UNIVERSITÉ DE MOHAMED BOUDIAF- M'SILA

MEMOIRE

Présentée à la Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

Pour l'obtention du diplôme de MASTER

Spécialité: Mathématiques

Option: Mathématiques discrètes

Par:

BAKRI Norelhouda

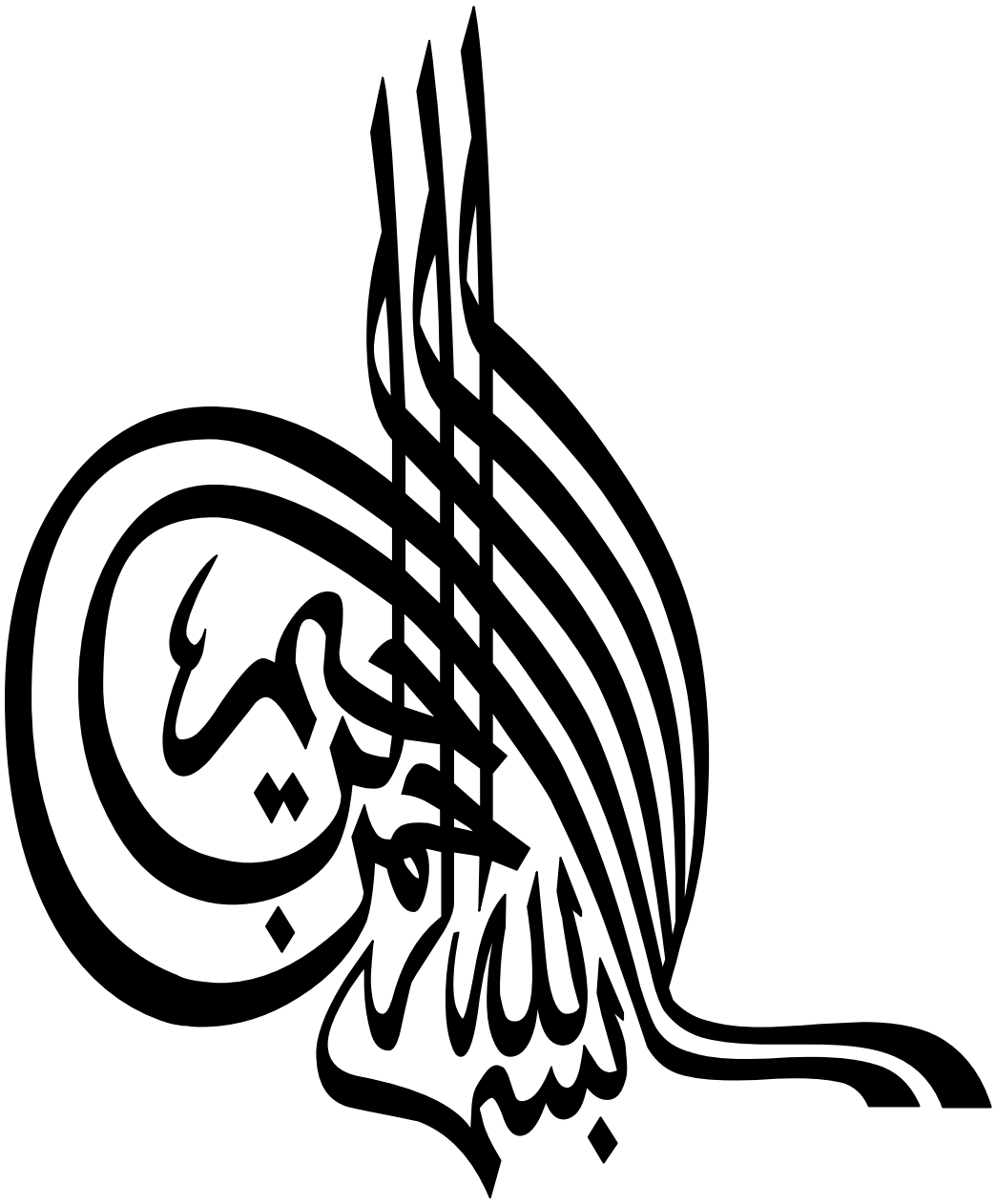
Intitulée:

Products of semigroups and applications on state machines

Soutenue publiquement le : /06/2015, devant le jury :

Lemnouar ZADEM	**Prof.**	**Université de M'sila**	**Président**
Douadi MIHOUBI	**Prof.**	**Université de M'sila**	**Rapporteur**
Lehcene LADJELAT	**M.A.A**	**Université de M'sila**	**Examinateur**
Nacer GHADBANE	**M.A.A**	**Université de M'sila**	**Examinateur**

Promotion 2014/2015


بسم الله الرحمن الرحيم

Université de M'sila

FACULTÉ DES MATHÉMATIQUES ET INFORMATIQUES

Département de Mathématiques

Mémoire de Fin D'etude

Présenté pour l'obtention du diplôme de **Master**

Domaine :Mathématiques et Informatique

Filière :Mathématiques

Spécialité :Mathématiques discrètes

Par

Norelhouda BAKRI

sujet

Products of semigroups and applications on state machines

Président

Promotion:2014/2015

Acknowledgements

Thanks to **GOD** almighty for the completion of this work. Only due to his blessings I could finish it.

I would like to express my deepest gratitude to my advisor, Mr : **D.Mihoubi**, for his valuable advices and suggestions, I also would like to express my thanks to Mr : **N.Ghadbane**, for his advices.

My thanks also go to the jury members for the honor they have done me by accepting to judge this modest work.

I would like to thank my beloved **parents** for their encouragement who are so supportive to me throughout my life. My sisters, brothers deserve my wholehearted thanks as well, to all my friends and all people who have helped me during my study.

this work is only a begining of my journey.

thanks

Index of notation

$\Re$	Relation
$dom(\Re)$	Domain of $\Re$
$rang(\Re)$	Range of $\Re$
$[a]$	Equivalence class defined by a
$A/\Re$	Quotient set of A with respect to $\Re$
$\sum^n$	Set of all words of length n
Λ	Empty string (null word)
$\sum^*$	Set of all words from $\sum$
$\sum^+$	Set of all words of length greater than or equal to 1 in $\sum$
$S^\cdot$	Semigroup S with adjoined unit
$\|G\|$	Order of a group G
$\langle S \rangle$	Subgroup of G generated by S
$End(G)$	Set of all endomorphisms of a group G
$Aut(G)$	Set of all automorphisms of a group G
$S \times T$	Direct product of semigroups
$G \times H$	Direct product of groups
$S \times_\theta T$	Semidirect product of semigroups with respect to θ
$G \ltimes_\theta H$	Semidirect product of groups with respect to θ
$S \circ T$	Wreath product of semigroups
$S^{T^\cdot}$	Set of all fuctions from the monoid $T^\cdot$ to the semigroup S
$A\ W_r\ B$	Wreath product of groups
$S(M)$	Semigroup of a state machine M
$(\alpha, \beta) : M \to M'$	State machine homomorphism
$M \cong M'$	Isomorphic state machines
$M \leq M'$	Covering (state machine)
$M \wedge M'$	Restricted direct product of state machines
$M \times M'$	(Full) direct product

$M \omega M'$	Cascade product
$M \circ M'$	Wreath product

Contents

General Introduction

The theory of machines that has developed in last twenty years has had a considerable influence, not only on the computer systems, but also biology, biochemestry, etc. So here we will interest in mathematical theory of various types of machines.

The area of mathematics that is of most use to us is that which is known as Modern (or abstract) algebra. For a hundred years, algebra has developed in different directions. The advent of the theory of machines, has provided us with new motivation for the development of algebra.

Recently the semigroups and groups has become an intresting area of study, and one of their operations is semidirect product and wreath product .

What we will be doing is to to apply this operations on state machines, by looking at various types of machines, their properties, and we will replace a general state machine by a collection of "algebraically simpler" machines connected up in suitable ways (cascade and wreath product).

This work is devided into three chapters

First we begin with some elementary material concerning the theory of semigroups and groups.

In the second chapter we have direct product, semidirect product and wreath product of semigroups and groups.

The third chapter examines many elementary properties of the state machine, the ways in which it can be connected together (direct, cascade and wreath product) and the use of this in decompostion theorem.

Chapter 1

algebraic preliminaries

Algebraic notions and connections used later are presented in this chapter.

1.1 Binary operation

Definition 1.1.1 *If A is a set, the direct product $A \times A$ consists of all ordered pairs (a, b) with a, b belongs to A. Using this terminology, a binary operation ,$\star$, on a set A is just a function from $A \times A$ to A.we denote the image of the pair (a, b) under this function by $a \star b$. In other words, the binary operation $\star$ assigns to any two elements a and b of A the element $a \star b$ of A.*

- *Many symbols are used for binary operation; like $+$, $\cdot$, $\circ$, $\wedge$, $*, \star, ...$*
- *A binary operation on a finite set can often presented conveniently by means of a table.*

1.2 Relations and mappings

Relations are one of the basic building blocks of mathematics.

1.2.1 Binary relation

Definition 1.2.1 *A **relation** $\Re$ from a set A to a set B is a subset of $A \times B$ and we say that a is related to b under $\Re$ if the pair (a, b) belongs to the subset, and we write this as $a \Re b$.*

- *A relation from a set A to itself is called a* ***relation on*** *A or a relation over A.*
- *"Equals" is a relation on any set A and is defined by the subset $\{(a,a) \mid a \in A\}$ of $A \times A$.*
- *$dom\ \Re = \{a \mid \exists b, a\Re b\}$ is the set of all such a's for which there exists at least one b such that $a\Re b$ holds, this set is called the domain of $\Re$.*
- *$rang\ \Re = \{b \mid \exists a, a\Re b\}$ is called the range of $\Re$.*

1.2.2 Equivalence relation

Definition 1.2.2 *A relation $\Re$ on a set A is called an* ***equivalence relation*** *if the following conditions hold*

(i) $a\Re a$ for all $a \in A$, (reflexive condition)

(ii) if $a\Re b$, then $b\Re a$, (symmetric condition)

(iii) if $a\Re b$ and $b\Re c$ then $a\Re c$. (transitive condition)

- *If $\Re$ is an equivalence relation on A and $a \in A$, then $[a] = \{x \in A \mid x\Re a\}$ is called the equivalence class containing a, the set of all equivalence classes is called the quotient set of A by $\Re$ and is denoted by $A/\Re$. Hence*

$$A/\Re = \{[a] \mid a \in A\}.$$

1.2.3 Mapping

In set theory mappings are a special binary relations.

Definition 1.2.3 *A relation φ from a set A to the set B satisfying the condition (1) is called a* ***mapping*** *from A into B (In words : every element of $dom\ \Re$ is in relation φ with exactly one element of $rang\ \Re$).*

$$a\varphi b_1, a\varphi b_2 \Rightarrow b_1 = b_2. \tag{1}$$

- *Distinct elements of A can be mapped by φ on the same element of B.*
- *A mapping is often also called a* ***function****. the image of a under the mapping φ is denoted by $\varphi(a)$ or $a\varphi$, then, for any relation φ*

$$a\varphi = \{b \mid a\varphi b\}.$$

- *A function (mapping) $\varphi : A \to B$ is called* ***injective*** *or* ***one-to-one*** *if*

$$\varphi(a_1) = \varphi(a_2) \Rightarrow a_1 = a_2 \text{ for all } a_1, a_2 \in A.$$

- *φ is called* ***surjective*** *or* ***onto*** *if*

$$\forall b \in B, \exists a \in A : b = \varphi(a).$$

- *A bijective function or* ***one-to-one correspondence*** *is a function that is both injective and surjective.*
- *a permutation of a set A is simply a bijection from A to A.*

1.3 Pointwise operation

Definition 1.3.1 *Pointwise operation is an extension of an algebraic operation $\star$ on a set A to a set of functions on a set B taking values in A. If f, g are functions taking values in A then the pointwise extension of a binary operation $\star$ is*

$$f \star g : b \to f(b) \star g(b) \text{ for each } b \in B$$

The terme "pointwise addition ", "pointwise multiplication" are also used.

