NOTAS DE MATEMATICAS
N° 152

TEORIA DE AUTOMATA

POR

LUZ E. SOLE

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS
DEPARTAMENTO DE MATEMATICA
MERIDA-VENEZUELA
1994

Teoría de Autómata

Mérida, Diciembre 1994

Las notas presentes corresponden a una redacción realizada por el Lic. Guelvis E. Mata D. del curso, de postgrado de Matemáticas, Teoría de Autómata, dictado por la prof. Luz E. Solé. Estas constituyen los fundamentos básicos para el desarrollo del Proyecto de Investigación SISTEMAS DE EVENTOS DISCRETOS MODELADOS POR REDES DE PETRI ESTOCASTICAS.

Contenido

Introducción

La teoría de Autómatas fue originalmente propuesta para modelar Redes Neuronales. Sin embargo, ésta teoría tomó fuerza con el tiempo, hasta el punto que hoy día es usada para modelar una clase de Sistemas llamados Sistemas de Eventos Discretos.

Tanto la teoría de Autómatas como la teoría del Lenguaje Formal son cuerpos de Investigación que se han venido desarrollando durante los últimos 45 años. Ambos tópicos están estrechamente relacionados y constituyen partes distintas de lo que actualmente se conoce como Ciencia de la Computación.

El objetivo más importante dentro de estas notas será determinar las conexiones más estrictas en cuanto a la estructura misma de los Autómatas Finitos y la teoría del Lenguaje Formal, junto con el estudio de estructuras matemáticas que pueden ser descritas o reconocidas por dispositivos de estado finito. Se usará el término racional para éstas estructuras, el cual queda justificado por la conexión con los números racionales.

La organización de éstas notas es dada de la manera siguiente: El capítulo 0 constituye los fundamentos para desarrollar los capítulos posteriores. Este incluye algunos conceptos de la teoría de grafos y algunos conceptos algebraicos. En el capítulo 1 se introducirán las nociones de Autómata finito, en sus diferentes formas, y las expresiones Regulares, dando la equivalencia entre éstas. Esta equivalencia constituye el primer gran resultado en estas notas. En el capítulo 2 se introducirán las propiedades de los conjuntos regulares (o expresiones regulares), algoritmos de decisión para estos y la minimización de Autómatas Finitos. En el capítulo 3 se estudiaran dos tipos de Máquinas Secuenciales (máquinas de Moore y Mealy), y las nociones de Código y Precódigo. Luego en el capítulo 4 los Autómatas Finitos son llamados a permitir entradas infinitas.

Concluimos en el capítulo 5 con la generalización de los Autómatas Finitos, y se desarrollará un método algebraico que consiste en el estudio de las ecuaciones lineales, para describir el comportamiento de un A.F dado. Este es el Segundo gran resultado en estas notas.

Capítulo 0

Preliminares Algebraicos

En éste capítulo introducimos algunas nociones de la teoría de grafos y algunos conceptos y resultados algebraicos, los cuales nos proveerán de una herramienta básica para formalizar los conceptos dados en los capítulos posteriores.

0.1 Grafos, Relaciones y Estructuras.

Definición 0.1.1 *Un grafo G, es un par $G := (V, E)$, donde V es un conjunto finito no vacío y E es una colección finita de pares no ordenados de $V \times V$ que pueden repetirse. Los elementos de V y E serán llamados respectivamente vértices (o nodos) y aristas (o líneas).*

Un grafo G puede ser representado gráficamente identificando los elementos de V con círculos y los elementos de E con líneas.

