

# 오토마타와 그들의 입력 반군들에 대한 어떤 성질들

박진홍<sup>†</sup> 이천진<sup>††</sup>

## 요 약

본 논문의 주된 목적은 입력 반군들에 대해서 환에서 얻어진 것들에 비슷한 래디칼 및 원시성과 이행성의 개념들을 발전시킨다. 더구나 우리는 그들의 어떤 성질들을 조사한다.

## Some Properties on Automata and Their Input Semigroups

Chin Hong Park<sup>†</sup> and Chun Jin Lee<sup>††</sup>

### ABSTRACT

The purpose of this paper is to develop for input semigroups the notions of radical and primitiveness similar to those which have been developed for rings and of transitivity. Moreover, some of their properties are investigated.

### 1. Introduction and Preliminaries

We will start with the definition of an automaton.

#### DEFINITION 1.1.

- (1) An automaton,  $A=(M, S, \delta)$ , is a triple where  $M$  is a nonempty set (the set of states),  $S$  is a nonempty semigroup (the set of inputs),  $\delta$  is a function (called the state transition function) mapping  $M \times S$  into  $M$ . Also, we shall assume the useful property that  $\delta(m, st) = \delta(\delta(m, s), t)$  for all  $st, \in S$  and  $m \in M$ .

NOTE. An automaton  $A$  means a triple  $(M, S, \delta)$  and  $M$  does not mean an automaton. But the attribute "automaton" will be sometimes used for  $M$ .

NOTATION. For convenience we will denote  $\delta(m, s)$  as  $ms$ .

- (2) A *subautomaton* of  $M$  is a non-void subset  $H$  of  $M$  such that  $HS \subseteq H$ .
- (3) An automaton,  $A=(M, S, \delta)$ , is called *irreducible* if  $MS \not\subseteq F(M)$  and  $M$  has no non-trivial subautomata where  $F(M) = \{m \in M : ms = m \text{ for all } s \in S\}$ .
- (4) A right congruence of a semigroup  $S$  is called *modular* if there is an element  $e$  of  $S$  such that  $(es, s) \in \alpha$  for all  $s \in S$ . The element  $e$  is called a *left identity* for  $\alpha$ .

#### DEFINITION 1.2

Let  $A=(M, S, \delta_A)$  and  $B=(N, S, \delta_B)$  be automata.

- (1) A mapping  $f:A \rightarrow B$  (or  $M \rightarrow N$ ) is an *S-homomorphism* (or *S-map* or *S-operation preserving*) if  $f(ms) = f(m)s$  for all  $m \in M$  and  $s \in S$ .  $f$  is called an *S-isomorphism* if it is bijective and an *S-homomorphism*.  $f$  is called an *S-homomorphism*.
- (2) An automaton  $A$  is *cyclic* if  $M = mS$  for some  $m \in M$ . Also,  $m$  is called a generator.

<sup>†</sup> 정 회 원: 선문대학교 수학과 부교수

<sup>††</sup> 정 회 원: 선문대학교 전자계산학과 부교수

논문접수: 1994년 3월 17일, 심사완료: 1994년 9월 9일

- (3) An automaton  $A$  is *strongly connected* if every element of  $M$  is a generator.
- (4) An automaton  $A$  is *abelian* if  $m(st)=m(ts)$  for all  $m \in M$  and  $s, t \in S$ .
- (5)  $S$  is *M-abelian* if  $m(ab)=m(ba)$  for all  $m \in M$  and  $a, b \in S$ .
- (6) An automaton  $A$  is *perfect* iff  $A$  is strongly connected and  $S$  is M-abelian.
- (7)  $T_a: M \rightarrow M$  is called a *right translation* if  $T_a(m) = ma$  for all  $m \in M$  where  $a \in S$ .
- (8) We define a congruence  $\mu_M \subset S \times S$  on  $S$  through  $(a, b) \in \mu_M \Leftrightarrow T_a = T_b$ .
- (9)  $M$  is faithful iff  $\mu_M = O_S$  (the identity relation).
- (10) We define a right congruence  $\mu_M$  on  $S$  by  $(a, b) \in \mu_M \Leftrightarrow T_a(m) = T_b(m)$  for  $a, b \in S$  where  $m \in M$ .
- (11) Let  $\alpha$  be a right congruence on  $S$ . For any  $s \in S$  we define a relation  $\alpha s$  on  $S$  by  $(a, b) \in \alpha s$  if and only if  $(sa, sb) \in \alpha$ .

