CHAPTER II

PRELIMINARIES

Let S be a semigroup. If S contains an element 1 with the property that for all x in S,

$$x1 = 1x = x,$$

then S is called a *monoid* and 1 is said to be the *identity element* of S.

An element e of S is an *idempotent* of S if $e^2 = e$. The set of all idempotents of S is denoted by $E(S)$.

A nonempty subset T of S is called a *subsemigroup* of S if it is closed with respect to the operation on S.

Let X be a set. A partial transformation of X is a map of a subset of X into X. The empty partial transformation is the map with empty domain.

The set $\mathcal{P}(X)$ consisting of all partial transformations of X is a semigroup under composition acting on the right. Note that, for any $\alpha, \beta \in \mathcal{P}(X)$,

$$\mathrm{Dom}(\alpha\beta) = [\mathrm{Im}\alpha \cap \mathrm{Dom}\beta]\alpha^{-1},$$

$$\mathrm{Im}(\alpha\beta) = [\mathrm{Im}\alpha \cap \mathrm{Dom}\beta]\beta,$$

and

$$\chi(\alpha\beta) = (\chi\alpha)\beta \quad \text{for all } \ \chi \in \mathrm{Dom}(\alpha\beta).$$

The set $\mathcal{I}(X)$ consisting of all $1-1$ partial transformations of X is a subsemigroup of $\mathcal{P}(X)$. It can be shown that

$$E(\mathcal{I}(X)) = \{ \ 1_Y \mid Y \subseteq X\}$$

where 1_Y denotes the identity map on Y.

An idea of great importance in semigroup theory is that of an *inverse* of an element. If a is an element of a semigroup , then we say that a' is an *inverse* of a if

$$aa'a = a \quad \text{and} \quad a'aa' = a'.$$

In general, an element a may have more than one inverse. For example, let $X = \{\ 1, 2, 3\ \}$. Considering

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 3 & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \quad \text{and} \quad \gamma = \begin{pmatrix} 3 \\ 3 \end{pmatrix}$$

which are elements in $\mathcal{P}(X)$, we have

$$\alpha\beta\alpha = \alpha, \quad \beta\alpha\beta = \beta, \quad \alpha\gamma\alpha = \alpha \quad \text{and} \quad \gamma\alpha\gamma = \gamma.$$

This implies that β and γ are inverses of α.

For a semigroup S, if each element a of S has a unique inverse, then we say that S is an *inverse semigroup.* The unique inverse of a is denoted by a^{-1}. Note here that, if a has an inverse, then $aa^{-1}, a^{-1}a \in E(S)$.

A typical example of an inverse semigroup is $\mathcal{I}(X)$, the semigroup of all $1-1$ partial transformations of X mentioned before.

Let S and T be semigroups. A map $\phi : S \to T$ is said to be a *homomorphism* if $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in S$. An *isomorphism* from S to T is a homomorphism which is both surjective and injective.

A *homomorphism* ϕ from a monoid M to a monoid M' is a semigroup homomorphism ϕ from M to M' such that $\phi(1) = 1'$.

A *congruence* ρ on a semigroup S is an equivalence on S which is both left and right compatible; that is, for every $x, y, z \in S$, $x \ \rho \ y$ implies $zx \ \rho \ zy$ and $xz \ \rho \ yz$.

Let ρ be a congruence on a semigroup S. Then the set $S/\rho = \{\ x\rho \mid x \in S\ \}$ is a semigroup under the operation defined by $(x\rho)(y\rho) = (xy)\rho$ for every $x, y \in S$ and it is called a *quotient* of S by ρ. Moreover, if S is a monoid, then so is S/ρ.

Let S and T be semigroups and $\phi : S \to T$ a homomorphism. Then the relation on S defined by $\rho = \phi \circ \phi^{-1}$; that is,

$$x\rho y \Leftrightarrow x\phi = y\phi \quad \text{for all} \ \ x, y \in S$$

is a congruence on S and $S/\rho \cong \text{Im } \phi$ by $x\rho \mapsto x\phi$.
The relation ρ defined above is called the *kernel* of ϕ and it may be written by $Ker\phi$.