Ejemplo 0.1.1 *Consideremos el grafo $G := (V, E)$, donde $V = \{u, v, w, z\}$ y $E = \{(u, v), (v, v), (v, v), (v, w), (v, w), (u, w), (u, w), (w, z)\}$, entonces gráficamente tenemos su representación en la figura* 0.1

Ejemplo 0.1.2 *Consideremos el grafo $G := (V, E)$, donde $V = \{1, 2, 3, 4, 5\}$ y $E = \{(1, 3), (3, 4), (2, 5)\}$, es decir,*

$$E = \{(n, m) \in V \times V : n + m = 4 \ \text{ó} \ n + m = 7\}.$$

La representación gráfica de G es dada en la figura 0.2

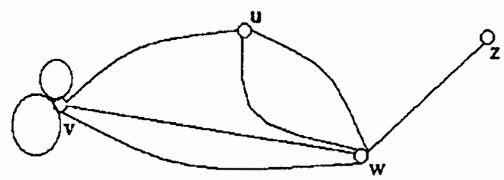

Figura 0.1:

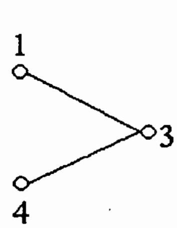

Figura 0.2:

Definición 0.1.2 *Un grafo dirigido D es un par $D := (V, E)$, donde V es como en la definición 0.1.1. y E es una colección finita de pares ordenados de $V \times V$. que pueden repetirse. Los elementos de E serán llamados arcos. Un arco $(u, v) \in E$ es llamado un arco de u a v y lo denotamos por $u \longrightarrow v$.*

Un grafo dirigido D puede ser representado gráficamente identificando los elementos de V con círculos y los arcos con líneas dirigidas.

Ejemplo 0.1.3 *Consideremos el grafo dirigido $D := (V, E)$ donde $V = \{P, Q, R, S, T\}$ y*

$$E = \{(P, Q), (Q, R), (R, S), (P, S), (P, T), (Q, T), (S, T), (Q, S), (S, Q)\}.$$

Entonces la representación gráfica de D está dada por la figura 0.3.

Definición 0.1.3 *Dos grafos G_1, G_2 son isomorfos si existe una aplicación inyectiva entre los vértices de G_1 y los de G_2, con la propiedad que el número de aristas uniendo dos vértices de G_1 sea igual al número de aristas uniendo los correspondientes vértices de G_2.*

Definición 0.1.4 *Sean $G_1 := (V_1, E_1)$ y $G_2 := (V_2, E_2)$ dos grafos tales que $V_1 \cap V_2 = \emptyset$. Entonces:*

- *(i) La unión de los grafos G_1 y G_2, denotada por $G_1 \cup G_2$, es el grafo $G_1 \cup G_2 = (V_1 \cup V_2, E_1 \cup E_2)$.*
- *(ii) La suma de los grafos G_1 y G_2, denotada por $G_1 + G_2$, es el grafo $G_1 + G_2 := (V_1 \cup V_2, E \cup H)$, donde $E = E_1 \cup E_2$ y $H = \{(n, m) : n \in V_1,\ m \in V_2\}$.*

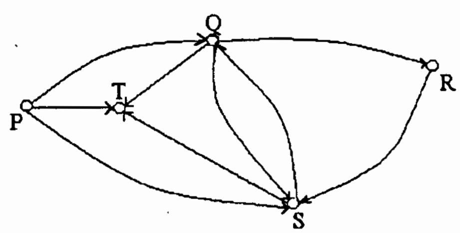

Figura 0.3:

Ejemplo 0.1.4 *Si G_1 y G_2 son los grafos cuyas representaciones gráficas son dadas en la figura 0.4 ,4(a) y 4(b) respectivamente. Entonces a $G_1 \cup G_2$ le corresponde la representación gráfica dada en la figura 0.5 y, a $G_1 + G_2$ le corresponde la representación gráfica dada en la figura 0.6*

Observación 1. Las operaciones de unión y suma de grafos son conmutativas y asociativas, y estas pueden ser extendidas a cualquier número finito de grafos.