**LEMMA 1.3.**

- (1)  $\mu_{\alpha/a} = \bigcap_{t \in S} at$  if  $\alpha$  is a right congruence on  $S$ . We note that if  $\alpha$  is a modular right congruence on  $S$ ,  $\mu_{\alpha/a} = \bigcap_{a \in S} a\alpha \leq \alpha$ .
- (2)  $[\alpha]_{\bigcap_{M \in S} \mu_M} = \bigcap_{M \in S} [\alpha]_{\mu_M}$  for  $\alpha \in S$ .
- (3) Let  $M$  and  $N$  be two automata. If  $f: M \rightarrow N$  is an S-isomorphism, then  $\mu_M = \mu_N$ .

**Proof.**

For(1), let  $M$  be an automaton and  $m \in M$ . Then for  $a, b \in S$   $(a, b) \in \mu_m \Leftrightarrow ma = mb$  define a right congruence on  $S$ .

$(a, b) \in \mu_{S/a} = \bigcap_{[t]_a \in S/a} \mu_{[t]_a} \Leftrightarrow (a, b) \in \mu_{[t]_a}$  for all  $[t]_a \in S/a \Leftrightarrow [t]_a a = [t]_a$ ,  $b \Leftrightarrow (ta, tb) \in \alpha$  for all  $t \in S \Leftrightarrow (a, b) \in at$  for all  $t \in S \Leftrightarrow (a, b) \in \bigcap_{t \in S} at$ . For(2)  $x \in [\alpha]_{\bigcap_{M \in S} \mu_M} \Leftrightarrow (x, a) \in \bigcap_{M \in S} \mu_M \Leftrightarrow (x, a) \in \mu_M$  for all  $M \in S \Leftrightarrow x \in \bigcap_{M \in S} [\alpha]_{\mu_M}$ . For (3),  $(a, b) \in \mu_M \Leftrightarrow ma$

$= mb$  for all  $m \in M \Leftrightarrow f(ma) = f(mb) \Rightarrow f(m)a = f(m)b$  for all  $m \in M$ .

Now for any  $n \in N$ ,  $n = f(m)$  for some  $m \in M$ . Hence  $na = nb$  implies  $(a, b) \in \mu_N$ . Also it is easy for us to check the converse.

The following proposition is a generalization for a new right congruence induced by right congruences on  $S$  and right ideals of  $S$ . This follows from Oehmke [6].

**PROPOSITION 1.4.**

Let  $A$  be an indexes set. Let  $\tau_\alpha$  be a right congruence on  $S$  and let  $I_\alpha$  be a right ideal of  $S$  for each  $\alpha \in A$ . We define a relation  $\omega = \omega(\bigcap_{\alpha \in A} \tau_\alpha, \bigcap_{\alpha \in A} I_\alpha)$  as follow:

$(a, b) \in \omega \Leftrightarrow (a, b) \in \bigcap_{\alpha \in A} \tau_\alpha$  or  $(a, b) \in \bigcap_{\alpha \in A} I_\alpha$ . Then  $\omega$  is a right congruence on  $S$  with  $\bigcap_{\alpha \in A} I_\alpha \leq \omega$ .

**PROPOSITION 1.5.**

Let  $A$  be an indexes set. Let  $I_\alpha$  be an ideal of  $S$  and  $\omega(I_\alpha)$  be a congruence induced by  $I_\alpha$  for each  $\alpha \in A$ . If  $\bigcap_{\alpha \in A} I_\alpha = \{0\}$ , then  $\bigcap_{\alpha \in A} \omega(I_\alpha) = O_r$  where  $O_r$  means the identity relation.

**Proof.**

For each  $(a, b) \in \bigcap_{\alpha \in A} \omega(I_\alpha)$  it its enough to show that  $a = b$ . Now,  $(a, b) \in \omega(I_\alpha)$  for all  $\alpha \in A$ . This means that  $a = b$  or  $a, b \in I_\alpha$  for all  $\alpha \in A$ . The latter case implies that  $a, b \in \bigcap_{\alpha \in A} I_\alpha = \{0\}$ . Hence  $a = b$ .

**PROPOSITION 1.6.**

Let  $G$  be a non-trivial group and let  $H$  be a proper subgroup of  $G$ . We define the relation  $\alpha$  on  $G$  by

$$(a, b) \in \alpha \Leftrightarrow ab^{-1} \in H.$$

Let  $L(\alpha) = \{\text{all left identities of } \alpha\}$ . Then

- (1)  $H \subset L(\alpha)$ ;
- (2)  $\alpha$  is a modular right congruence on  $G$  with  $\alpha \neq 1_c$  where  $1_c$  means the universal relation;
- (3)  $\tau(L(\alpha)) \subset \alpha$  where  $\tau(L(\alpha)) = \text{Sup}_{\mu \in L(\alpha)} \tau(\mu)$  and  $\tau(\mu) =$  the intersection of all modular right congruences with respect to  $u$ ;

**Proof.**

(1) and (2) are clear. (3) comes from Seidel [4].