J.A. Green introduced five equivalences which have played a fundamental role in the development of semigroup theory.

In an arbitrary semigroup S and let $a, b \in S$,

$$a\mathcal{L}b \Leftrightarrow S^1a = S^1b,$$

$$a\mathcal{R}b \Leftrightarrow aS^1 = bS^1,$$

$$\text{and} \quad a\mathcal{J}b \Leftrightarrow S^1aS^1 = S^1bS^1$$

where S^1 is the semigroup S with an identity adjoined if necessary. It follows immediately that

$$\mathcal{L} \subseteq \mathcal{J} \quad \text{and} \quad \mathcal{R} \subseteq \mathcal{J}.$$

We define $\mathcal{H}$ as the intersection of $\mathcal{L}$ and $\mathcal{R}$, and $\mathcal{D}$ as the join of $\mathcal{L}$ and $\mathcal{R}$; that is, the smallest equivalence containing both $\mathcal{L}$ and $\mathcal{R}$. Hence $\mathcal{D} \subseteq \mathcal{J}$. For $a \in S$, we denote the equivalence classes of a with respect to $\mathcal{L}, \mathcal{R}, \mathcal{J}, \mathcal{H}$ and $\mathcal{D}$ by L_a, R_a, J_a, H_a and D_a, respectively.

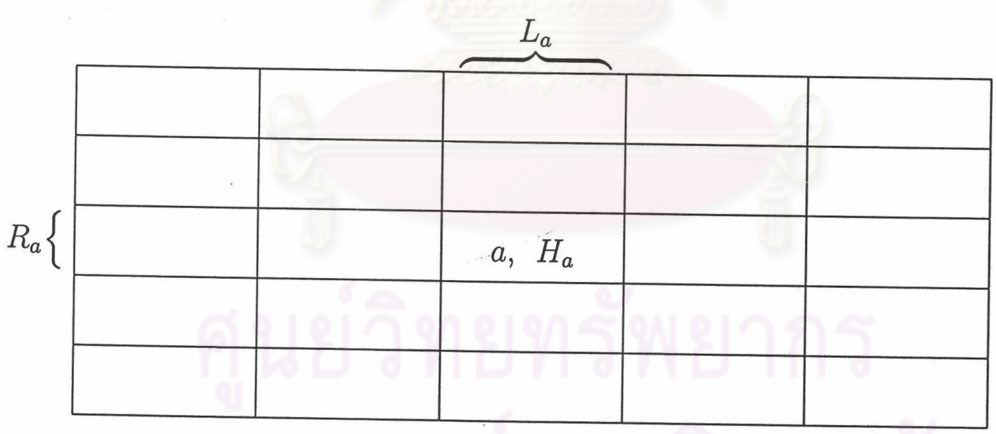
There is a natural partial ordering on the sets of classes of the relations $\mathcal{L}, \mathcal{R}, \mathcal{J}$

and $\mathcal{H}$. For example, $R_a \leq R_b$ if and only if $aS^1 \subseteq bS^1$, defines a partial ordering on the set of $\mathcal{R}$ - classes. For the global description of S, the partial ordering on the set of $\mathcal{J}$ - classes defined by $J_a \leq J_b$ if and only if $S^1aS^1 \subseteq S^1bS^1$ is the most important. We call the partially ordered set of $\mathcal{J}$ - classes of S the *frame* of S. It is well-known that in a finite semigroup, $\mathcal{D} = \mathcal{J}$. Thus finite semigroups can be described in terms of their frame and of the local structure of the various $\mathcal{D}$ - classes.