Definición 0.1.5 *Un grafo G es llamado conexo si no existen grafos G_1 y G_2 tales que $G = G_1 \cup G_2$. En caso contrario diremos que G es disconexo.*

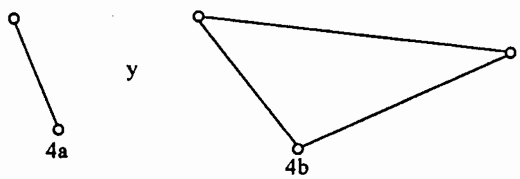

Figura 0.4:

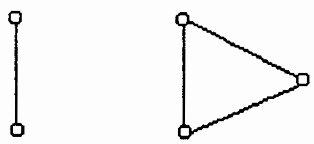

Figura 0.5:

Ejemplo 0.1.5 *Si G es un grafo cuya representación gráfica es dada por la figura* 0.5*, entonces G es disconexo.*

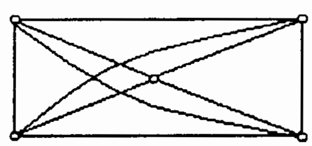

Figura 0.6:

Ejemplo 0.1.6 *Si G es un grafo cuya representación gráfica es dada por la figura* 0.6*, entonces G es conexo.*

Definición 0.1.6 *Sea G un grafo. Una sucesión de aristas en G es una sucesión finita de aristas de la forma $(V_0, V_1), (V_1, V_2), \ldots, (V_{m-1}, V_m)$ la cuál denotamos por $V_0 \rightarrow V_1 \rightarrow \ldots \rightarrow V_m$.*

Una sucesión de aristas determina una sucesión finita de vértices $V_0, V_1, \ldots, V_m$. LLamaremos a V_0 vértice inicial y a V_m vértice final de la sucesión de aristas, y diremos que la sucesión de aristas vá desde V_0 hasta V_m.

Definición 0.1.7 *Sea G un grafo y sea $(V_0, V_1), (V_1, V_2), \ldots, (V_{m-1}, V_m)$ una sucesión de aristas en G. La longitud de la sucesión de aristas es el número de aristas que determinan dicha sucesión.*

Definición 0.1.8 *Dado un grafo G. Una sucesión de aristas (V_0, V_1), $(V_1, V_2), \ldots, (V_{m-1}, V_m)$ es llamada una trayectoria en G, si todas las aristas son distintas. Además, si $V_i \neq V_{i+1}$, para todo $1 \leq i \leq m$ (excepto posiblemente $V_0 = V_m$), entonces la trayectoria será llamada una cadena en G.*

Ejemplo 0.1.7 *Sea G el grafo cuya representación gráfica es dada en la figura* 0.7,

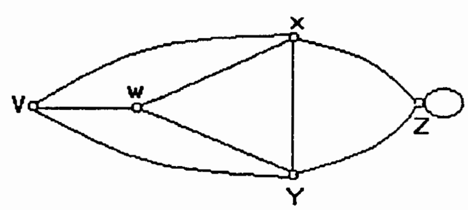

Figura 0.7:

entonces $V \to W \to X \to Y \to Z \to Z \to X$ es una trayectoria en G y $V \to W \to X \to Y \to Z$ es una cadena en G.

Definición 0.1.9 *Dado un grafo G. Una trayectoria $(V_0, V_1), (V_1, V_2), \ldots, (V_{m-1}, V_m)$ en G es llamada cerrada sí $V_0 = V_m$.*

Ejemplo 0.1.8 *En el ejemplo 0.1.7 la trayectoria $V \to W \to X \to Y \to Z \to X \to V$ es una trayectoria cerrada.*

Definición 0.1.10 *Un grafo infinito G es un par (V, E), donde V es un conjunto infinito cuyos elementos son llamados Vértices, y E es una colección infinita de pares no ordenados cuyos elementos son llamadas aristas. Si V y E son infinitos numerables, entonces G es llamado un grafo numerable.*

Definición 0.1.11 *Un árbol es un grafo dirigido que tiene las propiedades siguientes:*

- *(i) Existe un vértice, llamado raíz, que no tiene predecesor y del cuál hay una trayectoria a cada vértice.*
- *(ii) Cada vértice distinto de la raíz tiene exactamente un predecesor.*
- *(iii) Los sucesores de cada vértice son ordenados de izquierda a derecha.*

Definición 0.1.12 *Sean X e Y dos conjuntos no vacíos y consideremos sus conjuntos potencias, denotados 2^X y 2^Y respectivamente. Una relación f de X en Y, que denotamos por $f : X \to Y$, es una aplicación $f : 2^X \to 2^Y$ tal que*

$$f\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} f(A_i), \quad \text{donde } \{A_i : \ i \in I\}$$

es una familia arbitraria de elementos de 2^X.