**LEMMA 1.7.**

Let  $M$  be an automaton and let  $H$  and  $K$  be subsets of  $M$ . Let  $A$  be a subset of  $S$ . if  $KA = H$ , then  $A \subset K^{-1}H = \{s \in S \mid Ks \subset H\}$

**DEFINITION 1.8.**

- (1) A right congruence  $\tau$  on  $S$  is said to be *modular* with respect to  $a \in S$  if and only if  $(s, as) \in \tau$  for all  $s \in S$ .
- (2) An element  $a \in S$  is a *right q-element* (or a *right quasi-regular element*) if  $\tau(a) = 1_c$  or equivalent to  $a^m s = a^n t$  for some  $m, n \geq 0$  and all  $s, t \in S$  where  $\tau(a) =$  the intersection of all modular right congruences with respect to  $a$ .
- (3) An element  $a \in S$  is an  $O(S)$ -potent if  $a^n \in O(S)$  for some  $n \geq 1$  where  $O(S) = \{\text{all left zero elements in } S\}$ .
- (4) An element  $a \in S$  is an *eigentlich  $O(S)$ -potent* if  $(as)^n \in O(S)$  for some  $n \geq 1$  and for all  $s \in S$ .
- (5) A set  $M$  is called an *automaton with null* ( $0$ ) if  $M$  is an automaton and  $F(M) = \{0\}$  where  $0 \in S$ .

**NOTE :**

with each automaton  $M$  we associate the set  $M_0 = \{s \in S \mid mss_1 = m \text{ implies } m \in F(M) \text{ where } m \in M, s_i \in S^i\}$  where  $S^i = S \cup \{1\}$ .

- (6) We define  $rad_0 S = \bigcap_{M \in \mathcal{IS}} K_M S_M$  or  $rad_0 S = \bigcap_{M \in \mathcal{IS}} M_0$  where  $S_M$  is the representation of  $S$  generated by an automaton  $M$  and  $\mathcal{IS}_0 = \{\text{all irreducible automata with null}(0) \text{ where } 0 \in S\}$ .

**NOTATION.**

- $Q(S) = \{\text{all } q\text{-elements in } S\}$ .
- $E(S) = \{\text{all idempotent elements in } S\}$ .
- $O(S) = \{\text{all left zero elements in } S\}$ .
- $R(S) = \{a \in S \mid (as, s) \in \alpha \text{ for all } s \text{ in } S \text{ implies } \alpha = 1, \text{ where } \alpha \text{ is a right congruence on } S\}$ .
- $O(S)_p = \{\text{all } O(S)\text{-potent elements in } S\}$ .

The following proposition gives us a relationship among these.

**PROPOSITION 1.9.**

- (1)  $Q(S) \cap E(S) \subset O(S) \subset O(S)_p \subset Q(S)$ .
- (2)  $Q(S) \cap E(S) = O(S)$  if  $R(S) = S$ .

**Proof.**

For(1), this is clear from Seidel[4]. For(2), We have  $O(S) = E(S)$  if  $R(S) = S$  and also, we have  $O(S) \subset Q(S)$  from Seidel[4].

**PROPOSITION 1.10.**

Let  $N(S) = \{\text{all eigentlich } O(S)\text{-potent elements in } S\}$ . Then we have

- (1)  $F\left[\frac{S}{N(S)}\right] = \{N(S)\}$  and  $F\left[\frac{S}{M_0}\right] = \{M_0\}$ ;
- (2)  $F\left[\frac{S}{rad_0(S)}\right] = \{rad_0 S\}$ .

**Proof.**

We note that  $F(M/H) = \{H\}$  if  $F(M) \subset H \neq \emptyset$  where  $H$  is a non-void subautomaton of an automation  $M$  and also we know that  $rad_0 S = N$

S). Since  $F(S) = O(S)$ , we have  $F(S) = O(S) \subset \text{rad}_0 S = N(S) \subset M_0$ .

**PROPOSITION 1.11.**

Let  $0 \in S$  and  $S' = S \cup \{1\}$ .

Let  $\mathcal{Q} = \{\text{all right ideals } I_\alpha \text{ in } S, \alpha \in A\}$ . Let  $\Pi = \{\text{all right congruences on } S\}$ . We define the relation  $\omega_{I_\alpha}(\sigma_\alpha)$  on S by  $(a, b) \in \omega_{I_\alpha}(\sigma_\alpha) \Leftrightarrow (as_1, bs_1) \in \sigma_\alpha$  for all  $s_1 \in S'$  where  $\sigma_\alpha = I_\alpha \times I_\alpha \cup (S - I_\alpha) \times (S - I_\alpha)$ . then

- (1) there exists a function  $F: \mathcal{Q} \rightarrow \Pi$  given by  $F(I_\alpha) = \omega_{I_\alpha}(\sigma_\alpha)$ ;
- (2)  $F$  is 1-1.