However, by the definition of $\mathcal{D}$,

$$a\mathcal{D}b \quad \Leftrightarrow \quad R_a \cap L_b \neq \varnothing \quad \Leftrightarrow \quad L_a \cap R_b \neq \varnothing.$$

Consequently, a $\mathcal{D}$-class D of S can be represented by the following egg-box diagram, in which each row represents an $\mathcal{R}$ - class, each column represents an $\mathcal{L}$ - class, and each cell represents an $\mathcal{H}$ - class.



In this research, we focus on $\mathcal{D}$ - classes of a finite subsemigroup of $\mathcal{I}(X)$. For this purpose, we characterize $\mathcal{L}$ and $\mathcal{R}$ equivalences on such a semigroup in term of domains and images of elements.

Theorem 2.1. *Let T be a finite inverse subsemigroup of $\mathcal{I}(X)$ and $\alpha, \beta \in T$. Then*

(i) $\alpha \mathcal{L} \beta$ *if and only if* $Im\ \alpha = Im\ \beta$

(ii) *$\alpha\mathcal{R}\beta$ if and only if Dom $\alpha =$ Dom β.*

Proof. Before proving the theorem, we will show that

$$\beta^{-1}\beta = 1_{\mathrm{Im}\beta} \quad \text{and} \quad \beta\beta^{-1} = 1_{\mathrm{Dom}\beta}.$$

Since $\beta^{-1}\beta$ and $\beta\beta^{-1}$ are idempotents, they are identity maps on their domains (which are the same as images).

Thus it remains to show that

$$\mathrm{Im}\ \beta^{-1}\beta = \mathrm{Im}\ \beta \quad \text{and} \quad \mathrm{Dom}\ \beta\beta^{-1} = \mathrm{Dom}\ \beta.$$

Since $\beta\beta^{-1}\beta = \beta$, Im $\beta \subseteq$ Dom $\beta^{-1}\beta$ and Im $\beta^{-1}\beta \subseteq$ Im β. Hence

$$|\ \mathrm{Im}\ \beta| \leq |\ \mathrm{Dom}\ \beta^{-1}\beta| = |\ \mathrm{Im}\ \beta^{-1}\beta| \leq |\ \mathrm{Im}\ \beta|.$$

Thus $|$ Im $\beta^{-1}\beta| = |$ Im $\beta|$. Since Im $\beta^{-1}\beta \subseteq$ Im β and $|$Im $\beta^{-1}\beta| = |$ Im $\beta|$, we have Im $\beta^{-1}\beta=$ Im β. It follows from $(\beta\beta^{-1})\beta = \beta$ that Dom $\beta\beta^{-1}=$ Dom β.

(i) : It suffices to show that Im $\alpha \subseteq$ Im β if and only if there is $\gamma \in T$ such that $\alpha = \gamma\beta$.

Assume that Im $\alpha \subseteq$ Im β.

Set $\gamma = \alpha\beta^{-1}$. Then $\gamma \in T$ and

$$\gamma\beta = (\alpha\beta^{-1})\beta = \alpha(\beta^{-1}\beta) = \alpha 1_{\mathrm{Im}\ \beta} = \alpha.$$

Conversely, assume that there exists $\gamma \in T$ such that $\gamma\beta = \alpha$. Then

$$\mathrm{Im}\ \alpha = \mathrm{Im}\ \gamma\beta \subseteq \mathrm{Im}\ \beta.$$

(ii) : It suffices to show that Dom $\alpha \subseteq$ Dom β if and only if there is $\gamma \in T$ such that $\alpha = \beta\gamma$.

Assume that Dom $\alpha \subseteq$ Dom β.

Set $\gamma = \beta^{-1}\alpha$. Then $\gamma \in T$ and

$$\beta\gamma = \beta(\beta^{-1})\alpha = (\beta\beta^{-1})\alpha = 1_{\mathrm{Dom}\ \beta}\alpha = \alpha.$$

Conversely, assume that there exists $\gamma \in T$ such that $\beta\gamma = \alpha$. Then

$$\text{Dom } \alpha = \text{Dom } \beta\gamma \subseteq \text{Dom } \beta.$$

$\square$

As a consequence of Theorem 2.1, if we denote the common cardinality of Dom α and Im α for any α in $\mathcal{I}(X)$ by rank α, then the next corollary follows immediately.