1.4 Monoids and semigroups

We will usually drop the multiplication symbol "."when dealing with products of elements, writing ab in place of $a.b$.

1.4.1 Monoid

Definition 1.4.1 *A **monoid** $(M, ., e)$ consists of a set M together with a binary operation "." on M and identity element "e" such that*

(i) The operation "." is associative; that is

$$(a.b).c = a.(b.c) \text{ for all } a, b, c \in M.$$

(ii) There is an identity element $e \in M$ such that

$$e.a = a.e = a \text{ for all } a \in M.$$

- *The closure axiom is already implied by the definition of a binary operation.*
- *If the operation is **commutative**, that is, if $a.b = b.a$ for all $a, b \in M$ then, the monoid is called **commutative** or **abelien**, in honor of the mathematician Niels Abel.*

Example 1.4.1 *The algebraic objects $(\mathbb{N}, +); (\mathbb{N}, \times); (\mathbb{Z}, +); (\mathbb{Z}, \times); (\mathbb{Q}, +)$ are all commutative monoids.*

Example 1.4.2 *A computer receives its information from an input terminal that feeds in a sequence of symbols, usually binary digits consisting of 0's and 1's. If one sequence is fed in after another, the computer receives one long sequence that is the concatenation of the two sequences. These input sequences together with the binary operation of concatenation form a monoid.*

- *Let Σ be any set (sometimes called alphabet), and let Σ^n be the set of n-tuples of elements in Σ. We write an n-tuple as a string of elements of Σ without any symbols between them. The elements of Σ^n are called words of length n over Σ, then if $\alpha \in \Sigma^n$, length of α is the number of the symbols, and it is denoted by $|\alpha|$. A word of length 0 is an empty string and it is denoted by Λ .*
- *Let Σ^* denote the set of all words from Σ more formally*

$$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup ..... = \bigcup_{n=0}^{\infty} \Sigma^n$$

Then $(\Sigma^*, \cdot)$ is called the free monoid generated by Σ, where the binary operation $\cdot$ is concatenation, and the identity is the empty word Λ. If we do not include the empty word Λ, we optain a semigroup, this is often denoted by Σ^+ , that's mean $\Sigma^* = \Sigma^+ \cup \{\Lambda\}$.

1.4.2 Semigroup

sometimes an algebraic object would be a monoid but for the fact that it lacks an identity element; such an object is called semigroup.Hence

Definition 1.4.2 *A **semigroup** $(S, .)$ is just a set S together with an associative binary operation, that is*

$$(a.b).c = a.(b.c) \text{ for all } a, b, c \in S.$$

Example 1.4.3 *The algebraic objects $(\mathbb{N}, +); (\mathbb{Z}, +); (\mathbb{R}, +)$ are all semigroups, however $(\mathbb{Z}, -)$ is not a semigroup because subtraction is not associative, in general,*

$(a - b) - c \neq a - (b - c)$.

Remark 1.4.1 *Let S be a semigroup. suppose that S is not a monoid, choose any element $e \notin S$, the set $S^{\cdot} = S \cup \{e\}$ is a monoid under the multiplication $*$ on $S^{\cdot}$ and unit element e*

$$a * b = \begin{cases} ab \text{ if } a, b \in S \\ b \text{ if } a = e \\ a \text{ if } b = e \end{cases} \quad \text{where } a, b \in S.$$

- *If S is already a monoid then $S^{\cdot} = S$.*

1.4.3 Congruence relation on a semigroup

Definition 1.4.3 *Let S be any semigroup, a **congruence relation on** S is an equivalence relation $\sim$ satisfying*

$$a \sim b \text{ and } c \sim d \Rightarrow ac \sim bd \text{ such that } a, b, c \in S \quad \text{or}$$
$$a \sim b \Rightarrow as \sim bs \text{ and } sa \sim sb \text{ for all } s \in S.$$

Proposition 1.4.1 *Let S be a semigroup and $\sim$ a congruence relation on S. Consider the set of all equivalence classes defined on S by $\sim$, denote this set by $S/\sim$. We define a multiplication on $S/\sim$ as follows*

Let $[a], [b] \in S/\sim$

Put $[a] \star [b] = [ab]$ $(a, b \in S)$

Then the set $S/\sim$ under the operation $\star$ is a semigroup. We call $(S/\sim, \star)$ the quotient semigroup of S with respect to $\sim$.

Proof. This proof from [3]

The operation $\star$ is well defined for if

$[a] = [c]$ and $[b] = [d]$ then

$a \sim c$ and $b \sim d$, consequently

$ab \sim cb$ and $cb \sim cd$ and so $ab \sim cd$ (as $\sim$ is transitive)

that is $[ab] = [cd]$ and thus $[a] \star [b] = [c] \star [d]$.

Now we will prove that $\star$ is associative on $S/\sim$

Let $[a], [b], [c] \in S/\sim$ then

$$\begin{aligned}([a] \star [b]) \star [c] &= [ab] \star [c] \\ &= [(ab)c] \\ &= [a(bc)] \text{ as } S \text{ is a semigroup} \\ &= [a] \star [bc] \\ &= [a] \star ([b] \star [c]).\end{aligned}$$

Then $(S/\sim, \star)$ is a semigroup. ■

1.5 Groups theory

1.5.1 Group

Definition 1.5.1 *A **group** $(G, .)$ is a set together with a binary operation"." satisfying the following axioms*

(i) The operation "." is associative; that is

$$(a.b).c = a.(b.c) \text{ for all } a, b, c \in G.$$

(ii) There is an identity element $e \in G$ such that

$$e.a = a.e = a \text{ for all } a \in G.$$

(iii) Each element $a \in G$ has an inverse element $a^{-1} \in G$ such that

$$a^{-1}.a = a.a^{-1} = e.$$

- *If the operation is commutative, the group is called commutative or abelain.*
- *A group $(G, .)$ is called cyclic if there exists an element $g \in G$ such that*

$$G = \{g^n \mid n \in \mathbb{Z}\}$$

The element g is called a generator of the cyclic group .

- *The number of elements in a group G is written $|G|$ and is called the order of the group.*

Example 1.5.1 *Let G be a set of complex numbers $\{1, -1, i, -i\}$ and let "." be the standard multiplication of complex numbers, then $(G, .)$ is an abelian group, because*

- *The product of any two of these element is an element of G, and this can be represented in the Table* 1.1.
- *Multiplication of complex numbers is always associative and commutative.*
- *The identity element is* 1.
- *The inverse of each element a from G is the element $1/a$. Hence*

$1^{-1} = 1$, $(-1)^{-1} = -1, i^{-1} = -i$, $(-i)^{-1} = i$.

.	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Table 1.1 group G.

Remark 1.5.1

- *The identity element of a group (monoid) is a unique element and we can denote it by* e_G *or* 1_G.
- *If the element* a *has an inverse, this inverse is a unique element.*

Proposition 1.5.1 *If* $a, b,$ *and* c *are elements of a group* G *, then*

(i) $(a^{-1})^{-1} = a$.

(ii) $(ab)^{-1} = b^{-1}a^{-1}$.

(iii) $ab = ac$ *or* $ba = ca$ *implies that* $b = c$ *(cancellation law).*

Proof. *[9] (i) The inverse of* a^{-1} *is an element* b *such that* $a^{-1}b = ba^{-1} = e$ *, but* a *is such an element (because* a^{-1} *is the inverse of* a*), and we know that the inverse is unique. Hence* $(a^{-1})^{-1} = a$.

(ii) Using associativity, we have

$(ab)(b^{-1}a^{-1}) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e$.

Hence $b^{-1}a^{-1}$ *is the unique inverse of* ab.

(iii) Suppose that $ab = ac$. *then* $a^{-1}(ab) = a^{-1}(ac)$, *so* $(a^{-1}a)b = (a^{-1}a)c$. *that is,* $eb = ec$ *and* $b = c$. *similarly* $ba = ca$ *implies that* $b = c$. ■

1.5.2 subgroup

Definition 1.5.2 *If* $(G, .)$ *is a group and* H *is non empty subset of* G*, then* $(H, .)$ *is called a* ***subgroup*** *of* $(G, .)$ *if the following conditions hold*

(i) $a.b \in H$ *for all* $a, b \in H$ *(closure).*

(ii) $a^{-1} \in H$ *for all* $a \in H$ *(existence of inverses), And we will denote this by* $H \leq_G G$.

Example 1.5.2 • $\{e\}$ *and* G *are trivial subgroup of* $(G, .)$.

- $(\mathbb{Z}, +)$ *is a subroup of* $(\mathbb{Q}, .)$.

1.5.3 Subgroups generated by subsets

Definition 1.5.3 *Let S be a subset of a group G. Then the subgroup of G generated by S, denoted by $\langle S\rangle$, is defined to be the intersection*

$$\langle S\rangle = \bigcap_{\substack{S\subset K \\ K\leq_G G}} K$$

Then this definition ensures that $\langle S\rangle$ is the smallest subgroup of G containing S.

Remark 1.5.2 *If the set S in the definition above happens to be a finite, say $S = \{g_1, g_2, ...g_n\}$ then we normally write $\langle g_1, g_2, ...g_n\rangle$ instead of $\langle\{g_1, g_2, ...g_n\}\rangle$ when speaking about this subgroup.*

1.5.4 Normal subroup

Definition 1.5.4 *A subgroup H of a group G is called normal subgroup of G if*

$$\begin{aligned} g^{-1}hg &\in H \text{ for all } g \in G \text{ and } h \in H \quad \text{or} \\ Hg &= gH \text{ for all } g \in G. \end{aligned}$$

• Let G be a group with subgroup H, the right **cosets** of H in G are equivalence classes under the relation $\Re$ defined by $ab^{-1} \in H$. We can aslo define the relation L on G so that aLb if and only if $b^{-1}a \in H$, this relation is an equivalence relation, and the equivalence class containing a is the left **coset** $aH = \{ah \mid h \in H\}$.

• If H is a normal subgroup of G, then, the right coset and the left coset of H in G are the same, that is, $Ha = Ha$ for all $g \in G$.

And this is helps us to give this theorem.

Theoreme 1.5.1 *If N is a normal subgroup of G, the set of cosets $G/N = \{Ng \mid g \in G\}$ forms a group $(G/N, .)$ where the operation is defined by $(Ng_1).(Ng_2) = N(g_1g_2)$, this group is called the quotient group of G by N .*

1.5.5 Action of a group on a set

Definition 1.5.5 *The group $(G,.)$ acts on the set X if there is a function such that when we write $g(x)$ for $\psi(g,x)$ we have*

$$\psi : G \times X \to X$$

(i) $(g_1g_2)(x) = g_1(g_2(x))$ for all $g_1, g_2 \in G$, $x \in X$.
(ii) $e(x) = x$ if e is the identity of G and $x \in X$.

1.6 Morphisms

1.6.1 Group morphism

In group theory, the most important functions between two groups are those that "preserve" the group operations, and they are called homomorphisms (or morphisms).