**Proof.**

For(1), from proposition 15 of Seidel [4] there exists a unique maximal right congruence  $\omega_{I_\alpha}(\sigma_\alpha)$  for each right ideal  $I_\alpha$  in  $S$ . Hence it holds. For(2), To prove that  $F$  is 1-1, it is enough to show that  $F(I_\alpha) = F(I_\beta)$  implies  $I_\alpha = I_\beta$ . Also, we note that by proposition 15 if Seidel[4] we have  $\omega_{I_\alpha}(\sigma_\alpha) = \text{Sup}_\Pi \{ \gamma \in \Pi \mid I_\alpha = [0]_\gamma \}$ .

Since  $\omega_{I_\alpha}(\sigma_\alpha) = \omega_{I_\beta}(\sigma_\beta)$  and these are in  $\Pi$ , we have  $\omega_{I_\alpha}(\sigma_\alpha) = \gamma_0$  with  $I_\alpha = [0]_{\gamma_0}$  for some  $\gamma_0$  in  $\Pi$  and  $\omega_{I_\beta}(\sigma_\beta) = \gamma_1$  with  $I_\beta = [0]_{\gamma_1}$  for some  $\gamma_1$  in  $\Pi$ . Hence  $I_\alpha = I_\beta$ .

**COROLLARY 1.11.1.**

$|\mathcal{Q}| \leq |\Pi|$  where  $|\cdot|$  means the cardinality.

**PROPOSITION 1.12.**

Let  $0 \in S$  and let  $\alpha$  be a right congruence on  $S$ . Let  $\beta([O]_\alpha)$  on S and let  $\omega_{[O]_\alpha}(\sigma_\alpha)$  be the right congruence induced by  $[O]_\alpha$  on S and let  $\omega_{[0]_\alpha}(\sigma_\alpha)$  be the unique maximal right congruence induced by  $\sigma_\alpha$  with respect to  $[O]_\alpha$ . Then we have

$$\beta([O]_\alpha) \subset \alpha \subset \omega_{[0]_\alpha}(\sigma_\alpha).$$

**Proof.**

For the first part it is clear since  $(x, y)$  belongs to  $\beta([O]_\alpha)$  if and only if  $x=y$  or  $x, y \in [O]_\alpha$ .

For the second part we note that  $(a, b) \in \omega_{[0]_\alpha}(\sigma_\alpha) \Leftrightarrow (as_1, bs_1) \in \sigma_\alpha$  for all  $s_1$  in  $S'$ . So it enough to show that for each  $(x, y) \in \alpha$  for all  $s_1$  in  $S'$ .

(i) suppose  $(x, 0) \in \alpha$ . Then  $(x, y) \in \sigma_\alpha$ . For  $(y, 0) \in \alpha$  implies  $x, y \in [O]_\alpha$ . Since  $\alpha$  is a right congruence on  $S$ , we have  $(xs, 0) \in \alpha$  for all  $s$  in  $S$ . This implies that  $(xs, ys) \in \sigma_\alpha$  for all  $s$  in  $S$ . For  $(ys, 0) \in \alpha$  implies  $xs, ys \in [O]_\alpha$ . Hence  $(x, y) \in \alpha$  and  $(xs, ys) \in \alpha$  for all  $s$  in  $S$ .

i.e., we have  $(xs_1, ys_1) \in \sigma_\alpha$  for all  $s_1$  in  $S'$ .

(ii) suppose  $(x, 0) \notin \alpha$ . Then  $(x, y) \notin \sigma_\alpha$ . For  $(y, 0) \notin \alpha$  implies  $x, y \in [O]_\alpha$  and  $x, y \in S - [O]_\alpha$ . Hence we have  $(x, y) \in (S - [O]_\alpha) \times (S - [O]_\alpha) \subset \sigma_\alpha$ .

Next, if  $(xs, 0) \in \alpha$  for all  $s$  in  $S$ ,  $(xs, ys) \in \sigma_\alpha$  from (i). So, we have done. Now, suppose  $(xs, 0) \notin \alpha$  for all  $s$  in  $S$ . Then  $(xs, ys) \in \sigma_\alpha$ . For  $(ys, 0) \notin \alpha$  implies  $xs, ys \notin [O]_\alpha$  and  $xs, ys \in S - [O]_\alpha$ . Hence  $(x, y)$  and  $(xs, ys)$  are contained in  $\sigma_\alpha$  for all  $s$  in  $S$ . This means that  $(xs_1, ys_1) \in \sigma_\alpha$  for all  $s_1$  in  $S'$ .

**2. Radical and Maximality**

**DEFINITION 2.1.**

- (1) An automaton  $M$  is called *totally irreducible* if  $MS \not\subseteq F(M)$  and  $M$  has no non-trivial homomorphism.
- (2) An automaton  $M$  is called *strictly cyclic* if  $M = m_0 S$  for some  $m_0 \in M$ .

