.

Lemma 4.3.3. Let U be a language over an alphabet X. Then U is LP-regular if and only if U is a union of some classes of a congruence on X* which is left prime and of finite index.

Proof. Necessity. Let U be LP-regular. Then there exists a left prime acceptor $\hat{A} = (S, X, \delta, s_0, F)$ such that $U = L(\hat{A})$. It is known (see [9] and [11]) that U is a union of some classes of the congruence E_S on X*. Since S is finite, E_S is of finite index. Moreover, by Corollary 1 to Proposition 2.2.8, E_S is left prime.

Sufficiency. Let U be a union of some R-classes of a left prime congruence R on X* of finite index. Then the automaton A(X*/R) induced by R is a finite automaton. Let $\hat{A} = (X^*/R, X, \delta, s_0, F)$ be the acceptor with A = A(X*/R), $s_0 = [\Lambda]$ and $F = \{[u] | u \ \epsilon \ U\}$. Then it can be shown (see [9] and [11]) that $U = L(\hat{A})$.

Moreover, $\hat{A}(X^*/R)$ is left prime. For suppose [c]xa = [c]xb for all x ϵ X*, then [cxa] = [cxb] for all x ϵ X*. That is, cxa $\equiv$ cxb (mod R) for all x ϵ X* so that

$a \equiv b \pmod{R}$ since R is left prime. But R is a congruence; therefore $xa \equiv xb \pmod{R}$ for all $x \in X^*$. Hence $[x]a = [xa] = [xb] = [x]b$ for all $[x] \in X^*/R$. This implies that the automaton $A(X^*/R)$ is left prime and U is LP-regular. #

Before we set out to establish an analogue of Theorem 4.2.3 for LP-regular languages, we shall first consider a relation between RP-regular languages and LP-regular languages.

Lemma 4.3.4. Let R be an equivalence relation on the free monoid X^* generated by an alphabet X. Then R is right prime if and only if its transpose $\tilde{R}$ is left prime and vice versa.

Proof. Since $\tilde{\tilde{R}} = R$, it suffices to prove the implication one way.

Let R be right prime. Suppose for some $a, b, c \in X^*$ $cxa \equiv cxb \pmod{\tilde{R}}$ for all $x \in X^*$, then $\widetilde{axc} \equiv \widetilde{bxc} \pmod{R}$ for all $x \in X^*$, i.e., $\tilde{a}y\tilde{c} \equiv \tilde{b}y\tilde{c} \pmod{R}$ for all $y \in X^*$. Thus $\tilde{a} \equiv \tilde{b} \pmod{R}$ since R is right prime. Therefore $a \equiv b \pmod{\tilde{R}}$ and $\tilde{R}$ is left prime. #

Proposition 4.3.5. Let U be a language over an alphabet X. Then U is RP-regular if and only if its transpose $\tilde{U}$ is LP-regular.

Proof. Necessity. Let U be RP-regular. Then by Theorem 4.2.3.(iii), U is a union of some classes of a right prime congruence R on X^* of finite index. Applying Lemmas 4.1.5

and 4.3.4, we obtain that the transpose $\tilde{U}$ is a union of some classes of $\tilde{R}$ on X*, which is left prime and of finite index. Therefore by Lemma 4.3.3, $\tilde{U}$ is LP-regular.

The sufficiency follows by a similar argument. #

Following Thierrin [10], a language over an alphabet X is called p-regular if it is accepted by an acceptor whose automaton is a permutation automaton. As a corollary to the above Proposition, we have the following.

Corollary. Let U be a language over one letter. The following are equivalent.

(i) U is RP-regular.

(ii) U is LP-regular.

(iii) U is p-regular.

Proof. The equivalence of (i) and (ii) is due to the fact that $\tilde{U}$ = U in this case, while the equivalence of (i) and (iii) follows from Corollary 2 to Proposition 2.4.2. #

We are now able to prove the desired result.

Theorem 4.3.6. Let U be a language over an alphabet X. Then the following are equivalent.