Definición 0.1.13 *El grafo de una relación $f : X \to Y$, denotado $graf\,(f)$, es el subconjunto del producto $X \times Y$ dado por*

$$graf\,(f) := \{(x, y) \in X \times Y : \ y = f(x)\}.$$

Definición 0.1.14 *Sea $f : X \to Y$ una relación. El grafo de la relación inversa, denotada $f^{-1} : Y \to X$, es dado por*

$$graf\,(f^{-1}) := \{(y, x) \in Y \times X : \ y = f(x)\}.$$

Definición 0.1.15 *El dominio de una relación $f : X \to Y$, denotado por $Dom(f)$, es dado por $Dom(f) := \{x \in X \ : \ f(x) \neq \emptyset\}$*

Definición 0.1.16 *Una relación $f : X \to Y$ es llamada una función (o aplicación) si el conjunto $\{f(x), \ x \in X\}$ es unitario.*

Definición 0.1.17 *Una relación $R : X \to X$ es una relación de orden parcial si:*

- *(i) Para todo $x \in X$, $x\,R\,x$, es decir R es reflexiva.*
- *(ii) Para todo $x, y \in X$, $x\,R\,y \wedge y\,R\,x \Longrightarrow x = y$,es decir, R es antisimétrica.*
- *(iii) Para todo $x, y, z \in X$, $x\,R\,y \wedge y\,R\,z \Longrightarrow x\,R\,z$, es decir, R es transitiva.*

Definición 0.1.18 *Una relación $R : X \to X$ es llamada una relación de equivalencia si:*

- *(i) Para todo $x \in X$, $x\,R\,x$.*
- *(ii) Para todo $x_1, x_2 \in X$, $x_1\,R\,x_2 \Longrightarrow x_2\,R\,x_1$, es decir, R es simétrica.*
- *(iii) Para todo $x_1, x_2, x_3 \in X$, $x_1\,R\,x_2 \wedge x_2\,R\,x_3 \Longrightarrow x_1\,R\,x_3$.*

La relación de equivalencia R es llamada invariante a derecha si $x\,R\,y$ implica que $x \cdot z\,R\,y \cdot z$, para todo z en X, donde $\cdot$ es una operación binaria en X.

A continuación introducimos algunas definiciones y resultados algebraicos, bien conocidos, que son de mucha importancia y que se encuentran en cualquier libro de álgebra abstracta.

Dado un conjunto no vacío X y una relación de equivalencia R sobre X. Definimos el conjunto cociente de X, denotado por X/R, cuyos elementos son las clases de equivalencias dadas por: $\overline{x} = \{x' \in X \ : \ x'R\,x\}$. Además,

$$X = \bigcup_{x \in X} \bar{x} \quad \text{y} \quad \bar{x}_1 = \bar{x}_2 \Longleftrightarrow x_1\,R\,x_2,$$

llamaremos a X/R el cociente de X módulo R.

Podemos definir también el epimomorfismo canónico, $\varphi : X \to X/R$ por $\varphi(x) = \bar{x}$. Ahora bien, si $f : X \to Y$ es una función, entonces los subconjuntos no vacíos de X de la forma $f^{-1}(\{y\}) = \{x \in X : f(x) = y\}$ inducen una relación de equivalencia en X, la cual llamaremos Kernel de f (o núcleo de f); tal relación es denotada por $Ker(f)$ y es definida como sigue: para todo $x, x' \in X$, $x\,Ker(f)\,x'$ ó $x\,R\,x'\,(mod\,Ker(f)) \Longleftrightarrow f(x) = f(x')$.