**LEMMA 2.2.**

Let  $\alpha$  and  $\beta$  be modular right congruences on  $S$ . if  $S/\alpha$  and  $S/\beta$  are isomorphic and  $\alpha$  is

maximal, then  $\beta$  is maximal.

**Proof.**

We note that  $S/\alpha$  has a non-trivial homomorphism if and only if there exists a right congruence  $\omega$  on  $S$  such that  $\alpha < \omega < 1$ . Suppose that  $\beta$  is not maximal. Then there exists a modular right congruence  $\mu$  on  $S$  with  $\beta < \mu < 1$ . This means that  $S/\beta$  has a non-trivial homomorphism and also this means that  $S/\alpha$  has a non-trivial homomorphism. Therefore there exists a right congruence  $\omega_1$  on  $S$  with  $\alpha < \omega_1 < 1$ . Also,  $\omega_1$  is a modular since  $\alpha$  is a modular. It is impossible since  $\alpha$  is maximal.

**PROPOSITION 2.3.**

Let  $M$  be an automaton with  $|M| \geq 2$  and no homomorphism except for isomorphism.

Suppose  $O(S) \neq \phi$ . Then  $M$  is a totally irreducible if and only if  $M$  is strictly cyclic.

**Proof.**

( $\Rightarrow$ ) It is clear. ( $\Leftarrow$ ) Suppose  $M$  is strictly cyclic. Then  $M$  and  $S/\alpha$  are isomorphic where  $\alpha$  is a modular right congruence on  $S$ . Now, from Hoehnke[5] there exists a maximal modular right congruence  $\beta$  with  $\alpha < \beta$ . Also, from  $\alpha < \beta$  there is an onto-homomorphism from  $S/\alpha$  to  $S/\beta$ . But by the assumption  $S/\alpha$  and  $S/\beta$  are isomorphic. Hence  $\alpha$  is maximal from Lemma 2.2. This means that  $M$  is totally irreducible.

**NOTATION.**  $I$ , means the identical relation and  $1$ , means the universal relation.  $TA = \{\text{all totally irreducible automata}\}$ .

**DEFINITION 2.4.**

(1) We define  $rad S = \bigcap_{M \in IS} \mu_M$ .

(2)  $S$  is called *radical-free* if  $rad S = Ir$ .

The following statement is a similar one of a solvable group  $G$ . Let  $N$  be a normal subgroup of  $G$ . We note that  $F$  is solvable if and only if  $N$  and  $G/N$  are solvable.

**PROPOSITION 2.5.**

Let  $I$  be an ideal of  $S$  with  $I \subset Ker S_M$ . Then  $S$  is radical-free if and only if  $I$  and  $S/N$  are radical-free.

**Proof.**

( $\Rightarrow$ ) We note that  $rad I = I \times I \cap rad S$  from Seidel[4]. Since  $rad S = Ir$ , we have  $rad I = Ir$

Also, from Seidel[4] we note that for every ideal  $I \subset Ker S_M$   $M$  is an  $S$ -automaton if and only if  $M$  is an  $S/I$  automaton. Let  $ISI$  be the set of all irreducible  $S/I$ -automata. Then we have  $rad S/I = \bigcap_{M \in ISI} \mu_M(S/I) = \bigcap_{M \in IS} \mu_M(S) = rad S = Ir$ .

( $\Leftarrow$ ) It is clear from Seidel[4].

**DEFINITION 2.6.**

- (1) We define  $Rad S = \bigcap_{M \in TA} \mu_M$ .
- (2)  $S$  is  $O$ -radical free if  $rad_o S = \{0\}$ .

**PROPOSITION 2.7.**

- (1)  $rad_o S \times rad_o S \subset rad S \subset Rad S$ ;
- (2) Let  $O \in S$ . If  $S$  is radical-free, then  $S$  is  $O$ -radical free.

**Proof.**

For(1), since  $rad_o S$  is a congruence ideal with respect to  $rad S$   $rad_o S = [a_o]_{rad S}$  for some  $a_o \in rad_o S$ . Now, for each  $(x, y) \in rad_o S \times rad_o S$  we have  $x, y \in rad_o S$ . So,  $(x, a_o) \in rad S$  and  $(y, a_o) \in rad S$ .

Hence we have  $(x, y) \in rad S$ . For the second part it comes from Hoehnke [5]. For (2) we note that we can replace the condition  $O \in S$  by

$rad_0 S \neq \phi$  since  $rad S = Ir$  and  $rad_0 S \neq \phi$  implies that there exist a null element 0 in  $S$  from Seidel [4]. Hence it is clear.