Corollary 2.2. *Let T be a finite inverse subsemigroup of $\mathcal{I}(X)$ and $\alpha, \beta \in T$. If $\alpha\mathcal{D}\beta$, then rank $\alpha =$ rank β.*

An *alphabet* A is a nonempty set whose elements are called *letters.* For each n, let A^n be the set of all sequences, called *words*, of length n; that is

$$A^n = \{a_1a_2...a_n \mid a_1, a_2, ..., a_n \in A\}.$$

Let $A^+ = \bigcup_{n=1}^{\infty} A^n$ and $A^* = A^+ \bigcup \{\varepsilon\}$ where ε denotes the empty sequence. Define an operation (concatenation) on A^* by

$$(a_1a_2...a_n)(b_1b_2...b_m) = a_1a_2...a_nb_1b_2...b_m.$$

Then A^* becomes a monoid (with identity ε), called the *free monoid* on the set A. A non-empty subset of A^* is called a *language* of A^*. Let $u, v \in A^+$. Then u is called a *left* (resp.*right*) *factor* of the word w in A^+ if $w = uv$ (resp. $w = vu$).

Let M be a moniod with identity 1. An M- *automaton* $\mathfrak{A}$ is a pair (S, f), where S is a non-empty set whose elements are called *states* and $f : S \times M \longrightarrow S$ is a mapping satisfying:

(a) $f(s, 1) = s$ for every $s \in S$ and

(b) $f(f(s,m),m') = f(s,mm')$ for every $s \in S$ and $m, m' \in M$.

f is called the *transition function* of $\mathfrak{A}$. We usually denote $f(s,u)$ by su.

Let $\mathfrak{A} = (S,f)$ be an M- automaton. The mapping $\tau_{\mathfrak{A}} : M \to T(S)$ from M into the monoid of all transformations on S defined by

$$s\tau_{\mathfrak{A}}(u) = f(s,u) \text{ for all } s \in S \text{ and } u \in M$$

is a monoid homomorphism. We denote $\tau_{\mathfrak{A}}$ by τ when there is no chance of ambiguity. $M/Ker\tau$ is a monoid, called the *transition monoid* of $\mathfrak{A}$ where

$$Ker\tau = \{(x,y) \in M \times M \mid s\tau(x) = s\tau(y) \ for \ all \ \ s \in S\}.$$

We denote $M/Ker\tau$ by $T(\mathfrak{A})$. Note that $T(\mathfrak{A})$ is isomorphic to $\tau(M)$.

For A^*-automaton $\mathfrak{A} = (S,f)$ with A^* being the free monoid on the alphabet A, the transition function f is entirely known when f is defined on $S \times A$.

An A^*- automaton $\mathfrak{A} = (S,f)$ is called *monogenic* if there exists $s_0 \in S$ such that $f(s_0, A^*) = S$ (s_0 is called a *generator* of $\mathfrak{A}$).

Monogenic A^*-automata are directly related to right congruence on A^*. If $\mathfrak{A} = (S,f)$ is an A^*-automaton generated by $s_0 \in S$, we define $\gamma(\mathfrak{A})$ as follows :

$$\gamma(\mathfrak{A}) = \{ \ (u,v) \in A^* \times A^* \mid f(s_0,u) = f(s_0,v) \ \}.$$

It is clear that $\gamma(\mathfrak{A})$ is a right congruence on A^*. Conversely, if ρ is a right congruence on A^*, denoting by $\overline{w}$ the class of w modulo ρ, we define $\alpha(\rho)$, the automaton of ρ, by:

$$\alpha(\rho) = (A^*/\rho, f) \quad \text{ with } \ f(\overline{w}, a) = \overline{wa} \ \text{ for all } w, a \in A^*.$$

A language $L \subseteq A^*$ is called *recognizable* if there exists an A^*-automaton $\mathfrak{A} = (S,f)$, with S finite, a state $s_0 \in S$ and a subset T of S such that

$$L = \{ \ w \in A^* \mid f(s_0,w) \in T \ \}.$$

We also say that the finite A^*-automaton $\mathfrak{A}$ recognize L, or that L is recognized by $\mathfrak{A}$. We can show that L is recognizable if and only if L is a union of classes of a right congruence on A^* of finite index.