Definition 1.6.1 *If $(G,.)$ and $(H,*)$are two groups, the function $f : G \to H$ called a group morphism if*

$$f(g_1.g_2) = f(g_1) * f(g_2) \text{ for all } g_1, g_2 \in G.$$

- *A group morphism $f : G \to G$ will be called an endomorphism, the set of all endomorphism of a group will be denoted by $End(G)$.*

Example 1.6.1 • *For each real number c, the formula $c(x+y) = cx + cy$ for all x and y in $\mathbb{R}$ says that the function $f_c(x) = cx$ is a group homomorphism.*

• *For all positive numbers x and y , $\sqrt[2]{xy} = \sqrt[2]{x}\sqrt[2]{y}$, so the square root function $f : \mathbb{R}^+ \to \mathbb{R}^+$, where $f(x) = \sqrt[2]{x}$ is a homomorphism.*

Proposition 1.6.1 *Let $f : G \to H$ be a group morphism, and let e_G and e_H be the identities of G and H, respectively. then*

(i) $f(e_G) = e_H$.
(ii) $f(a^{-1}) = (f(a))^{-1}$ for all $a \in G$.

Proof. *this proof from [9]*

(i) Since f is a morphism

$f(e_G)\ f(e_G) = f(e_G.e_G) = f(e_G) = f(e_G).e_H$

Hence (i) follows by cancellation law in H (proposition 1.1.)

Then $f(e_G) = e_H$.

(ii) We have

$f(a)\ f(a^{-1}) = f(a.a^{-1}) = f(e_G) = e_H$ *by (i).*

Hence $f(a^{-1})$ is the unique inverse of $f(a)$;that is, $f(a^{-1}) = (f(a))^{-1}$. ■

1.6.2 Semigroup morphism

Definition 1.6.2 *Let $(S, \intercal)$ and $(T, *)$ be a semigroups, the function $g : S \to T$ is a semigroup morphism if*

$$g(x_1 \intercal x_2) = g(x_1) * g(x_2) \text{ for all } x_1, x_2 \in S.$$

Example 1.6.2 *Let $S = (\mathbb{N}, +)$ and $T = (\mathbb{N}, .)$; and define $g(n) = 2^n$ for all $n \in \mathbb{N}$. Now;*

$$g(n + m) = 2^{n+m} = 2^n.2^m = g(n).g(m)$$

And hence $g : S \to T$ is a semigroup morphism.

Remark 1.6.1 *the set of all endomorphism of a semigroup S will be denoted by $End(S)$, and this set form a semigroup under the composition of functions. Hence $(End(S), \circ)$ is a semigroup.*

1.6.3 monoid morphism

Definition 1.6.3 *If $(M_1, *)$ and $(M_2, \triangle)$ are monoids with identities e_1 and e_2 respectively, the function $h : M_1 \to M_2$ is a monoid morphism if the two conditions hold*

(i) $h(a * b) = h(a) \triangle h(b)$ for all $a, b \in M_1$.

(ii) $h(e_1) = e_2$.

1.7 Isomorphism

Definition 1.7.1 *A group isomorphism is a bijective group morphism, if there is an isomorphism between the group $(G, .)$ and $(H, *)$, we say that the two groups are isomorphic and write $(G, .) \cong (H, *)$.*

- *A group isomorphism $g : G \to G$ will be called an automorphism, the set of all automorphism of a group will be denoted by $Aut(G)$.*
- *A semigroup (monoid) isomorphism is a bijective semigroup (monoid) morphism.*

Chapter 2

Direct product, semidirect product and wreath product

Semigroups (groups) can be joined together in various way to produce more semigroups (groups). So we will examine here some important methods of doing this.

2.1 direct product

2.1.1 direct product of semigroups

Proposition 2.1.1 *Let S and T be semigroups, consider the set $S \times T$, the cartesian product of S and T, and define a multiplication "." on $S \times T$ as follows*

$$(x_1, y_1).(x_2, y_2) = (x_1x_2, y_1y_2) \text{ for all } x_1, x_2 \in S,\ y_1, y_2 \in T$$

The result is a semigroup $(S \times T, .)$ which is called the direct product of S and T, written $S \times T$.

Proof. *It is easy to show that this product is associative.* ■

Example 2.1.1 *Let $S = (\mathbb{N}, +)$ and $T = (\mathbb{N}, \times)$, then in the direct product $S \times T$ we have*

$$(n, r).(m, k) = (n + m, rk) \text{ where } n, m \in S,\ r, k \in T.$$

Lemma 2.1.1 *Given three semigroups S, T, W, we can form the direct product $(S \times T) \times W$; similarly $S \times (T \times W)$ and the relationship between these two semigroups is the isomorphism so*

$$(S \times T)W \cong S \times (T \times W).$$

Proof. the isomorphism is

$$\begin{aligned} f &: (S \times T)W \to S \times (T \times W) \text{ defined by} \\ f((x, y), z) &= (x, (y, z)) \text{ where } x \in S, y \in T, z \in W. \end{aligned}$$

■

2.1.2 Direct product of groups

Proposition 2.1.2 *If $(G, \circ)$ and $(H, *)$ are two groups, then $(G \times H, \cdot)$ is a group under the binary operation $\cdot$ defined by*

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \circ g_2, h_1 * h_2) \text{ where } g_1, g_2 \in G;\ h_1, h_2 \in H$$

The group $(G \times H, \cdot)$ is called the direct product of the groups $(G, \circ)$ and $(H, *)$.

Proof. *We will prove that $(G \times H, \cdot)$ is a group*

• *For the fact that $(G, \circ)$ and $(H, *)$ are associative we have*

$$\begin{aligned} ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) &= (g_1 \circ g_2, h_1 * h_2) \cdot (g_3, h_3) \\ &= ((g_1 \circ g_2) \circ g_3, (h_1 * h_2) * h_3) \\ &= (g_1 \circ (g_2 \circ g_3), h_1 * (h_2 * h_3)) \\ &= (g_1, h_1) \cdot (g_2 \circ g_3, h_2 * h_3) \\ &= (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)) \end{aligned}$$

Where $g_1, g_2, g_3 \in G$ and $h_1, h_2, h_3 \in H$.

Then the operation " $\cdot$ " is associative on $G \times H$.

- *The identity element of $G \times H$ is (e_G, e_H), where e_G is the identity element of G and e_H is the identity element of H.*
- *the inverse of (g, h) is (g^{-1}, h^{-1}), where $(g, h) \in G \times H$.*

Hence $(G \times H, \cdot)$ is a group. ■

Example 2.1.2 *Let $C_2 = \{e, g\}$, be a set, the direct product of C_2 with itself is $C_2 \times C_2 = \{(e,e), (e,g), (g,e), (g,g)\}$, and its table is given in Table 2.1.*
We see that $C_2 \times C_2$ is a group, where (e, e) is the identity element and the inverse of each element of $C_2 \times C_2$ is the same element .

$\cdot$	(e,e)	(e,g)	(g,e)	(g,g)
(e,e)	(e,e)	(e,g)	(g,e)	(g,g)
(e,g)	(e,g)	(e,e)	(g,g)	(g,e)
(g,e)	(g,e)	(g,g)	(e,e)	(e,g)
(g,g)	(g,g)	(g,e)	(e,g)	(e,e)

Table 2.1. Group $C_2 \times C_2$.

2.2 semidirect product

2.2.1 semidirect product of semigroups

Proposition 2.2.1 *Given any semigroups S and T, suppose that $\theta : T \to End(S)$ is a semigroup morphism. Then $(S \times T, \circledast)$ is a semigroup under the operation $\circledast$ defined by*

$$\begin{aligned} (x,y) \circledast (x',y') &= (x\theta(y)(x'), yy') \quad \text{where} \\ x, x' &\in S;\ y, y' \in T \\ \theta(y) &: S \to S \\ \theta(y)(x') &\in S \end{aligned}$$

The semigroup $(S \times T, \circledast)$ is called the semidirect product of S and T with respect to θ and it is denoted by $S \times_\theta T$.

Proof. *From [3], so we will prove that $\circledast$ is associative on $S \times T$*

Let $x, x', x'' \in S$; $y, y', y'' \in T$ so

$$\begin{aligned}((x,y) \circledast (x',y')) \circledast (x'',y'') &= (x\theta(y)(x'), yy') \circledast (x'',y'') \\ &= (x\theta(y)(x')\theta(yy')(x''), yy'\ y'') \\ &= (x\theta(y)(x')\theta(y)(\theta(y')(x'')), yy'\ y''),\ \textit{as } \theta \textit{ is a morphism} \\ &= (x\theta(y)(x'\theta(y')(x'')), yy'\ y''),\ \textit{as } \theta(y) \in End(S) \\ &= (x\theta(y)(x'\theta(y')(x'')), y\quad y'y''),\ \textit{as } T \textit{ is a semigroup} \\ &= (x,y) \circledast (x'\theta(y')(x''), y'y'') \\ &= (x,y) \circledast ((x',y') \circledast (x'',y''))\end{aligned}$$

Then $\circledast$ is associative on $S \times T$, hence $(S \times T, \circledast)$ is a semigroup. ■

2.2.2 semidirect product of groups

Proposition 2.2.2 *Given any groups G and H and a morphism $\theta : G \to Aut(H)$, denote the automorphism $\theta(g)$ by θ_g , then $G \times H$ is a group with the multiplication $\cdot$*

$$\begin{aligned}(g_1,h_1)\cdot(g_2,h_2) &= (g_1g_2, h_1\theta_{g_1}(h_2)) \quad \textit{where} \\ g_1, g_2 &\in G;\ h_1, h_2 \in H \\ \theta_{g_1} &\in Aut(H) \\ \theta_{g_1}(h_2) &\in H\end{aligned}$$

The group $(G \times H\ , \cdot)$ is called the semidirect product of G and H with respect to θ and it is denoted by $G \ltimes_\theta H$.

Proof. • *we will prove that the operation " $\cdot$ " is associative on $G \times H$*

Let $g_1, g_2, g_3 \in G$; $h_1, h_2, h_3 \in H$.

$$\begin{aligned}((g_1,h_1)\cdot(g_2,h_2))\cdot(g_3,h_3) &= (g_1g_2, h_1\theta_{g_1}(h_2))\cdot(g_3,h_3)\\ &= (g_1g_2 \quad g_3, h_1\theta_{g_1}(h_2)\theta_{g_1g_2}(h_3))\\ &= (g_1g_2 \quad g_3, h_1\theta_{g_1}(h_2)\theta_{g_1}(\theta_{g_2}(h_3))),\ \textit{as } \theta \textit{ is a group morphism}\\ &= (g_1g_2 \quad g_3, h_1\theta_{g_1}(h_2\theta_{g_2}(h_3))),\ \textit{as } \theta_{g_1}\in Aut(H)\\ &= (g_1 \quad g_2g_3, h_1\theta_{g_1}(h_2\theta_{g_2}(h_3))),\ \textit{as } G \textit{ is a group}\\ &= (g_1,h_1)\cdot(g_2g_3, h_2\theta_{g_2}(h_3))\\ &= (g_1,h_1)\cdot((g_2,h_2)\cdot(g_3,h_3))\end{aligned}$$

Then $\cdot$ is associative on $G\times H$.