We note that any finitely generated semigroup  $S$  contains at least one maximal subsemigroup.

The following proposition is easy to check it using Zorn's Lemma.

**PROPOSITION 2.8.**

Let  $A$  be a non-empty subset of  $S$ . Suppose there exist an ideal  $I$  of  $S$  such that  $I \cap A = \phi$ .

Let  $W = \{J \mid J \text{ is ideal of } S \text{ with } J \cap A = \phi\}$ . Then there exists a maximal subautomaton  $K$  containing  $H$ .

**PROPOSITION 2.9.**

Let  $M$  be an automaton with  $MS = M$ . If  $H$  is a subautomaton of  $M$  with  $H \neq M$ , there exists a maximal subautomaton  $K$  containing  $H$ .

**Proof.**

Let  $W = \{L \mid L \text{ is a proper subautomaton of } M \text{ with } H \subset L \subset M\}$  and partially order  $W$  by set inclusion (i.e.,  $L_1 \leq L_2$  if and only if  $L_1 \subset L_2$ ). We claim that  $W$  is a non-empty inductively ordered set. To prove this, (1)  $W \neq \phi$ : It is clear since  $H \in W$ . (2)  $W$  is inductively ordered: Let  $T$  be any non-empty totally ordered subset of  $W$ . To show that  $T$  has an upper bound in  $W$ , let  $U = \cup_{L \in T} L$ . Then (a)  $U$  is a subautomaton of  $M$  (i.e.,  $US \subset U$ ). To show this, choose any  $x \in US$ . Then  $x = ys$  for some  $y \in U$  and  $s \in S$ .  $y \in U$  implies  $y \in L$  for some  $L \in T$ . Hence  $x = ys \in LS \subset L \subset U$ . (b)  $H \subset U \subset M (U \neq M)$  (i.e.,  $U \subset W$ ). Now,  $H \subset U$  is clear. To show that  $U \neq M$ , suppose  $U = M$ . Then  $US = MS = M$ . For each  $m \in M$ ,  $m \in US$ . This implies  $m \in LS$  for some  $L \in T$ . So,  $m \in LS \subset L$ . Hence  $M \subset L$  and  $M = L$ . It is impossible. (c)  $U$  has an upper

bound for  $T$  (it is clear). Hence By Zorn's lemma  $W$  has a maximal element  $K$  in  $W$ .

**COROLLARY 2.9.1.**

Let  $M$  be a strictly cyclic automaton. If  $H$  is a subautomaton of  $M$  with  $H \neq M$ , then there exists a maximal subautomaton  $K$  containing  $H$ .

**COROLLARY 2.9.2.**

Let  $M$  be an automaton with  $F(M) = M$ . If  $H$  is a subautomaton of  $M$  with  $H \neq M$ , then there exists a maximal subautomaton  $K$  containing  $H$ .

**Proof.**

$F(M) = M$  implies  $MS = M$ .

**COROLLARY 2.9.3.**

Let  $M$  be an irreducible (or totally irreducible) automaton. If  $H$  is a subautomaton of  $M$  with  $H \neq M$ , then there exists a maximal subautomaton  $K$  containing  $H$ .

**Proof.**

The fact that  $M$  is totally irreducible implies that  $M$  is irreducible and also this implies  $MS = M$ .

**PROPOSITION 2.10.**

Let  $0 \in S$  and let  $\alpha$  be a maximal right congruence on  $S$ . Then  $S/[0]_\alpha$  is an irreducible  $S$ -automaton  $\Leftrightarrow S \neq \text{Ker } S_{s/\alpha}$ .

**Proof.**

Let  $I$  be a maximal right ideal of  $S$ . Then from Hoehnke[5]  $S/I$  is an irreducible  $S$ -automaton if and only if  $S \neq S^{-1}I$ . ( $\Rightarrow$ ):  $[0]_\alpha$  is a maximal right ideal since  $\alpha$  is a maximal right congruence on  $S$ . This implies that  $S \neq S^{-1}[0]_\alpha = (S/\alpha)^{-1}\{[0]_\alpha\} = \text{Ker } S_{s/\alpha}$ .

( $\Leftarrow$ ): It is clear since  $S \neq S^{-1}[0]_\alpha$  and  $[0]_\alpha$  is a maximal right ideal of  $S$ .

**DEFINITION 2.11.**

Let  $M$  be an  $S$ -automaton.  $M$  is cyclic if  $M = mSU\{m\}$  for some  $m$  in  $M$ .

**NOTATION.**  $M^* = \{\text{all non-generators in } M\}$  where  $M$  is cyclic.

**PROPOSITION 2.12.**

Let  $\alpha$  be a right congruence on  $S$ . Let  $S/\alpha$  be an  $S$ -automaton with  $F(S/\alpha) = \phi$ . Then  $S/\alpha$  is an irreducible  $S$ -automaton if and only if  $\alpha$  is a modular right congruence.