Given any subset L of A^*, there is a largest right congruence $P_L^{(r)}$ for which L is a union of classes. It is defined by

$$P_L^{(r)} = \{\ (u,v) \in A^* \times A^* \mid uw \in L \Leftrightarrow vw \in L \ \text{ for every } w \in A^*\ \}.$$

Thus the A^*-automaton $\alpha(P_L^{(r)}) = \mathfrak{A}$ is a minimal automaton recognizing L. It is called the *minimal automaton* of L.

Let L be language of A^*. The *syntactic congruence* P_L is defined by

$$P_L = \{(u,v) \in A^* \times A^* \mid xuy \in L \Leftrightarrow xvy \in L \ \text{ for all } \ x, y \in A^*\}.$$

The quotient monoid A^*/P_L is called the *syntactic monoid* of L, denoted by $M(L)$.

In addition, $M(L)$ is isomorphic to the transition monoid of the minimal automaton $\alpha(P_L^{(r)})$ of L. Thus we can consider $M(L)$ as the transition monoid of the minimal automaton of L.

In this thesis, we are interested in a special type of language, a prefix code.

A subset C of the monoid A^* is called a *code* if, for every $m, n \geq 1$ and $c_1, c_2, ..., c_m, c_1', c_2', ..., c_n' \in C$,

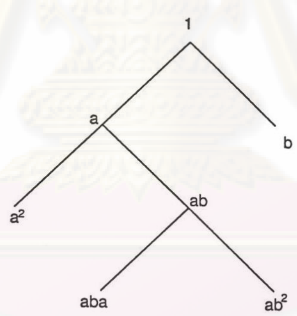
$$c_1c_2...c_m = c_1'c_2'...c_n' \Rightarrow m = n \text{ and } c_i = c_i' \text{ for all } i = 1, 2, ..., m.$$

A code C over the alphabet A is called a *prefix code*(resp. *suffix code*) if for every $u, v \in A^*$, uv and $u \in C$ implies $v = \varepsilon$ (resp. $u, v \in A^*$, uv and $v \in C$ implies $u = \varepsilon$); that is, a code C is a prefix code if no word in C is a proper left factor of other word of C. C is a *biprefix code* if it is both prefix and suffix.

In [5], P. Udomkavanich studied a prefix code whose syntactic monoid is an inverse semigroup. Such a code was proved to be biprefix. Thus it is called an *inverse biprefix code.*

The code $\{ a^2, ab, b^2 \}$ is an example of biprefix code on the alphabet $\{ a, b \}$. The code $\{ a^2, aba, ab^2, b \}$ is prefix which is not suffix.