- *The identity element of $G\times H$ is (e_G,e_H)*

$$\begin{aligned}(g,h)\cdot(e_G,e_H) &= (ge_G, h\theta_g(e_H))\\ &= (g, he_H),\ \textit{as } \theta_g\in Aut(H)\\ &= (g,h).\end{aligned}$$

And

$$\begin{aligned}(e_G,e_H)\cdot(g,h) &= (e_Gg, e_H\theta_{e_G}(h))\\ &= (g, e_H id(h)),\ \textit{as } \theta \textit{ is a morphism}\\ &= (g,h).\end{aligned}$$

- *The inverse of (g,h) is $(g^{-1},\theta_{g^{-1}}(h^{-1}))$ where $(g,h)\in G\times H$*

Its easy to find this inverse so

First because of the bijectivity of θ_g , there exist an element $h^{'}\in H$ such that

$\theta_g(h^{'}) = h^{-1}$,

Then

$$\begin{aligned}(g,h)\cdot(g^{-1},h^{'}) &= (gg^{-1}, h\theta_g(h^{'}))\\ &= (gg^{-1}, hh^{-1})\\ &= (e_G,e_H).\end{aligned}$$

Second we know that $\theta_{g^{-1}} = (\theta_g)^{-1}$, as θ is a morphism, then

$$\begin{aligned}\theta_{g^{-1}}(h^{-1}) &= \theta_{g^{-1}}(\theta_g(h^{'}))\\ &= (\theta_g)^{-1}(\theta_g(h^{'}))\\ &= h^{'}.\end{aligned}$$

And this give us

$$\begin{aligned}\theta_{g^{-1}}(h) &= \theta_{g^{-1}}((h^{-1})^{-1}) \\ &= (\theta_{g^{-1}}(h^{-1}))^{-1} \\ &= h'^{-1},\end{aligned}$$

Then

$$\begin{aligned}(g^{-1}, h') \cdot (g, h) &= (g^{-1}g, h'\theta_{g^{-1}}(h)) \\ &= (g^{-1}g, h'h'^{-1}) \\ &= (e_G, e_H).\end{aligned}$$

Then the inverse element of (g, h) *is* $(g^{-1}, \theta_{g^{-1}}(h^{-1}))$.

Hence $(G \times H\ , \cdot)$ *is a group.* ■

2.3 Wreath product

2.3.1 Wreath product of semigroups

Proposition 2.3.1 *Let* S *and* T *be two semigroups, and* $T^{\cdot}$ *be a monoid, and let* $S^{T^{\cdot}}$ *denote the set of all functions from the monoid* $T^{\cdot}$ *to the semigroups* S*, then*

The set $S^{T^{\cdot}} \times T$ *is a semigroup under the multiplication* $\circ$

$$(f, y_1) \circ (g, y_2) = (f \circ g, y_1 y_2)$$

Where $f \circ g \in S^{T^{\cdot}}$ *is defined by* $(f \circ g)(z) = f(z)g(zy_1)$ *for* $z \in T^{\cdot}$, $f, g \in S^{T^{\cdot}}$, $y_1, y_2 \in T$

We call the semigroup $S^{T^{\cdot}} \times T$ *the wreath product of* S *and* T *and write it as* $S \circ T$.

Proof. *From [3], we will prove that* $\circ$ *is associtive on* $S^{T^{\cdot}} \times T$ *so*

Let $f, g, h \in S^{T^{\cdot}}$ *and* $y_1, y_2, y_3 \in T$ *then*

$$\begin{aligned}(((f, y_1) \circ (g, y_2)) \circ (h, y_3)) &= (f \circ g, y_1 y_2) \circ (h, y_3) \\ &= ((f \circ g) \circ h, y_1 y_2 \quad y_3)\end{aligned}$$

And

$$\begin{aligned}((f, y_1) \circ ((g, y_2) \circ (h, y_3))) &= (f, y_1) \circ (g \circ h, y_2 y_3) \\ &= (f \circ (g \circ h), y_1 \quad y_2 y_3) \\ &= (f \circ (g \circ h), y_1 y_2 \quad y_3),\ \textit{as } T \textit{ is a semigroup}\end{aligned}$$

Then, we will prove that $(f \circ g) \circ h = f \circ (g \circ h)$.

Let $z \in T^{\cdot}$, then

$$((f \circ g) \circ h)(z) = (f \circ g)(z)h(zy_1y_2)$$
$$= f(z)g(zy_1)h(zy_1y_2)$$

And

$$(f \circ (g \circ h))(z) = f(z)(g \circ h)(zy_1)$$
$$= f(z)g(zy_1)h(zy_1y_2)$$

So we proved the associativity of the multiplication on the set $S^{T^{\cdot}} \times T$.

Hence the $S^{T^{\cdot}} \times T$ is a semigroup under the multiplication $\circ$. ■

2.3.2 Wreath product of groups

The wreath product of two groups A and B is consructed in the following way.

Proposition 2.3.2 *Let A^B be the set of all functions defined on B with values in A. With respect to pointwise multiplication, this set is a group; B acts on A^B as a group of automorphisms in the following way*

$$\text{if } b \in B, \phi \in A^B, \text{then } \phi^b(x) = \phi(xb^{-1}) \text{ for } x \in B$$

with respect to this operation, one can form the semidirect product W of B and A^B, that is, the set of all pairs (b, ϕ) where $b \in B, \phi \in A^B$, with multiplication operation given by

$$(b, \phi).(c, \psi) = (bc, \phi^c\psi) \text{ where } b, c \in B, \phi, \psi \in A^B$$

The resulting group W is called the wreath product of A and B, and is denoted by $A\ W_r\ B$ (or $A \bar{\wr} B$).

Proof. This proof from [5] is devided into three parts.

Part 1

• first we will prove that the set A^B forms a group such that for any $\phi_1, \phi_2 \in A^B$, let $\phi_1\phi_2$ in A^B be defined for all $x \in B$ by

$$(\phi_1\phi_2)(x) = \phi_1(x)\phi_2(x)$$

Thus composition of functions is pointwise.

(i) A^B is non-empty and is closed with respect to multiplication. If $\phi_1, \phi_2 \in A^B$, then $\phi_1(x), \phi_2(x) \in A$, for all $x \in B$

Hence $\phi_1(x).\phi_2(x) \in A$.This implies that $(\phi_1\phi_2)(x) \in A$ and so $\phi_1\phi_2 \in A^B$.

(ii) since multiplication is associative so also is the multiplication in A^B.

(iii) the identity element in A^B is the map $e : B \to A$ given by

$e(x) = 1_A$ for all $x \in B, 1_A \in A$.

(iv) every element $\phi \in A^B$ is defined for all $x \in B$ by $\phi^{-1}(x) = (\phi(x))^{-1}$.

Thus A^B is a group with respect to the multiplication defined above.

Part 2

• second we will prove that B acts on A^B as a group of automorphisms,

assume that B acts on A^B as follows

$B\times\ A^B \to A^B; (b, \phi) \to \phi^b$ such that

For $x \in B$ we have $\phi^b(x) = \phi(xb^{-1})$, $b \in B, \phi^b \in A^B$

Take $\phi, \phi_1, \phi_2 \in A^B, b, b_1, b_2 \in B$ then

$$
\begin{aligned}
(i)\ (\phi^{b_1})^{b_2}(x) &= \phi^{b_1}(xb_2^{-1}) \\
&= \phi((xb_2^{-1})b_1^{-1}) \\
&= \phi(x(b_1b_2)^{-1}) \\
&= \phi^{b_1b_2}(x).
\end{aligned}
$$

$$
\begin{aligned}
(ii)\ \phi^{1_B}(x) &= \phi(x1_B^{-1}) \\
&= \phi(x).
\end{aligned}
$$

$$
\begin{aligned}
(iii)\ (\phi_1\phi_2)^b(x) &= \phi_1\phi_2(xb^{-1}) \\
&= \phi_1(xb^{-1})\phi_2(xb^{-1}) \\
&= \phi_1^b(x)\phi_2^b(x).
\end{aligned}
$$

Then B acts on A^B as a group of automorphisms.

Part 3

• Now we can construct the wreath product W of A and B, that is, the semidirect product of B and A^B,

Then we will prove that $B \times A^B$ is a group with multiplication

$$(b, \phi).(c, \psi) = (bc, \phi^c\psi).$$

Then

(i) closure property follows from the definition of multiplication.

(ii) Take $\phi, \psi, \eta \in A^B$ and $b, c, d \in B$. then

$$\begin{aligned}((b,\phi).(c,\psi)).(d,\eta) &= (bc, \phi^c\psi).(d,\eta)\\ &= ((bc)d, (\phi^c\psi)^d\eta).\end{aligned}$$

Also we have

$$\begin{aligned}(b,\phi).((c,\psi).(d,\eta)) &= (b,\phi).(cd, \psi^d\eta)\\ &= (b(cd), \phi^{cd}(\psi^d\eta))\\ &= ((bc)d, \phi^{cd}(\psi^d\eta)).\end{aligned}$$

Now if $x \in B$ then

$$\begin{aligned}(\phi^c\psi)^d\eta(x) &= (\phi^c\psi)^d(x)\eta(x), \text{ (from pointwise multiplication)}\\ &= ((\phi^c)^d(x)\psi^d(x))\eta(x), \text{ (from part 2 } (iii))\\ &= (\phi^c(xd^{-1})\psi(xd^{-1}))\eta(x)\\ &= (\phi((xd^{-1})c^{-1})\psi(xd^{-1}))\eta(x)\\ &= (\phi(x(cd)^{-1})\psi(xd^{-1}))\eta(x)\\ &= (\phi^{cd}(x)\psi^d(x))\eta(x).\end{aligned}$$

And

$$\begin{aligned}\phi^{cd}(\psi^d\eta)(x) &= \phi^{cd}(x)(\psi^d\eta)(x), \text{ (from pointwise multiplication)}\\ &= \phi^{cd}(x)(\psi^d(x)\eta(x))\\ &= (\phi^{cd}(x)\psi^d(x))\eta(x), \text{ (from part 1 } (ii))\end{aligned}$$

And thus we have established the associativity of the multiplication on the set $B\times\ A^B$.

(iii) We know that for every $\phi \in A^B, \phi^{1_B} = \phi$ (part 2 (ii))

now for every $b \in B$, the map $\phi \to \phi^b$ is an automorphism of A^B. Also if e is the identity element in A^B then $e^b = e$

$$\begin{aligned}(b,\phi).(1_B, e) &= (b1_B, \phi^{1_B}e)\\ &= (b, \phi e)\\ &= (b,\phi).\end{aligned}$$

Also

$$\begin{aligned}(1_B, e).(b, \phi) &= (1_B b, e^b \phi) \\ &= (b, e\phi) \\ &= (b, \phi)\end{aligned}$$

Thus identity element exists.

$$\begin{aligned}(iv)\ (b, \phi).(b^{-1}, (\phi^{-1})^{b^{-1}}) &= (bb^{-1}, \phi^{b^{-1}}(\phi^{-1})^{b^{-1}}) \\ &= (1_B, \phi^{b^{-1}}(\phi^{-1})^{b^{-1}})\end{aligned}$$

And

$$\begin{aligned}(b^{-1}, (\phi^{-1})^{b^{-1}}).(b, \phi) &= (b^{-1}b, ((\phi^{-1})^{b^{-1}})^b \phi) \\ &= (1_B, ((\phi^{-1})^{b^{-1}})^b \phi).\end{aligned}$$

If $x \in B$ then

$$\begin{aligned}\phi^{b^{-1}}(\phi^{-1})^{b^{-1}}(x) &= \phi^{b^{-1}}(x)(\phi^{-1})^{b^{-1}}(x) \text{ (pointwise multiplication)} \\ &= (\phi\phi^{-1})^{b^{-1}}(x) \text{ (part 2 } (iii)) \\ &= e^{b^{-1}}(x) \\ &= e(x)\end{aligned}$$

Also

$$\begin{aligned}((\phi^{-1})^{b^{-1}})^b \phi(x) &= ((\phi^{-1})^{b^{-1}})^b(x)\phi(x) \\ &= (\phi^{-1})^{b^{-1}b}(x)\phi(x) \text{ (part 2 } (ii)) \\ &= (\phi^{-1})^{1_B}(x)\phi(x) \\ &= \phi^{-1}(x1_B^{-1})\phi(x) \\ &= \phi^{-1}(x)\phi(x) \\ &= e(x)\end{aligned}$$

Thus the inverse element of (b, ϕ) is $(b^{-1}, (\phi^{-1})^{b^{-1}})$.