(i) U is LP-regular.

(ii) U is a union of some classes of a congruence on X*, which is left prime and of finite index.

(iii) U is a union of some classes of a left congruence X*, which is left prime and of finite index.

Proof. The equivalence of (i) and (ii) has been proved in

Lemma 4.3.3.

(ii) implies (iii). This is immediate.

(iii) implies (i). Let U be a union of some R-classes of a left prime left congruence R of finite index. Then the transpose $\check{R}$ of R is a right congruence on X* of finite index. Moreover, by Lemma 4.3.4, $\check{R}$ is right prime. But the transpose $\check{U}$ of U is a union of some $\check{R}$-classes by Lemma 4.1.5. Therefore by Theorem 4.2.3, $\check{U}$ is RP-regular. Applying Proposition 4.3.5, we obtain that U is LP-regular. #

Let U be a language over an alphabet X. Thierrin has shown [10] that the following are equivalent.

(i) U is p-regular.

(ii) U is the union of some classes of a right cancellative right congruence on X* of finite index.

(iii) The principal right congruence R_U on X* is right cancellative and of finite index. #

Since every right cancellative equivalence relation is right prime, every p-regular language is RP-regular. It would then be interesting if the principal right congruence R_U of an RP-regular language U is right prime. This is not the case as we shall see in the following example.

Example 4.3.7. Let A = (S, X) be the f.i. automaton over

$X = \{a, b\}$, with $S = \{1, 2, 3, 4\}$ and the following transition table.

	a	b
1	3	2
2	2	4
3	1	2
4	4	3

It can be easily seen that A is strongly connected and therefore left prime. Thus the congruence E_S induced by A on X^* is left prime.

It is easy to check that

$$X^*/E_S = \{[\Lambda], [a], [b], [ba], [b^2], [b^2a], [b^3], [b^3a]\}$$

where $[u]$ denotes the E_S-class containing u. By Theorem 4.3.6, every class of E_S is LP-regular.

Let $U = [a] = \{a^{2n+1} | n \geq 0\}$. Then U is LP-regular. We have

$$U^{\cdot}.\Lambda = U,$$

$$U^{\cdot}.a = Ua,$$

$$U^{\cdot}.x = \emptyset, \text{ for all } x \notin [\Lambda] \cup [a].$$

Therefore $bxb \equiv bx\Lambda \pmod{{}_UR}$ for all $x \in X^*$. But $b \not\equiv \Lambda \pmod{{}_UR}$. This implies that ${}_UR$ is not left prime.

Moreover $\check{U} = U$. By Proposition 4.3.5, U is also RP-regular. By Proposition 4.1.6, $R_U = R_{\check{U}} = {}_{\check{U}}R$. Therefore R_U is not right prime by Lemma 4.3.4. ‡

Thus we have a language U which is both RP-regular and LP-regular, and yet neither the principal right congruence R_U is right prime nor the principal left congruence ${}_UR$ is left prime. Consequently, we are led to consider more restricted classes of regular languages, which we shall define and discuss in the following section.

4.4. Strictly RP-Regular Languages and Strictly LP-Regular Languages.

Let U be a language over an alphabet X. Then U is

(i) strictly RP-regular if the principal right congruence R_U on X* is right prime and of finite index;

(ii) strictly LP-regular if the principal left congruence ${}_UR$ on X* is left prime and of finite index.

We shall denote the families of strictly RP-regular languages and strictly LP-regular languages by $\Gamma_{\bar{R}}$ and $\Gamma_{\bar{L}}$ respectively. Clearly, $\Gamma_{\bar{R}}$ and $\Gamma_{\bar{L}}$ are proper subfamilies of Γ_R and Γ_L respectively.

We have the following immediate result.

Proposition 4.4.1. Let U be a language over an alphabet X. Then the following hold.

(i) U is strictly RP-regular if and only if for any $a, b, c \in X^*$, $U.^{\cdot}axc = U.^{\cdot}bxc$ for all $x \in X^*$ implies $U.^{\cdot}a = U.^{\cdot}b$.