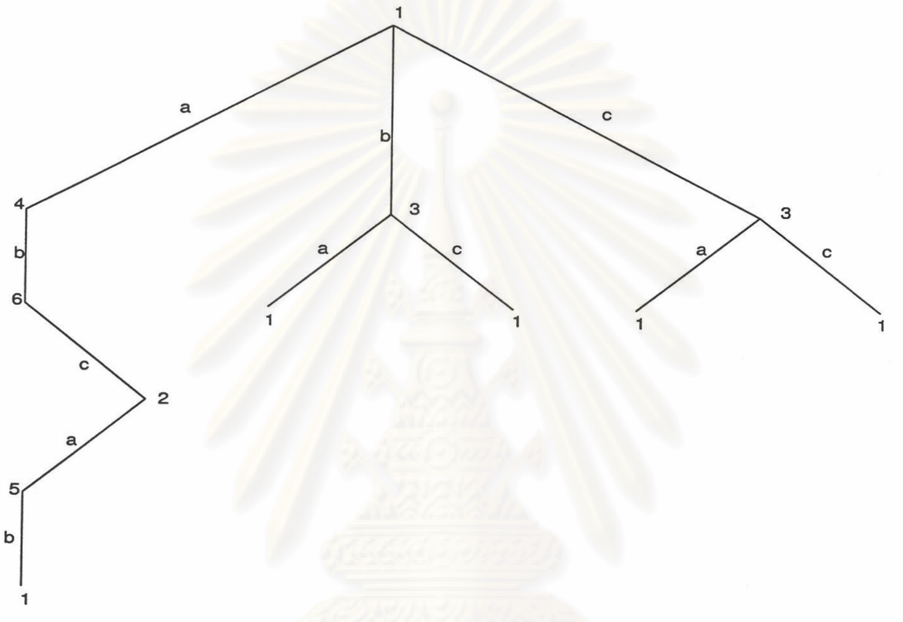
Defining the relation $\leq_l$ on A^* by $u \leq_l v$ if v is a left factor of u, we see that $\leq_l$ is a partial ordering on A^*. Hence $C \subseteq A^*$ is a prefix code if and only if for every $c \in C, u \in A^*; u \leq_l c$ and $u \neq c$ implies $u \in C$. Thus to obtain a prefix code, it suffices to select a subset C of A^* that will be endpoints for the relation $\leq_l$. For example the falling tree below



gives the prefix code $C = \{ a^2, aba, ab^2, b \}$ over $\{a, b\}$.

Let C be a prefix code over an alphabet A. To construct $P^{(r)}_{C^*}$, we denote by s the class of $P^{(r)}_{C^*}$ consisting of all words $u \in A^*$ such that $uA^* \cap C^* = \varnothing$. If $uA^* \cap C^* \neq \varnothing$, there exists a unique $c \in C^*$ and $z \in A^*$ such that $u = cz$ and z is a proper left factor of a word in C (eventually $z = \varepsilon$). The prefix property of C implies $(u, z) \in P^{(r)}_{C^*}$ and for any two proper left factor z_1, z_2 of words in C we have $(u, z) \in P^{(r)}_{C^*}$ if and only if $(u, z) \in P^{(r)}_{C}$. Finally, for every $c \in C, (c, \varepsilon) \in P^{(r)}_{C^*}$. It follows that the minimal automaton of C^* is obtained by drawing the tree representing words in C. Then we label the top of the tree and the end points with $\mathbf{1}$, and intermediate points using the same name, if they have identical subtrees.

Example 2.1. Let $A = \{a, b, c\}$ and $C = \{abcab, ba, bc, ca, c^2\}$ be a prefix code. The tree representing C is as shown:



The minimal automaton of C^* has six states, denoted by $1, 2, 3, 4, 5$ and 6. We have

$$f(1,a) = 4, \quad f(1,b) = 3, \quad f(1,c) = 3,$$

$$f(2,a) = 5, \quad f(4,b) = 6, \quad f(3,c) = 1,$$

$$f(3,a) = 1, \quad f(5,b) = 1 \text{ and } f(6,c) = 2$$

The corresponding syntactic monoid $M(C^*)$ is generated by

$$\tau(a) = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 1 \end{pmatrix} \quad \tau(b) = \begin{pmatrix} 1 & 4 & 5 \\ 3 & 6 & 1 \end{pmatrix} \quad \text{and} \quad \tau(c) = \begin{pmatrix} 1 & 3 & 6 \\ 3 & 1 & 2 \end{pmatrix}$$

In the tree representation of C^*, a node labelled s is called the *node associated with* a left factor x of a word in C, if x is a path joining the top of the tree and the nodes s. Thus the nodes associated with x and x' are labelled with the same name if $x^{-1}C = (x')^{-1}C$, where $u^{-1}C = \{ w \in A^* \mid uw \in C \}$.