Hence $B \times A^B$ is a group with respect to the multiplication defined above. ■

Chapter 3

Machines and its decomposition

In this chapter we will recognize the state machines and we will find that they are natural subjects for study also we can initiate the algebraic theory of these objects. As with other algebraic theories one approach is the decompostion of state machines.

3.1 Basic definitions on state machines

3.1.1 State machine

Definition 3.1.1 *A state machine is a triple $M = (Q, \Sigma, \delta)$ where Q is a finite set of states, Σ is a finite set of symbols called the input alphabet and $\delta : Q \times \Sigma \to Q$ is a partial function called the transition function.*

- *A partial state machine is such where δ may be undefined for some combinations of state and symbols.*
- *A state machine $M = (Q, \Sigma, \delta)$ is called complete if the partial function $\delta : Q \times \Sigma \to Q$ is in fact a function. In this situation we can specify what the resultant $\delta(q, \sigma)$ is, for all possible combinations of $q \in Q$ and $\sigma \in \Sigma$.*
- *the transition function can be extended naturally to sequences of input symbols, by letting $\delta(q, w\sigma) = \delta(\delta(q, w), \sigma)$, and to set of states by letting $\delta(Q', \sigma) = \{\delta(q, \sigma) : q \in Q'\}$.*

3.1.2 How to represente a state machine

A state machine is often descriped by means of a table (called the transition table) because we will write the transition function δ in tabular form.

This form of representation can be sisualized by a directed graph (diagram) whose nodes correspond to states and its edges to transitions (see figure 3.1).

Although such a representation is finite, it might be impractical in many situations where the state space is large.

• We have a simple example that show us the representation of a state machine M such that $Q = \{p, q, r\}$, $\Sigma = \{a, b, c\}$ and a transition function δ.

δ	p	q	r
a	q	q	r
b	p	p	$\varnothing$
c	q	r	r

Table 3.1 Transition table of M.

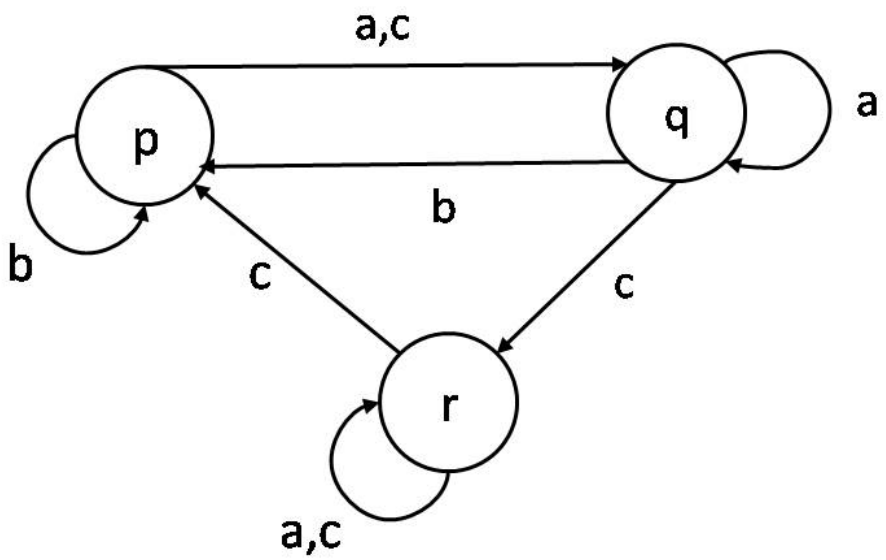


Figure 3.1 A state machine M.

Here $\delta(r,b)$ is undefined, we write it as $\varnothing$ in the table, the fact that $\delta(r,b)$ is undefined is indicated on the diagram by the lack of an arrow labelled by b emanating from the state r, and we call M an incomplete state machine.

Example 3.1.1 *suppose that* $Q=\{1,2,3,4,5,6\}$, $\Sigma=\{\sigma_0,\sigma_1\}$,

$$\delta=\left\{\delta_{\sigma_0}=\begin{pmatrix}1&2&3&4&5&6\\3&1&2&1&3&5\end{pmatrix},\delta_{\sigma_1}=\begin{pmatrix}1&2&3&4&5&6\\4&5&3&3&3&3\end{pmatrix}\right\}$$

Then $M=(Q,\Sigma\ ,\delta)$ *is a state machine with six states and two inputs,*

M	*1*	*2*	*3*	*4*	*5*	*6*
σ_0	*3*	*1*	*2*	*1*	*3*	*5*
σ_1	*4*	*5*	*3*	*3*	*3*	*3*

Table 3.2 The transition table of M.

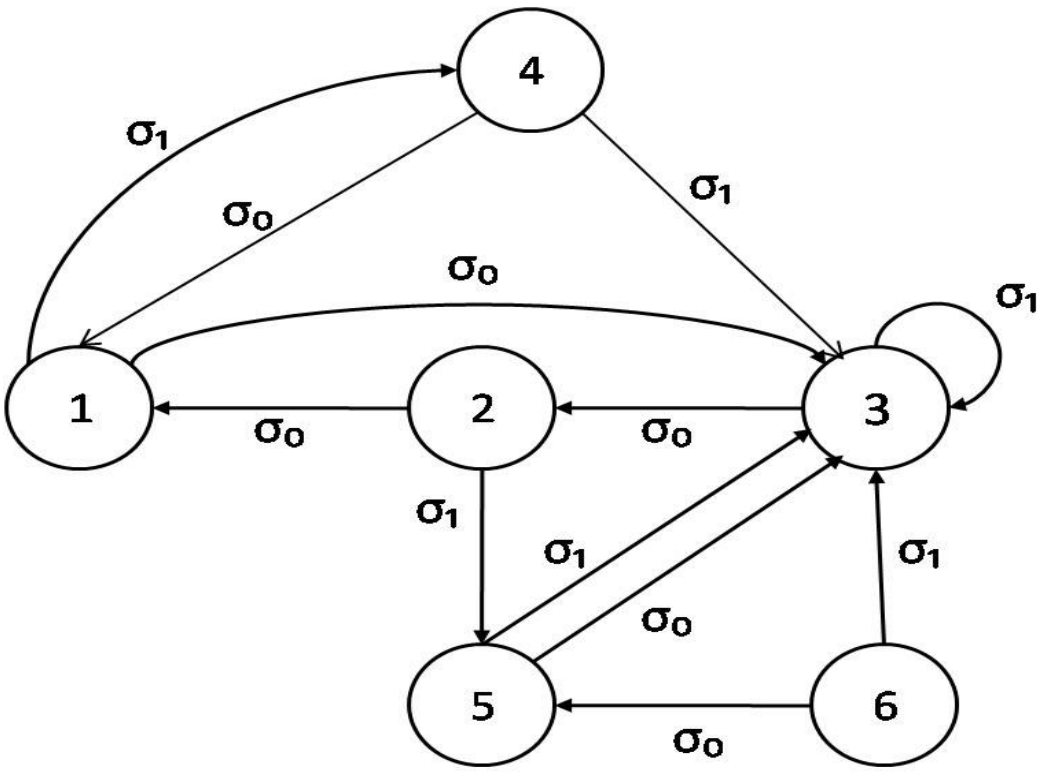


Figure 3.2 the state machine M.

From the table and the diagram we can see that the state machine M is complete.

3.1.3 How the state machine operate

We will present the machine $M = (Q, \Sigma, \delta)$ with a symbol $\sigma \in \Sigma$ while it is in some state, say $q \in Q$. The machine then moves to state $\delta(q, \sigma) \in Q$. This notation is a little cumbersome, so we will introduce another consept.

• Let $\sigma \in \Sigma$, define $\delta_\sigma : Q \to Q$ by $q\delta_\sigma = \delta(q, \sigma)$ for each $q \in Q$

The machine may not be complete, so δ_σ may only be a partial function of Q to itself, so each input $\sigma \in \Sigma$ yieldz a partial function $\delta_\sigma : Q \to Q$.

• Suppose that σ is applied to the machine in the state q then the machine moves to state $q\delta_\sigma$. If further, another input $\sigma' \in \Sigma$ is applied we get the resultant state $q\delta_\sigma\delta_{\sigma'}$.

• Now let $\alpha \in \Sigma^+$ and suppose that $\alpha = \sigma_1\sigma_2.....\sigma_k$ then we define $\delta_\alpha : Q \to Q$ by $q\delta_\alpha = q\delta_{\sigma_1}\delta_{\sigma_2}.....\delta_{\sigma_k}$.

3.2 The semigroup of a state machine

Proposition 3.2.1 *Let $M = (Q, \sum, \delta)$ be a state machine and consider the set Σ^+ of all words of length greater than or equal to 1 in the alphabet Σ . Define a relation $\sim$ on Σ^+ by*

$$\alpha \sim \beta \Leftrightarrow \delta_\alpha = \delta_\beta \quad \textit{where } \alpha, \beta \in \Sigma^+$$

The relation $\sim$ is a congruence on Σ^+, and we can construct the quotient semigroup $\Sigma^+ / \sim$.

We call this semigroup, the semigroup of the state machine M, the notation used being $S(M)$. The elements of $S(M)$ will be equivalence classes $[\alpha]$, $\alpha \in \Sigma^+$.

Proof. *From [3]*

We will prove that $\sim$ is a congruence on Σ^+

The relation $\sim$ is easily seen to be an equivalence relation because of

The reflexivity of $\sim$, that is, $\delta_\alpha = \delta_\alpha$ for any $\alpha \in \Sigma^+$, then $\alpha \sim \alpha$.

The symmetry of $\sim$, that is, $\alpha \sim \beta \Leftrightarrow \delta_\alpha = \delta_\beta$ where $\alpha, \beta \in \Sigma^+$, and we have $\delta_\beta = \delta_\alpha$ then $\beta \sim \alpha$.

The transitivity of $\sim$ *, that is,*

$\alpha \sim \beta \Leftrightarrow \delta_\alpha = \delta_\beta$ *and* $\beta \sim \gamma \Leftrightarrow \delta_\beta = \delta_\gamma$ *where* $\alpha, \beta, \gamma \in \Sigma^+$

And we have $\delta_\alpha = \delta_\beta = \delta_\gamma$ *then* $\alpha \sim \gamma$.

Since Σ^+*has a natural semigroup structure, using concatenation of words as the operation, it is natural to ask whether* $\sim$ *is a congruence on* Σ^+*, then*

If $\alpha, \beta, \gamma \in \Sigma^+$ *and* $\alpha \sim \beta$ *then* $\delta_\alpha = \delta_\beta$ *and for any* $q \in Q$

$q\delta_{\gamma\alpha} = (q\delta_\gamma)\delta_\alpha = (q\delta_\gamma)\delta_\beta = q\delta_{\gamma\beta}$ *and so* $\delta_{\gamma\alpha} = \delta_{\gamma\beta}$ *which yields* $\gamma\alpha \sim \gamma\beta$*, etc .*

We now construct the quotient semigroup $\Sigma^+ / \sim$. ■

3.3 State machine homomorphism

Definition 3.3.1 *Let* $M = (Q, \Sigma, \delta)$ *and* $M' = (Q', \Sigma\ , \delta')$ *be state machines.*

let $\alpha : Q \to Q'$ *;* $\beta : \Sigma \to \Sigma'$*be mappings (functions) such that*

$$\alpha(\delta(q, \sigma)) \subseteq \delta'(\alpha(q), \beta(\sigma)) \text{ for any } q \in Q \ , \ \sigma \in \Sigma,$$

This means that if $\delta(q, \sigma)$ *is undefined we put* $\alpha(\delta(q, \sigma) = \varnothing$ *and if* $\delta(q, \sigma)$ *is defined then* $\delta'(\alpha(q), \beta(\sigma))$ *is also and* $\alpha(\delta(q, \sigma)) = \delta'(\alpha(q), \beta(\sigma))$

We call the pair (α, β) *a state machine homomorphism from* M *to* M' *and write* $(\alpha, \beta) : M \to M'$.