(ii) U is strictly LP-regular if and only if for any $a, b, c \in X^*$, $U^{\cdot}.cxa = U^{\cdot}.cxb$ for all $x \in X^*$ implies $U^{\cdot}.a = U^{\cdot}.b$. #

Proposition 4.4.2. Let U be a language over an alphabet X. Then U is strictly RP-regular if and only if its transpose $\tilde{U}$ is strictly LP-regular.

Proof. Necessity. Let U be strictly RP-regular. Then the principal right congruence R_U on X* is right prime and of finite index. Therefore its transpose $\tilde{R}_U$ is of finite index. Further, $\tilde{R}_U$ is left prime by Lemma 4.3.4. But $\tilde{R}_U = {}_{\tilde{U}}R$, by Proposition 4.1.6. Therefore $\tilde{U}$ is strictly LP-regular.

The sufficiency follows by a similar argument. #

Proposition 4.4.3. The languages X* and Ø are both strictly RP-regular and strictly LP-regular.

Proof. Since the relations R_{X^*}, $R_{\emptyset}$, ${}_{X^*}R$ and ${}_{\emptyset}R$ are all equal to the universal congruence, they are trivially right prime and left prime. #

Proposition 4.4.4. Let U be a language over X. Then the following statements hold.

(i) If U is strictly RP-regular, then so is $\overline{U}$.

(ii) If U is strictly LP-regular, then so is $\overline{U}$.

Proof. These follow immediately from the fact that $R_{\overline{U}} = R_U$ and ${}_{\overline{U}}R = {}_{U}R$. #

Since right cancellative aquivalence relations are right prime, every p-regular language is strictly RP-regular. For the converse, if $|X| = 1$, then a stronger result holds, namely, every RP-regular language is p-regular (see the Corollary to Proposition 4.3.5); but if $|X| > 1$, this is no longer true. The following is an example, in which $|X| = 2$ and the language U is strictly RP-regular but not p-regular.

Example 4.4.5. Let $X = \{a, b\}$ and $U \triangleq aX^*b$. Then we have

$$U.^{\cdot}ax = X^*b \quad \text{for all } x \in X^*,$$
$$U.^{\cdot}bx = \emptyset \quad \text{for all } x \in X^*,$$
$$U.^{\cdot}\Lambda = U.$$

Thus R_U has three classes, namely $[\Lambda]$, $[a]$, $[b]$. The reduced automaton $A(R_U)$ is as follows.

$A(R_U)$	a	b
$[\Lambda]$	$[a]$	$[b]$
$[a]$	$[a]$	$[a]$
$[b]$	$[b]$	$[b]$

It can be checked that the transition monoid $T(A)$ of $A(R_U)$ has three elements, namely $\bar{\Lambda}$, $\bar{a}$, $\bar{b}$, and the following table.

$T(A)$	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$
$\bar{\Lambda}$	$\bar{\Lambda}$	$\bar{a}$	$\bar{b}$
$\bar{a}$	$\bar{a}$	$\bar{a}$	$\bar{a}$
$\bar{b}$	$\bar{b}$	$\bar{b}$	$\bar{b}$

Clearly $T(A) = H \cup \{\bar{\Lambda}\} = H^1$ where $H = \{\bar{a}, \bar{b}\}$ is a right cancellative semigroup. Thus by Proposition 2.1.7, $T(A)$ is right prime and hence R_U is right prime. This implies that U is strictly RP-regular, But R_U is not right cancellative, for $\Lambda a \equiv aa \pmod{R_U}$ and $\Lambda \not\equiv a \pmod{R_U}$. Therefore U is not p-regular. #

We have shown that both Γ_R and Γ_L are boolean algebras. However, $\Gamma_{\bar{R}}$ and $\Gamma_{\bar{L}}$ are not boolean algebras, since they are not closed under intersection. To show this, we consider the following example.