Finalmente, una aplicación $f : X \to Y$ induce una aplicación inyectiva única, $\bar{f} : X/Ker(f) \to Y$ definida por $\bar{f}(\bar{x}) = f(x)$ tal que el diagrama siguiente conmuta,

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & Y \\
& X/\ker f \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Figura 0.8:

es decir, $\bar{f}(\varphi(x)) = f(x)$.

Definición 0.1.19 *Sea S un conjunto no vacío y sea $\cdot : S \times S \to S$ una operación binaria en S. Diremos que el par $(S, \cdot)$ es un semigrupo si $\cdot$ es asociativa.*

Definición 0.1.20 *Sea S un conjunto no vacío y sea $\cdot : S \times S \to S$ una operación binaria en S. Diremos que el par $(S, \cdot)$ es un monoide si:*

- (i) *$\cdot$ es asociativa.*
- (ii) *existe $e \in S$ tal que $e \cdot s = s \cdot e = s$, para todo $s \in S$.*

  Es decir, $(S, \cdot)$ es un monoide si $(S, \cdot)$ es un semigrupo y se cumple (ii).

Definición 0.1.21 *Sean $(S_1, \cdot)$ y $(S_2, *)$ dos semigrupos (respectivamente monoides). Un Homomorfismo de los semigrupos $(S_1, \cdot)$ y $(S_2, *)$ (respectivamente monoides) es una aplicación $\phi : (S_1, \cdot) \to (S_2, *)$ tal que $\phi(x \cdot y) = \phi(x) * \phi(y)$, para todo $x, y \in S_1$.*

Observación 2. La composición de dos homomorfismos es también un homomorfismo.

Definición 0.1.22 *Sea $(S, \cdot)$ un monoide. Un submonoide de $(S, \cdot)$ es un subconjunto T de S que contiene a e (identidad en S), junto con la operación inducida de $(S, \cdot)$.*

De la definición 0.1.22 se sigue que si S es un monoide y $A \subseteq S$, entonces el subconjunto $A^* = \{e\} \cup A \cup A^2 \cup \ldots \cup A^n \cup \ldots$ es un submonoide de S, donde $A^{n+1} = A^n \cdot A, \;\; n \geq 0, \;\; A^0 = \{e\}$.

Sea Σ un conjunto cualquiera y consideremos el conjunto de todas las combinaciones finitas, formadas con elementos de Σ, el cuál denotamos por Σ^*. En Σ^* consideramos una operación $\cdot$ llamada concatenación como sigue: si $u = a_1 a_2 \ldots a_n$ y $v = b_1 b_2 \ldots b_m$ estan en Σ^*, entonces $u \cdot v = (a_1 a_2 \ldots a_n) \cdot (b_1 b_2 \ldots b_m) = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m$. La concatenación le da a Σ^* estructura de monoide poniendo $e = \theta$ (la combinación que no tiene símbolos). La longitud de $s \in \Sigma^*$, denotada por $|s|$, es el número de símbolos que aparecen en s. Claramente si $s, t \in \Sigma^*$, entonces $|s \cdot t| = |s| + |t|$; en consecuencia $|\theta| = 0$.

Todo subconjunto $L \subseteq \Sigma^*$ será llamado un lenguaje sobre Σ, y cada elemento de Σ^* será llamado palabra.

Definición 0.1.23 *Sea Σ un conjunto finito, (el cual llamaremos alfabeto), y sea $L \subseteq \Sigma^*$. La llamada clausura de Kleene de L es la unión infinita*

$$L := \bigcup_{n=0}^{\infty} L^n, \;\; donde \;\; L^n = L^{n-1}L, \; n \geq 1 \;\; y \;\; L^0 = \{e\}.$$

En Σ^* definimos una relación de orden parcial, llamada prefijo y denotada $\underline{\alpha}$, como sigue: para $u, v \in \Sigma^*$, $u \,\underline{\alpha}\, v$ si existe $w \in \Sigma^*$ tal que $v = u \cdot w$. En este caso diremos que u es prefijo de v.