• *If* α *and* β *are both bijective functions, then the pair* (α, β) *is a state machine isomorphism and we write* $M \cong M'$.

Example 3.3.1 *Let $M = (Q, \Sigma, \delta)$ be the state machine defined by the diagram*

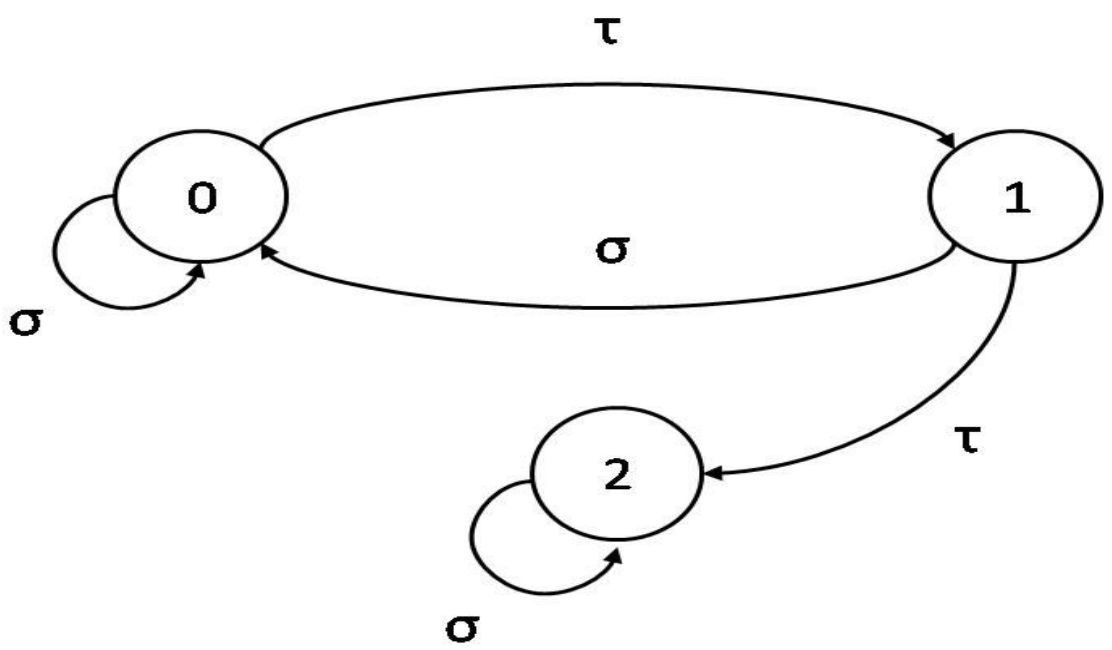


Figure 3.3 The state machine M.

Such that $Q = \{0, 1, 2\}$, $\Sigma = \{\sigma, \tau\}$.
If $M' = (Q', \Sigma', \delta')$ is the state machine defined by the diagram

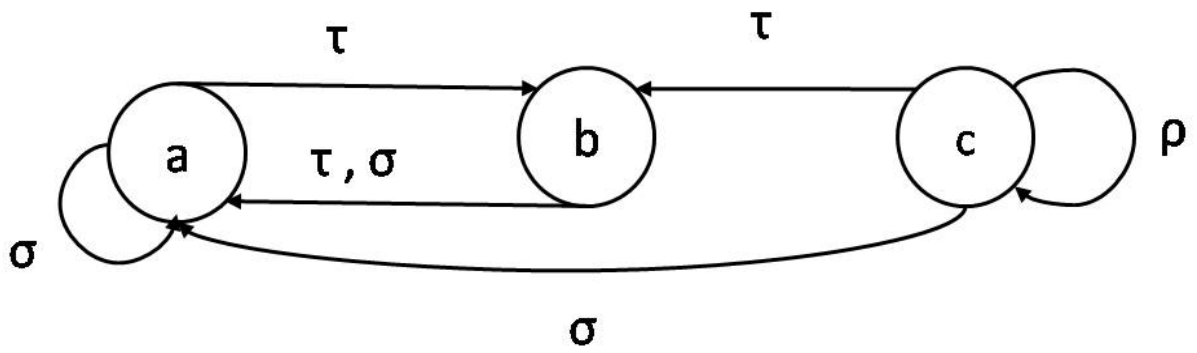


Figure 3.4 The state machine M'.

Where $Q = \{a, b, c\}$, $\Sigma' = \{\sigma, \tau, \rho\}$.

Define

$\alpha : Q \to Q'$ *by* $\alpha(0) = \alpha(2) = a$; $\alpha(1) = b$

$\beta : \Sigma \to \Sigma'$ *by* $\beta(\sigma) = \sigma$; $\beta(\tau) = \tau$

Then $(\alpha, \beta) : M \to M'$ *is a homomorphism; note that*

$\alpha(\delta(2, \tau)) = \varnothing \subseteq \delta'(\alpha(2), \beta(\tau)) = b$

$\alpha(\delta(0, \sigma)) = a = \delta'(\alpha(0), \beta(\sigma))$.

etc.

3.4 Coverings

Definition 3.4.1 *Let* $M = (Q, \Sigma, \delta)$ *and* $M' = (Q', \Sigma', \delta')$ *be state machines. If* $\psi : \Sigma \to \Sigma'$ *is a function and* $\varphi : Q' \to Q$ *is a surjective partial function such that*

$$\delta(\varphi(q'), \alpha) \subseteq \varphi(\delta'(q', \psi(\alpha))) \text{ for } q' \in Q' \text{ and } \alpha \in \Sigma^*$$

We say that (φ, ψ) *is a covering of* M *by* M'*, written* $M \leq M'$.

Remark 3.4.1 *If* M *and* M' *are state machines with the same alphabet* Σ *than*

$$\delta(\varphi(q'), \alpha) \subseteq \varphi(\delta'(q', \alpha)) \text{ for } q' \in Q' \text{ and } \alpha \in \Sigma$$

and we say that φ *is a covering of* M *by* M'.

Example 3.4.1 *Let* M *be a state machine defined by the diagram*

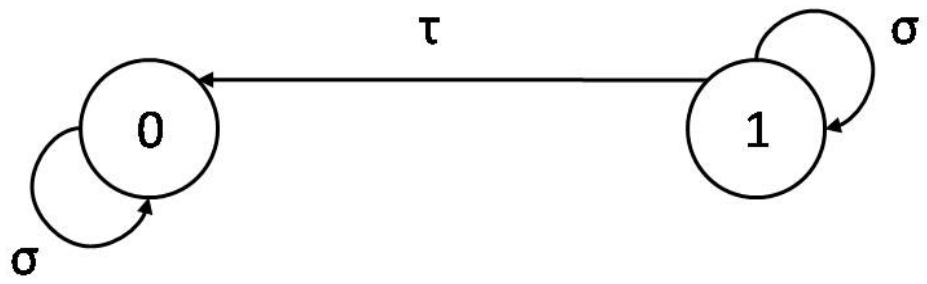


Figure 3.5 The state machine M.

Such that $Q = \{0, 1\}$, $\Sigma = \{\sigma, \tau\}$ *with transition function* δ.

And M' by

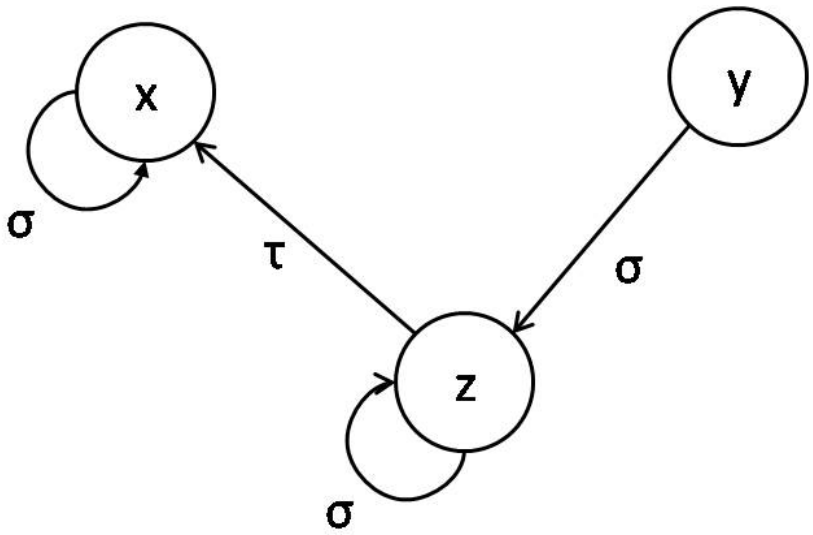


Figure 3.6 The state machine M'.

Such that $Q' = \{x, y, z\}$, $\Sigma' = \{\sigma, \tau\}$ with transition function δ'.
Defining $\varphi : x \to 0$, $y \to 1$ and $1_\Sigma : \sigma \to \sigma$, $\tau \to \tau$ does not yield a covering $(\varphi, 1_\Sigma)$ since $\delta(\varphi(y), \tau) = 0 \nsubseteq \varphi(\delta'(y, \tau)) = \varnothing$.
However by butting a surjective partial function $\varphi' : x \to 0$, $z \to 1$ we may check that $(\varphi', 1_\Sigma)$ gives a covering $M \leq M'$ because
$\delta(\varphi'(x), \sigma) = 0 \subseteq \varphi'(\delta'(x, \sigma)) = 0$
$\delta(\varphi'(z), \sigma) = 1 \subseteq \varphi'(\delta'(z, \sigma)) = 1$
$\delta(\varphi'(x), \tau) = \varnothing \subseteq \varphi'(\delta'(x, \tau)) = \varnothing$
$\delta(\varphi'(z), \tau) = 0 \subseteq \varphi'(\delta'(z, \tau)) = 0.$

3.5 Products of state machines

There are many major methods of connecting up the state machines, so this various products show us how to do this

Let $M = (Q, \Sigma, \delta)$ and $M' = (Q', \Sigma', \delta')$ be state machines.

3.5.1 Direct product

Restricted direct product

Definition 3.5.1 *Suppose that M and M' are state machines with the same input set Σ, that's mean $\Sigma = \Sigma'$. connecting them up in this way, will produce a new state machine*

$$M \wedge M' = (Q \times Q', \Sigma\ , \delta \wedge \delta') \text{ where}$$

$(\delta \wedge \delta')((q, q'), \sigma) = (\delta(q, \sigma), \delta'(q', \sigma))$ *for* $\sigma \in \Sigma$, $(q, q') \in Q \times Q'$
We call this machine the restricted direct product of M and M'.

The (full) direct product

Another type of connection can be made, even when the input alphabets are different.

Definition 3.5.2 *Let M and M' be state machines, and we will define*

$$M \times M' = (Q \times Q', \Sigma \times \Sigma', \delta \times \delta') \text{ where}$$

$(\delta \times \delta')((q, q'), (\sigma, \sigma')) = (\delta(q, \sigma), \delta'(q', \sigma'))$ *for* $\sigma \in \Sigma$, $\sigma' \in \Sigma'$, $(q, q') \in Q \times Q'$
This state machine is called the full direct product of M and M'.