<u>Example 4.4.6</u>. Let $X = \{a, b\}$. Let $U = aX^*b$ be the strictly RP-regular language and let

$$V = \{w \in X^* \mid N_a(w)=2n+1,\ N_b(w)=2m,\ n, m \geq 0\}$$

where $N_a(w)$ denotes the number of a's appearing in w.

We shall show that V is also strictly RP-regular. It is easily seen that $x \equiv y \pmod{R_V}$ if and only if $N_a(x) \equiv N_a(y) \pmod 2$ and $N_b(x) \equiv N_b(y) \pmod 2$. Thus R_V has four classes, namely $[\Lambda]$, $[a]$, $[b]$ and $[ab]$. The reduced automaton $A(R_V)$ is as follows.

$A(R_V)$	a	b
$[\Lambda]$	$[a]$	$[b]$
$[a]$	$[\Lambda]$	$[ab]$
$[b]$	$[ab]$	$[\Lambda]$
$[ab]$	$[b]$	$[a]$

It is clear that $A(R_V)$ is a permutation automaton. Thus V is p-regular and hence strictly RP-regular.

Now let $L = U \cap V$. Then

$$L = \{awb \mid w \in X^*,\ N_a(w)=2n,\ N_b(w)=2m+1,\ n, m \geq 0\}.$$

It can be checked that

$$axa \equiv ab^2xa \pmod{R_L} \quad \text{for all } x \in X^*.$$

But $a \not\equiv ab^2 \pmod{R_L}$ since

$L.\cdot a = \{wb \mid w \in X^*, N_a(w)=2n, N_b(w)=2m+1, n, m \geq 0\}$ and

$L.\cdot ab^2 = \{\Lambda\} \cup \{wb \mid w \in X^*, N_a(w)=2n, N_b(w)=2m+1, n, m \geq 0\}$.

Therefore R_L is not right prime and L is not strictly RP-regular. This implies that $\Gamma_{\bar{R}}$ is not closed under intersection.

By virtue of Proposition 4.4.2, $\tilde{U}$ and $\tilde{V}$ are strictly LP-regular, and $\tilde{L}$ is not strictly LP-regular. But $\tilde{L} = \tilde{U} \cap \tilde{V}$. Thus $\Gamma_{\bar{L}}$ is not closed under intersection either. Therefore neither of $\Gamma_{\bar{R}}$ and Γ_L is boolean algebra. #

In the following, we shall study some properties of strictly RP-regular languages and strictly LP-regular languages.

Recall that the syntactic monoid S(U) of a language U over an alphabet X is a quotient monoid of X* modulo P_U, where P_U is defined by $x \equiv y \pmod{P_U}$ if for every $u, v \in X^*$, $uxv \in U$ if and only if $uyv \in U$. Observe that $x \equiv y \pmod{P_U}$ if and only if $\tilde{x} \equiv \tilde{y} \pmod{P_{\tilde{U}}}$. Therefore $P_{\tilde{U}} = \tilde{P}_U$ and $S(\tilde{U})$ is dual to S(U).

<u>Theorem 4.4.7.</u> Let X be an alphabet and U be a language over X. Then

(i) if U is strictly RP-regular, then its syntactic monoid S(U) is right prime;

(ii) if U is strictly LP-regular, then its syntactic monoid S(U) is left prime.

Proof. (i) If U is strictly RP-regular, then its principal right congruence R_U is right prime. Hence the reduced automaton $A(R_U)$ is right prime and by Proposition 2.1.6, the transition monoid T(A) of $A(R_U)$ is right prime. But S(U) is isomorphic to T(A) by Theorem 4.1.7. Therefore S(U) is right prime.

(ii) If U is strictly LP-regular, then its transpose $\tilde{U}$ is strictly RP-regular by Proposition 4.4.2. Thus $S(\tilde{U})$ is right prime by part (i). But S(U) is dual to $S(\tilde{U})$. Therefore S(U) is left prime. #

Proposition 4.4.8. Let U be a nonempty subset of X*. Then

(i) if U is strictly RP-regular, then $U..x \neq \emptyset$ for all $x \in X^*$;

(ii) if U is strictly LP-regular, then $U..x \neq \emptyset$ for all $x \in X^*$.