Capítulo 1

Autómatas finitos y expresiones regulares

En este capítulo estudiaremos los Autómatas finitos y demostraremos la equivalencia entre éstos y las llamadas expresiones regulares. Un Autómata finito es un modelo matemático de un sistema, con entradas y salidas discretas. El sistema puede ser visto como un número finito de estados, los cuales resumen la información concerniente a las entradas pasadas que son necesarias para determinar el comportamiento del sistema en subsiguientes entradas.

1.1 Autómata finito determinista.

Un Autómata finito determinista (A.F.D.) consiste de un conjunto finito de estados y un conjunto de transiciones de estado a estado que ocurren en símbolos de entradas, escogidos de un alfabeto finito. Por cada símbolo de entrada existe exáctamente una transición a otro estado (posiblemente la transición sea al mismo estado). Un estado, usualmente denotado q_o, es el estado inicial en el cual el Autómata comienza. Algunos estados son designados como finales. Formalmente tenemos la definición siguiente.

Definición 1.1.1 *Un autómata finito determinista (A.F.D.) es un quíntuple* $(Q, \sum, \delta, q_o, F)$*, donde* Q *es un conjunto finito cuyos elementos serán llamados estados,* $\sum$ *es un alfabeto cuyos elementos serán llamados entradas,*

$q_o \in Q$ y $F \subseteq Q$ serán llamados respectivamente estado inicial y conjunto de estados finales y δ es una función parcial que asigna a cada elemento de $Q \times \sum$ un elemento de Q (posiblemente ninguno, es decir, δ no es definida) y la cual será llamada función de transición.

Dibujamos un A.F.D. como un control finito, el cual en algún estado de Q lee una sucesión de símbolos de $\sum$ y la escribe en una cinta.

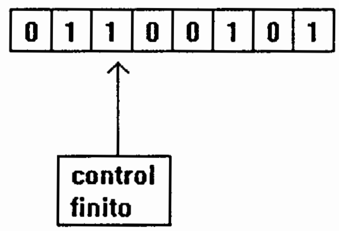

Figura 1.1:

En un movimiento el A.F.D., en el estado q, explora un símbolo a, entra al estado $\delta(q, a)$ y mueve su cabeza un símbolo a la derecha. Si $\delta(q, a)$ es un estado aceptado, entonces el A.F.D. es llamado a aceptar la palabra escrita en la cinta de entrada, pero no incluyendo la posición en la cual la cabeza se ha movido. Si la cabeza se ha movido a la derecha totalmente (final de la cinta), entonces el A.F.D. acepta la cinta completa.

Para definir el comportamiento de un A.F.D. en elementos de $\sum^*$ es necesario extender la función parcial δ como una función parcial $\hat{\delta} : Q \times \sum^* \to Q$. Definimos $\hat{\delta}$ como sigue:

- (i) $\hat{\delta}(q, \theta) = q$, para todo $q \in Q$.
- (ii) $\hat{\delta}(q, wa) = \delta(\hat{\delta}(q, w), a)$, para todo $w \in \sum^*$, para todo $a \in \sum$ y para todo $q \in Q$.

$\hat{\delta}$ así definida es efectivamente una extensión de δ. En efecto, si $a \in \sum$, entonces $\hat{\delta}(q, \theta a) = \delta(\hat{\delta}(q, \theta), a) = \delta(q, a)$, para todo $q \in Q$.

(i) Dice que no hay cambio de estado por la entrada θ y (ii) dice que para determinar el estado $\hat{\delta}(q, wa)$, hay que hallar previamente el estado $\hat{\delta}(q, w) = p$ y luego el estado $\delta(p, a)$.