3.5.2 Cascade product

Definition 3.5.3 *Suppose that M and M' are state machines, we will define the cascade product of M and M' with respect to $\omega : Q' \times \Sigma' \to \Sigma$ by*

$$M \omega M' = (Q \times Q', \Sigma', \delta^\omega) \text{ where}$$

$\delta^\omega((q, q'), \sigma') = (\delta(q, \omega(q', \sigma')), \delta'(q', \sigma'))$ *for* $\sigma' \in \Sigma$, $(q, q') \in Q \times Q'$.

3.5.3 Wreath product

Definition 3.5.4 *The wreath product of state machines M and M' is $M \circ M'$ such that*

$$M \circ M' = (Q \times Q', \Sigma^{Q'} \times \Sigma', \delta^\circ)$$

$\delta^\circ((q, q'), (f, \sigma')) = (\delta(q, f(q')), \delta'(q', \sigma'))$ *for* $\sigma' \in \Sigma$, $f \in \Sigma^{Q'}, (q, q') \in Q \times Q'$.

Remark 3.5.1 *The wreath product (cascade product) of more than two state machines,* $M_1 \circ M_2 \circ M_3 \circ ..... \circ M_n$ *is defined as* $(...(M_1 \circ M_2) \circ M_3 \circ ....) \circ M_n$.

Example 3.5.1 *Let* M *be state machine given by*

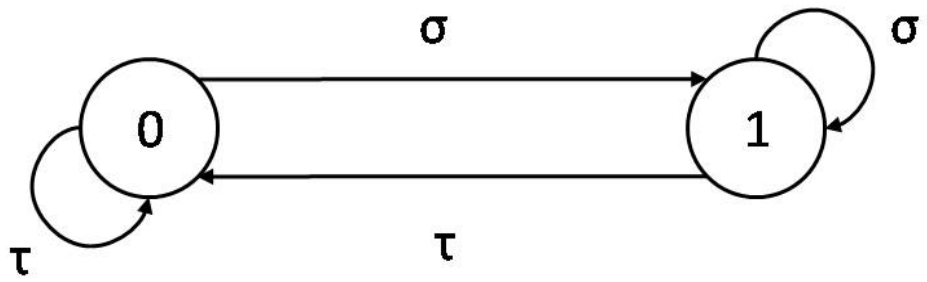


Figure 3.7 The state machine M.

Where $Q = \{0, 1\}, \Sigma = \{\sigma, \tau\}$.
And M' *given by*

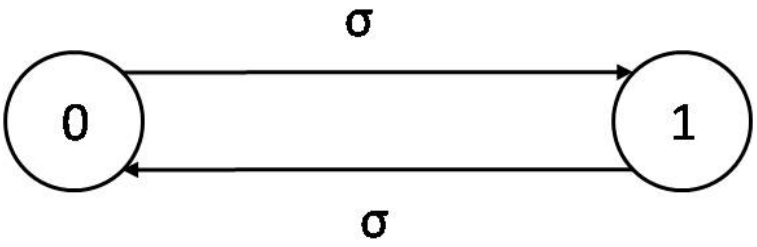


Figure 3.8 The state machine M'.

Where $Q' = Q = \{0, 1\}, \Sigma' = \{\sigma\}$.
Define a mapping $\omega : Q' \times \Sigma' \to \Sigma$ *by* $\omega(0, \sigma) = \sigma$, $\omega(1, \sigma) = \tau$.

Now we will define the cascade product $M\omega M'$ which has diagram

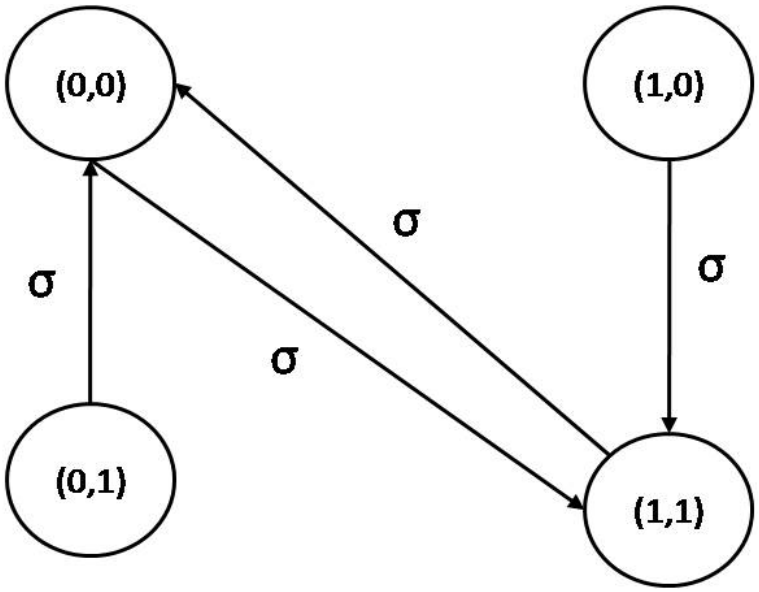


Figure 3.9 The cascade product of M and M'.

such that $M\omega M' = (Q \times Q', \Sigma', \delta^{\omega})$ where

$\delta^{\omega}((0,0),\sigma) = (\delta(0,\omega(0,\sigma)),\delta'(0,\sigma)) = (1,1)$

$\delta^{\omega}((0,1),\sigma) = (\delta(0,\omega(1,\sigma)),\delta'(1,\sigma)) = (0,0)$

$\delta^{\omega}((1,0),\sigma) = (\delta(1,\omega(0,\sigma)),\delta'(0,\sigma)) = (1,1)$

$\delta^{\omega}((1,1),\sigma) = (\delta(1,\omega(1,\sigma)),\delta'(1,\sigma)) = (0,0).$

Finaly we examine the wreath product of M and M', such that the input alphabet is $\Sigma^{Q'} \times \Sigma'$. Denote the four elements of $\Sigma^{Q'}$ by $\alpha, \beta, \gamma, \eta$ where

$\alpha(0) = \alpha(1) = \sigma$; $\beta(0) = \sigma$, $\beta(1) = \tau$

$\gamma(0) = \tau$, $\gamma(1) = \sigma$; $\eta(0) = \eta(1) = \tau$,

then the state machine $M \circ M'$ has the table

δ°	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
(α,σ)	$(1,1)$	$(1,0)$	$(1,1)$	$(1,0)$
(β,σ)	$(1,1)$	$(0,0)$	$(1,1)$	$(0,0)$
(γ,σ)	$(0,1)$	$(1,0)$	$(0,1)$	$(1,0)$
(η,σ)	$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$

Table 3.3 the transition table of $M \circ M'$.

3.6 Decomposition

Definition 3.6.1 *Let $M = (Q, \Sigma, \delta)$ be a state machine. A cascade decomposition for M is a covering*

$$M \leq N_1\omega_1 N_2\omega_2 ....\omega_{n-1}N_n$$

Where $N_1, N_2, ..., N_n$ are state machines, such that this machines are simpler than M; usualy this means that the state sets of $N_1, N_2, ..., N_n$ are all "smaller" than the state set of M, the connecting mapping $\omega_1, \omega_2, ..., \omega_{n-1}$ are defined suitably (a cascade or restricted direct product).

Remark 3.6.1 *Recall that the cascade product is a generalization of the restricted direct product so that this type of decomposition will be the most general. however if we can replace some of the cascade products by restricted direct products we will do so because this will yield a much more effecient covering. (The semigroup of the covering machine will be smaller).*

3.7 Permutation-reset machines

An important class of state machines are permutaion-reset state machines, before we start this section, we will give some definition.

Definition 3.7.1 *A reset state machine $M = (Q, \Sigma, \delta)$ is a state machine in which input $\sigma \in \Sigma$ either defines an identity on Q or $|(Q)\delta_\sigma| = 1$.*

Definition 3.7.2 *A permutation state machine $\bar{M} = (\bar{Q}, \bar{\Sigma}, \bar{\delta})$ is a state machine in which input gives a permutation of $\bar{Q}$, that is, $(\bar{Q})\bar{\delta}_{\bar{\sigma}} = \bar{Q}$ for all $\bar{\sigma} \in \bar{\Sigma}$.*

3.7.1 Permutation-reset machine

Definition 3.7.3 *Let $M = (Q, \Sigma, \delta)$ be a state machine with $|Q| > 1$ and suppose that for each $\sigma \in \Sigma$ either $(Q)\delta_\sigma = Q$ or $|(Q)\delta_\sigma| = 1$, then we call M a permutation-reset machine. (each input defines a permutation of Q or a reset).*

Now we will examine a method of decomposing them.

Theorem 3.7.1 *Let M be a permutation-reset machine then*

$$M \leq N \dot{\omega} P$$

Where N is a reset machine and P is a permutation machine.

Proof. *From [3]*

- *Let $M = (Q, \Sigma, \delta)$, and Σ can be devided into two disjoint subsets*

$$\Sigma = \Theta \cup \Xi \qquad \Theta \cap \Xi = \varnothing$$

Where Θ is the set of all permutation inputs of M, and Ξ is the set of all reset inputs of M, that is,

$$\Theta = \{\sigma \in \Sigma \mid (Q)\delta_\sigma = Q\}$$

And

$$\Xi = \{\sigma \in \Sigma \mid |(Q)\delta_\sigma| = 1\}.$$

- *Define G to be the subgroup of $S(M)$ generated by Θ, then the elements of G are equivalence classes, $[\alpha]$.*

And put $P = (G, \Sigma, \bar{\delta})$ where

$$\begin{aligned} [\alpha]\,\bar{\delta}_\theta &= \bar{\delta}([\alpha], \theta) = [\alpha\theta] \quad , \theta \in \Theta, \alpha \in \Theta^* \\ [\alpha]\,\bar{\delta}_\xi &= \bar{\delta}([\alpha], \xi) = [\alpha] \quad , \xi \in \Xi, \alpha \in \Theta^* \end{aligned}$$

We have $\alpha\theta \in \Theta^*$ and $[\alpha\theta] \in G$ then P is a permutation machine.

- *Let $N = (Q, G \times \Sigma, \delta^*)$ where*

$$\delta^*(q, (g, \xi)) = \delta^{-1}(\delta(\delta(q, \alpha), \xi), \alpha)$$

such that $g = [\alpha] \in G$, $\alpha \in \Theta^*, \xi \in \Xi$, $q \in Q$

With notation

$q\delta^*_{(g,\xi)} = q\delta_\alpha\delta_\xi(\delta_\alpha)^{-1}$

Now δ_α is a permutation of Q , as $\alpha \in \Theta^*$, and so $(\delta_\alpha)^{-1}$ is defined.

Furthermore $\left|(Q)\delta^*_{(g,\xi)}\right| = |(Q)\delta_\alpha\delta_\xi(\delta_\alpha)^{-1}| = 1$

Because $(Q)\delta_\alpha = Q \qquad (\alpha \in \Theta^*)$

$|(Q)\delta_\xi| = 1 \qquad (\xi \in \Xi)$

And thus N *is a reset machine.*

• *The state machine* $N^{\cdot}$ *consists of the state machine* N *with the identity map* 1_Q *adjoined, we thus adjoin a new symbol* Λ *to the set* $G \times \Sigma$ *and*

$$N^{\cdot} = (Q, (G \times \Sigma) \cup \{\Lambda\}, \delta^{**}) \text{ where}$$

$q\delta^{**}_{(g,\xi)} = q\delta^*_{(g,\xi)}$ *for* $q \in Q$, $g \in G$, $\xi \in \Xi$

And

$q\delta^{**}_\Lambda = q \qquad$ *for* $q \in G$.