**Proof.**

$S/\alpha$  is a strictly cyclic  $S$ -automaton since  $S/\alpha$  is irreducible. This means that  $\alpha$  is modular.

Conversely, we assume that  $\alpha$  is a modular right congruence on  $S$ . Then  $S/\alpha$  is strictly cyclic. This means that  $(S/\alpha)^* = \phi$  since  $F(S/\alpha) = \phi$ . Hence it holds.

**3. Faithfulness, Primitiveness and transitiveness.**

**DEFINITION 3.1.**

Let  $0 \in S$  and let  $M$  be an  $S$ -automaton.

- (1)  $M$  is faithful if  $\mu_M = I_r$  where  $0 \notin S$ .
- (2)  $M$  is  $0$ -faithful if  $Ker S_M = M^{-1}[0] = \{0\}$ .
- (3)  $S$  is  $0$ -primitive if  $S$  has an  $0$ -faithful irreducible  $S$ -automaton.
- (4) Let  $P$  be an ideal of  $S$ .  $P$  is  $0$ -primitive if  $S/P$  is  $0$ -primitive semigroup and  $S \neq P$ .

**PROPOSITION 3.2.**

Let  $0 \in S$ . If  $\alpha$  is a maximal modular right congruence, then  $Ker S_{S/\alpha}$  is an  $0$ -primitive ideal of  $S$ .

**Proof.**

By the assumption  $[0]_\alpha$  is a maximal modular right ideal of  $S$ . This means that  $S^{-1}[0]_\alpha$  is an  $0$ -primitive ideal by Hoehnke[3]. Hence we have  $S^{-1}[0]_\alpha = (S/\alpha)^{-1}\{[0]_\alpha\} = Ker S_{S/\alpha}$ .

**DEFINITION 3.3.**

Let  $M$  be an  $S$ -automaton.

- (1)  $M$  is 2-minimal if  $|M| \geq 2$  and  $M$  has the only trivial  $S$ -autotmaton.
- (2)  $M$  is 2-null if  $|M| = 2$  and  $|MS| = 1$ .
- (3)  $M$  is 0-transitive if  $M$  is strictly cyclic with  $|M| \geq 2$  and  $|F(M)| = 1$ .

**LEMMA 3.4.**

Let  $M$  be an  $S$ -automaton. If  $M$  is 2-minimal reducible, then  $M$  is either 2-null or  $|M| = |MS| = |F(M)| = 2$ .

**PROPOSITION 3.5.**

Let  $M$  be an 2-minimal  $S$ -automaton with  $|F(M)| = 1$ . Then

- (1) If  $MS \not\subseteq F(M)$ , then  $M$  is  $0$ -transitive.
- (2) If  $M$  is reducible, then  $M$  is 2-null.

**Proof.**

- (1)  $MS \not\subseteq F(M)$  means that  $M$  is irreducible. This means that  $M$  is strictly cyclic. Hence it holds.
- (2) It is clear from lemma 3.4 and  $|F(M)| = 1$ .

**COROLLARY 3.5.1.**

Let  $M$  be an 2-minimal  $S$ -automaton with  $|F(M)| = 1$ . If  $MS \not\subseteq F(M)$  or  $M$  is reducible, then  $M$ ,  $F(M)$  and  $\phi$  are the only invariant subsets of  $M$ .

**Proof.**

It comes from Tully[1] and proposition 3.5.

**DEFINITION 3.6.**

- (1)  $S$  is transitive if  $S$  is strictly cyclic with  $O(S) = \phi$ .
- (2)  $S$  is 0-transitive if  $S$  is strictly cyclic with  $|S| \geq 2$  and  $O(S) = \phi$ .
- (3)  $S$  is h-primitive if  $S$  has a faithful irreducible  $S$ -automaton  $M$ .
- (4)  $S$  is t-primitive if  $I_r$  and  $1_r$  are the only right congruence on  $S$ .

We have the following lemma a from Tully[1].

**LEMMA 3.7.**

- (1) If  $S$  is 0-transitive, then  $|O(S)| = 1$  and  $S$ ,  $O(S)$  and  $\phi$  are the only invariant subsets of  $S$ .
- (2) If  $S$  is t-primitive with  $|S| \geq 3$ , then  $S$  is either 0-transitive or transitive.

**PROPOSITION 3.8.**

If  $S$  is t-primitive with  $|S| \geq 3$  and  $E(S) \not\subseteq O(S)$ , then  $S$  is an h-primitive.