Proof. (i) If U = X*, then it is immediate. If U is a proper subset of X*, then the principal right congruence R_U of U is not ~~the~~ universal congruence. Thus there exist $a, b \in X^*$ such that $a \not\equiv b \pmod{R_U}$. Suppose U is strictly RP-regular and $U..c = \emptyset$ for some $c \in X^*$. Then $U..axc = \emptyset = U..bxc$ for all $x \in X^*$. By Proposition 4.4.1.(i), $U..a = U..b$. This implies $a \equiv b \pmod{R_U}$, contrary to the choice of a and b.

Part (ii) follows by a similar argument. #

Corollary. Every strictly RP-regular language is infinite and so is every strictly LP-regular language.

Proof. We only prove the assertion for strictly RP-regular languages; the proof for strictly LP-regular languages is similar.

Let U be a strictly RP-regular language. If U is finite, then $n = \max \{|u| \mid u \in U\}$ exists. Let $a \in X^*$ be such that $|a| > n$. Then $U..a = \emptyset$. This is a contradiction by the Proposition. #

Lemma 4.4.9. Let U be a language over an alphabet X and $a \in X^*$. Then

(i) $x \equiv y \pmod{R_{U..a}}$ if and only if $ax \equiv ay \pmod{R_U}$;

(ii) if R_U is of finite index n, then $R_{U..a}$ is of finite index m and $m \leq n$.

Proof. (i) $x \equiv y \pmod{R_{U..a}}$ if and only if $(U..a)..x = (U..a)..y$ if and only if $U..ax = U..ay$ if and only if $ax \equiv ay \pmod{R_U}$.

(ii) Since R_U is of finite index n, the set A of representatives (one from each class) of R_U-classes is finite and has n elements, say $A = \{a_1, \ldots, a_n\}$. Let $B = \{b \in A \mid ay \equiv b \pmod{R_U}$ for some $y \in X^*\}$. Then $B = \{b_1, \ldots, b_k\} \subseteq A$ and $k \leq n$. For each $b_i \in B$, choose one $r_i \in X^*$ such that $ar_i \equiv b_i \pmod{R_U}$ and let

$T = \{r_1, \ldots, r_k\}$. For every $x \varepsilon X^*$, there exists $a_i \varepsilon A$ such that $ax \equiv a_i \pmod{R_U}$ since A is a set of representatives of R_U-classes. Thus $a_i \varepsilon B$ and $a_i = b_j$ for some j, $1 \leq j \leq k$. Hence $ar_j \equiv b_j \pmod{R_U}$ where $r_j \varepsilon T$. Consequently, $ax \equiv ar_j \pmod{R_U}$ and $x \equiv r_j \pmod{R_{U.\cdot a}}$ by part (i). This proves that T contains a set of representatives of $R_{U.\cdot a}$-classes. Thus $R_{U.\cdot a}$ is of finite index m and $m \leq k \leq n$.

The proof of (ii) is due to Thierrin (cf. [10], Theorem 2.3(ii)).

Proposition 4.4.10. Let U be a language over an alphabet X. Then

(i) U is strictly RP-regular if and only if $U.\cdot a$ is strictly RP-regular for every $a \varepsilon X^*$;

(ii) U is strictly LP-regular if and only if $U\cdot.a$ is strictly LP-regular for every $a \varepsilon X^*$.

Proof. (i) Necessity. Assume U is strictly RP-regular; then the principal right congruence R_U is right prime and of finite index. Suppose $uxc \equiv vxc \pmod{R_{U.\cdot a}}$ for all $x \varepsilon X^*$; then by Lemma 4.4.9(i), $auxc \equiv avxc \pmod{R_U}$ for all $x \varepsilon X^*$. But R_U is right prime so that $au \equiv av \pmod{R_U}$ and $u \equiv v \pmod{R_{U.\cdot a}}$. Thus $R_{U.\cdot a}$ is right prime. Moreover, R_U is of finite index and hence, by Lemma 4.4.9(ii), $R_{U.\cdot a}$ is also of finite index. Therefore $U.\cdot a$ is strictly RP-regular.