• *Now define* $\omega : G \times \Sigma \to G \times \Sigma \cup \{\Lambda\}$ *by*

$$\omega(g,\sigma) = \begin{cases} \Lambda & \text{if } \sigma \in \Theta \\ (g,\sigma) & \text{if } \sigma \in \Xi \end{cases}$$

We may form the cascade product $N^{\cdot}\omega P$*; the state mapping of this machine will be denoted by* δ^ω

Then $N^{\cdot}\omega P = (Q \times G, \Sigma, \delta^\omega)$ *where*

$$\delta^\omega((q,g),\sigma) = (\delta^{**}(q,\omega(g,\sigma)), \bar{\delta}(g,\sigma))$$

With notation

$(q,g)\delta^\omega_\sigma = (q\delta^{**}_{\omega(g,\sigma)}, g\bar{\delta}_\sigma)$ *for* $q \in Q$, $g \in [\alpha] \in G$, $\alpha \in \Theta^*, \sigma \in \Sigma$.

• *The covering map* $\varphi : Q \times G \to Q$ *between* M *and* $N^{\cdot}\omega P$ *is defined by*

$$\varphi(q,g) = q\delta_\alpha = \delta(q,\alpha) \qquad (*)$$

where $g = [\alpha] \in G$, $q \in Q$.

We must now establish the covering properties for φ

First φ *is clearly surjective as* $G \neq \varnothing$ *and* δ_α *is a permutation of* Q, $(\alpha \in \Theta^*)$

Now we will verify the last condition of covering

$$\delta(\varphi(q,g),\sigma) \subseteq \varphi(\delta^\omega((q,g),\sigma)).$$

Then we will examine the cases of $\sigma \in \Sigma$

Let $\sigma \in \Theta$ *and* $(q, g) \in Q \times G$. *If* $g = [\alpha]$ *where* $\alpha \in \Theta^*$, *then*

$$\begin{aligned}\delta(\varphi(q,[\alpha]),\sigma) &= \delta(\delta(q,\alpha),\sigma)\\ &= \delta(q,\alpha\sigma)\\ &= \varphi(q,[\alpha\sigma]), \quad \textit{from } (*)\end{aligned}$$

Since $\alpha\sigma \in \Theta^*$. *Hence*

$$\begin{aligned}\varphi(\delta^{\omega}((q,[\alpha]),\sigma)) &= \varphi(\delta^{**}(q,\omega([\alpha],\sigma)),\bar{\delta}([\alpha],\sigma))\\ &= \varphi(\delta^{**}(q,\Lambda),\bar{\delta}([\alpha],\sigma)),\ \textit{as } \sigma \in \Theta\\ &= \varphi(q,[\alpha\sigma]),\ \textit{as } \sigma \in \Theta\end{aligned}$$

Then

$\delta(\varphi(q, g), \sigma) = \varphi(\delta^{\omega}((q, g), \sigma))$.

If $\sigma \in \Xi$ *and* $(q, g) \in Q \times G$ *with* $g = [\alpha]$ *for* $\alpha \in \Theta^*$

Then

$$\begin{aligned}\delta(\varphi(q,[\alpha]),\sigma) &= \delta(\delta(q,\alpha),\sigma)\\ &= \delta(q,\sigma).\end{aligned}$$

Also

$$\begin{aligned}\varphi(\delta^{\omega}((q,[\alpha]),\sigma)) &= \varphi(\delta^{**}(q,\omega([\alpha],\sigma)),\bar{\delta}([\alpha],\sigma))\\ &= \varphi(\delta^{**}(q,([\alpha],\sigma)),\bar{\delta}([\alpha],\sigma)),\quad \textit{as } \sigma \in \Xi\\ &= \varphi(\delta^{*}(q,([\alpha],\sigma)),[\alpha]),\qquad \textit{as } \sigma \in \Xi\\ &= \varphi(\delta^{-1}(\delta(\delta(q,\alpha),\sigma),\alpha),[\alpha])\\ &= \delta(\delta^{-1}(\delta(\delta(q,\alpha),\sigma),\alpha),\alpha),\quad \textit{from } (*)\\ &= \delta(\delta(q,\alpha),\sigma)\\ &= \delta(q,\sigma).\end{aligned}$$

Then $\delta(\varphi(q, g), \sigma) = \varphi(\delta^{\omega}((q, g), \sigma))$.

Hence in all cases

$\delta(\varphi(q, g), \sigma) \subseteq \varphi(\delta^{\omega}((q, g), \sigma))$.

Then $M \leq N \cdot \omega P$. ■

Example 3.7.1 *Consider the state machine* $M = (Q, \Sigma, \delta)$ *defined by*

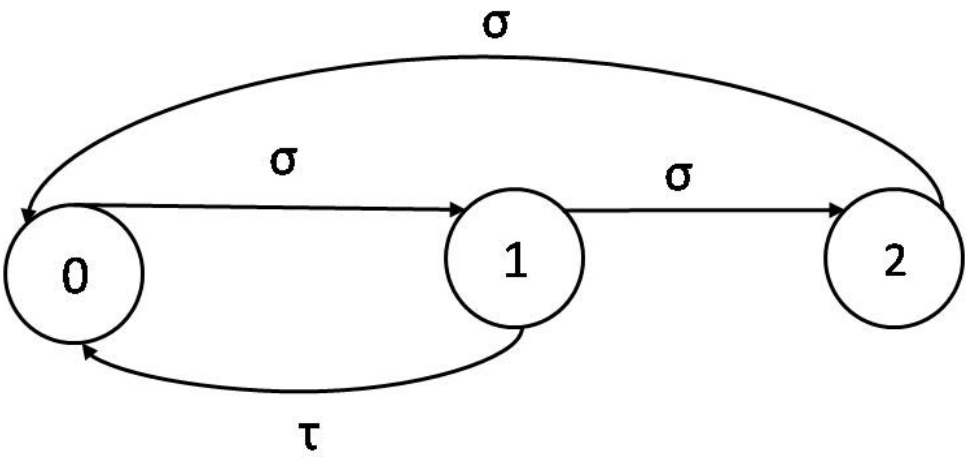


Figure 3.10 The state machine M.

where $Q = \{0, 1, 2\}$, $\Sigma = \{\sigma, \tau\}$,

This machine is a permutation-reset machine such that the permutation machine $P = (\mathbb{Z}_3, \Sigma, \bar{\delta})$ *is given by*

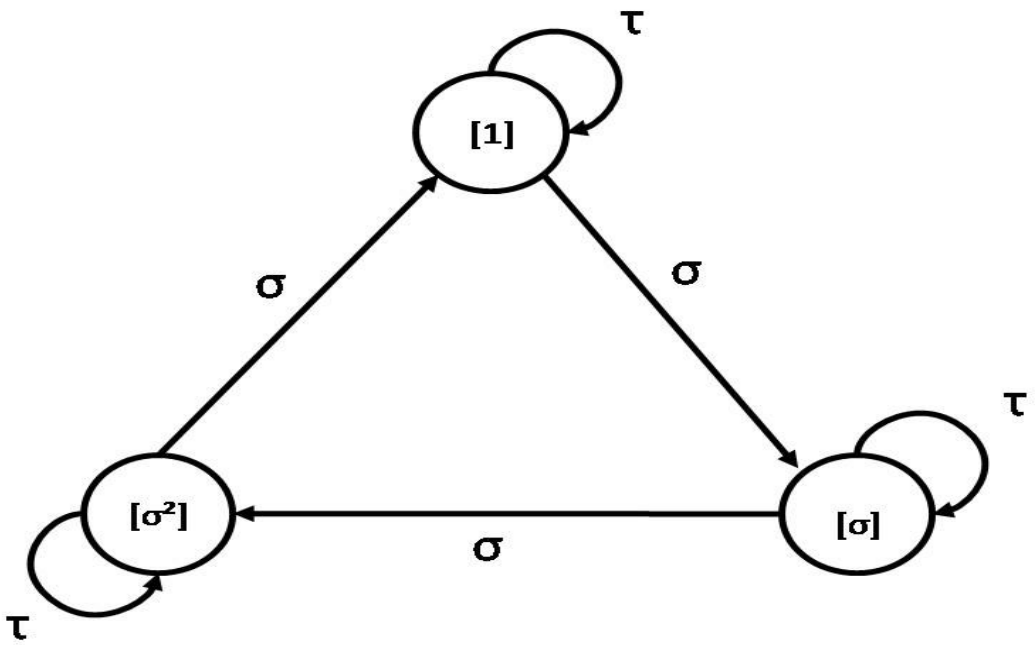


Figure 3.11 The permutation machine P.

Where $\mathbb{Z}_3 = \{[1], [\sigma], [\sigma^2]\}$.

$N^{\cdot} = (Q, (\mathbb{Z}_3 \times \Sigma) \cup \{\Lambda\}, \delta^{**})$ *is a reset machine given by the table*

δ^{**}	0	1	2
Λ	0	1	2
$([1], \sigma)$	$\varnothing$	$\varnothing$	$\varnothing$
$([1], \tau)$	$\varnothing$	0	$\varnothing$
$([\sigma], \sigma)$	$\varnothing$	$\varnothing$	$\varnothing$
$([\sigma], \tau)$	$\varnothing$	2	$\varnothing$
$([\sigma^2], \sigma)$	$\varnothing$	$\varnothing$	$\varnothing$
$([\sigma^2], \tau)$	$\varnothing$	1	$\varnothing$

Table 3.4 The trasition table of $N^{\cdot}$.

Conclusion

In this project, we presented a way to produce more semigroups and groups from an initial semigroups and groups using semidirect product and wreath product. We know that the problem of decomposing a state machine was studied quite thoroughly and various methods were proposed in order to improve its effeciency, so in this project we have seen a method of decomposing a general state machine into "algebraically simpler" machines doing the same work as the original state machine by choosing a suitable ways like cascade product or restricted direct product of state machines.

The subject discussed here is undergoing much rapid development and it is likely that over the next few years many new useful results will appear.

Bibliography

[1] **L.Chrystopher Nehaniv, Attila Egri-Nagy** (2013). Cascade Product of Permutation Groups. Search Report. Centre for computer science & informatics, U.K and Centre for research in mathematics, Australia.

[2] **A.Ginzburg,** Algebraic Theory of Automata, Academic Press, New York, London, 1968.

[3] **W.M.L.Holcomb,** Algebraic Automata Theory, Cambridge University Press, New York, 1982.

[4] **J.A.Holdener** (2001), Subgroups Generated by Subsets, Lecture Notes, Department of Mathematics, Kenyon College, Gambier.

[5] **A.A.Ibrahim, M.S.Audu** (2007). On Wreath Product of Permutation Groups. Search Report. USMANU Danfodiyo University, Sokoto-Negeria, University of JOS, JOS-Negeria.

[6] **K.Conrad** (2014). Homomorphisms. Lecture Notes. University of Washington-Tacoma Campus.

[7] **O.Maler, A.Pnueli** (1994). On The Cascade Decomposition of Automata, Its Complexity and Its Application to Logic. inpuplished manuscript.

[8] **T.HAJRO** (1996). Semigroups. Lecture Notes. Department of Mathematics University of Turku, Turku, Finlind.

[9] **W.J.Gilbert, W.K.Nichlson.** Modern Algebra With Applications, Second Edition. Jhon Wiley & Sons, Inc, Hoboken, Newjersey, Canada, 2004.


تم بحمد الله