**Proof.**

By lemma 3.7,  $S$  is either 0-transitive or transitive. To prove that  $S$  is a faithful irreducible  $S$ -automaton, (1) assume that  $S$  is 0-transitive. Then  $\mu_s = I_r$  from the fact that for each  $a$  in  $S$ ,  $\mu_a$  is a right congruence on  $S$  and  $\mu_a = I_r$  or  $1_r$ . We will show that  $S$  is irreducible. (i)  $SS \not\subseteq F(S) = O(S)$  since  $|O(S)| = 1$  by lemma 3.7. (ii)  $S$  has the only trivial  $S$ -automaton since  $S$ ,  $O(S)$  and  $\phi$  are the only invariant subsets of  $S$  by lemma 3.7. (2) assume that  $S$  is transitive.

Then  $\mu_s = I_r$  from the case (1). To show that  $S$  is irreducible, we know that if  $S$  is transitive,

then  $S$  is strictly cyclic with  $F(S) = O(S) = \phi$ . This implies that  $S$  is irreducible since  $S^* = \phi$  from Hoehnke[5].

**DEFINITION 3.9.**

Let  $M$  be an  $S$ -automaton.  $M$  is strongly connected(or transitive) if  $M$  is strictly cyclic with  $F(M) = \phi$ (i.e., every element of  $M$  is a strict generator).

We have the following proposition by combining proposition 2.1 of Tully[1] with theorem 3 of Oehmke[2].

**PROPOSITION 3.10.**

Let  $M$  be a strictly cyclic  $S$ -automaton. Then the following statements are equivalent:

- (1)  $M$  is strongly connected(or transitive);
- (2)  $S/\mu_m$  is strongly connected for every  $m$  in  $M$ ;
- (3) For every  $a, b \in S$ ,  $(ac, b) \in \mu_m$  for some  $c$  in  $S$  and each  $m$  in  $M$ ;
- (4) any  $\mu_m$ -class  $\cap$  any right ideal of  $S \neq \phi$  for every  $m$  in  $M$ .

**Proof.**

(1) $\Rightarrow$ (2):By the definition we have  $M = mS$  for every  $m$  in  $M$ . Also, we have that  $mS$  and  $S/\mu_m$  are isomorphic from theorem 3 of Oehmke[2]. Hence it holds. (1) $\Leftarrow$ (2): $S/\mu_{m_0} \sim m_0S = M$  for some  $m_0 \in M$ . The proofs that (2), (3) and (4) are equivalent come from Tully[1].

**PROPOSITION 3.11.**

Let  $O \in S$ .

- (1) If  $S$  is 0-primitive, then  $S$  is 0-radical free.
- (2) If  $S$  is h-primitive, then  $S$  is radical free.
- (3) If  $S$  is 0-primitive or h-primitive, then  $S$  is 0-radical free.



**Proof.**

(1) and (2) come from the definitions. (3) is clear from proposition 2.7.

**References**

- [1] E. J. Tully, Representations of a semigroup by transformations acting transitively on a set, Amer. J. Math. 83(1961), pp. 533-541.
- [2] R. H. Oehmke, On the structure of an automaton and its input semigroup, J. ACM10 (1963), pp. 521-525.
- [3] H.J.Hoehnke, Zur Strukturtheorie der Halbgruppe, diese Nachr. 26, pp. 1-13(1963/64).
- [4] H.Seidel, Über das Radical einer Halbgruppe, MATH. Nachr., 29(1965), pp. 255-263.
- [5] H.J.Hoehnke, Structure of Semigroups, Canad. J. Math. 18(1966), pp. 449-491.
- [6] R. H. Oehmke, On maximal congruenced and finite semisimple semigroups, Trans. AMS 125(1966), pp. 223-237.
- [7] Chin-Hong Park, Algebraic properties associated with the input simigroup S of an automaton, Bull.Korean Math. Soc. 27(1990), pp. 69-83.

**박진홍**



서울대학교 사범대학 수학과졸 (이학사)  
 서울대학교 대학원 수학과졸 (이학석사)  
 University of Michigan(Ann Arbor, 미국), 공학석사(Computer)  
 University of Illinois(Urbana, 미국), Computer 박사과정수료

University of Iowa(미국), 수학박사(Ph. D. in Mathematics)  
 서울대, 고려대, 한양대 강사  
 충북대학교 수학과 전임강사  
 Blackburn University(미국), 조교수(tenure track)  
 Fayetteville State University(미국), 조교수(tenure track)  
 현, 선문대학교(구, 성화대), 수학과 부교수  
 한국정보처리응용학회, 전산수학 연구회 위원장

**이천진**



서울대학교 사범대학 수학과 (이학사)  
 Univ. Of Arkansas, Applied Statistics(이학석사)  
 Univ. of Texas, Environmental Statistics and Computer Science(이학박사)  
 McMurry University(Abilene, Texas, U.S.A)

Dept. of Computer Science(Chairman)  
 전산수학연구회 교문  
 현, 선문대학교 전자계산학과 부교수