The sufficiency follows from the fact that $U = U..\Lambda$. #

A language U over an alphabet X is bounded (see [4]) if there exist a finite number of words $w_1, w_2, \ldots, w_n \in X^*$ such that $U \subseteq w_1^* w_2^* \ldots w_n^*$.

Proposition 4.4.11. Let X be an alphabet with $|X| \geq 2$. Then no bounded language over X can be strictly RP-regular or strictly LP-regular.

Proof. Let U be a bounded language over X. Then there exist a finite number of words $w_1, w_2, \ldots, w_n \in X^*$ such that $U \subseteq w_1^* w_2^* \ldots w_n^*$. By Proposition 4.4.8, it suffices to show $U..v = \emptyset$ for some $v \in X^*$. Suppose there exists $a \in X$ such that a does not appear in any of $w_1, \ldots, w_n$. Then clearly $U..a = \emptyset$ since $U \subseteq w_1^* w_2^* \ldots w_n^*$. Suppose for all $a \in X$, a appears in some w_k, $1 \leq k \leq n$. Then for every i, j, $1 \leq i \leq j \leq n$, let a_{ij} be a letter such that the number of consecutive occurings of a_{ij} in $w_i w_j$ is maximal. Let $H = \{a_{ij}^{n_{ij}} \mid 1 \leq i \leq j \leq n\}$, $\alpha = \max\{n_{ij} \mid 1 \leq i \leq j \leq n\}$ and a be a letter such that $a^\alpha \in H$. Since $|X| \geq 2$ and $U \subseteq w_1^* w_2^* \ldots w_n^*$, by the choice of a and α, $xa^{\alpha+1}y \notin U$ for all $x, y \in X^*$. Thus $U..a^{\alpha+1} = \emptyset$. This completes the proof. #

REFERENCES

1. Birkhoff, G., "Lattice Theory", New ed., Colloquium Publication 25, Amer. Math. Soc., Providence, 1967.

2. Clifford, A. H. and G. B. Preston, "The Algebraic Theory of Semigroups", Vol. 1 and Vol. 2, Mathematical Surveys 7, Amer. Math. Soc., Providence, 1964 and 1967.

3. Gécseg, F. and I. Peák, "Algebraic Theory of Automata", Disquisitiones Mathematicae Hungaricae 2, Akadémiai Kiadó, Budapest, 1972.

4. Ginsburg, S. and E. H. Spanier, "Bounded Regular Sets", Proc. Amer. Math. Soc. 17(1966), 1043-1049.

5. Hoehnke, H. J., "Structure of Semigroups", Can. J. Math. 18(1966), 449-491.

6. McNaughton, R. and S. Papert, "The Syntactic Monoid of a Regular Event", in "Algebraic Theory of Machines, Languages and Semigroups", M. A. Arbib ed., Academic Press, New York, 1968, 297-312.

7. Perrot, J. F., "Contribution à l'Etude des Monoides Syntactiques et de Certains Groupes Associés aux Automates Finis", Thèse de Doctorat d'Etat, Fac. Sci. Paris, 1972.

8. Petrich, M., "Introduction to Semigroups", Charles E. Merrill Publishing Co., A Bell & Howell Company, Columbus, 1973.

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

10. Thierrin, G., "Permutation Automata", Math. Sys. Theory 2(1968), 83-90.

11. Thierrin, G., "Automata", Lecture Notes, University of Western Ontario, 1971-72.

12. Thierrin, G., "Irreducible Automata", Proc. Can. Math. Congress, 1971, 245-262.

13. Thierrin, G., "Decomposition of Locally Transitive Semiautomata", Utilitas Math. 2(1972), 25-32.

14. Tully, Jr., E. J., "Representation of a Semigroup by Transformations of a Set", Thesis, Tulane University, 1960.