Como $\hat{\delta}$ es una extensión de δ en lo que sigue no haremos distinción entre éstas, siempre y cuando ambas sean definidas.

Definición 1.1.2 *Una palabra $x \in \sum^*$ se llamará aceptado por un A.F.D. $M :\doteq (Q, \sum, \delta, q_o, F)$ dado, si $\delta(q_o, x) \in F$. El conjunto de todas las palabras aceptadas por M es entonces*

$$Lac(M) := \{x \in \textstyle\sum^* : \delta(q_o, x) \in F\}.$$

Definición 1.1.3 *Un subconjunto L de $\sum^*$ será llamado conjunto regular (o lenguaje regular) si L es aceptado por algún A.F.D. M, es decir, $L = Lac(M)$.*

Ejemplo 1.1.1 *Consideremos el A.F.D. $M := (Q, \sum, \delta, q_o, F)$, donde $Q = \{q_o, q_1, q_2, q_3\}$, $\sum = \{0, 1\}$, $F = \{q_o\}$ y δ es dada por la tabla 1.*

	Entradas	
Estados	0	1
q_o	q_2	q_1
q_1	q_3	q_o
q_2	q_o	q_3
q_3	q_1	q_2

Tabla 1.

La palabra 110101 *está en $Lac(M)$.*

En efecto, como $\delta(q_o, 1) = q_1$ y $\delta(q_1, 1) = q_o$, entonces $\delta(q_o, 11) = \delta(\delta(q_o, 1), 1) = \delta(q_1, 1) = q_o$, es decir $11 \in Lac(M)$. Ahora, $\delta(q_o, 110) = \delta(\delta(q_o, 11), 0) = \delta(q_o, 0) = q_2$. Por tanto,
$\delta(q_o, 1101) = \delta(\delta(q_o, 110), 1) = \delta(q_2, 1) = q_3$; así
$\delta(q_o, 11010) = \delta(\delta(q_o, 1101), 0) = \delta(q_3, 0) = q_1$. Finalmente,
$\delta(q_o, 110101) = \delta(\delta(q_o, 11010), 1) = \delta(q_1, 1) = q_o$, es decir, $110101 \in Lac(M)$.

Cuando digamos que un lenguaje regular $K \subseteq \sum^*$ es dado, significa que existe un A.F.D. M tal que $Lac(M) = K$.

Denotaremos por $L(M)$ al conjunto $\{x \in \sum^* : \delta(q_o, x) \text{ esta definida}\}$. Claramente $Lac(M) \subseteq L(M)$.

Definición 1.1.4 *Sea $L \subseteq \sum^*$. LLamaremos la clausura de L al conjunto denotado por $\bar{L}$ y dado por*

> $\bar{L} := \{x \in \sum^* :$ *existe* $t \in \sum^*, \;\; xt \in L\}$, *es decir, $\bar{L}$ es el conjunto de todas las palabras que son prefijos de los elementos de L*

Claramente, si $L = \emptyset$, entonces $\bar{L} = \emptyset$; y si $L \neq \emptyset$, entonces $\theta \in L$. Además $L \subseteq \bar{L}$.

Definición 1.1.5 *Diremos que un lenguaje L es cerrado si $L = \bar{L}$.*

De la definición 1.1.5 se sigue que si M es un A.F.D., entonces $L(M) = \overline{L(M)}$, es decir, $L(M)$ es cerrado.

Un grafo dirigido, llamado diagrama de transición, es asociado con un A.F.D. como sigue: Los vértices del grafo corresponden a los estados del A.F.D. . Si existe una transición del estado q al estado p por la entrada a, entonces existe un arco etiquetado a del estado q al estado p en el diagrama de transición.

Ejemplo 1.1.2 *Consideremos el A.F.D. $M := (Q, \sum, \delta, q_o, F)$, donde $Q = \{q_o, q\}$, $\sum = \{\alpha, \beta, r\}$, $F = \{q_o\}$ y δ es dada en al tabla 2.*

Entradas

Estados	α	β	r
q_o	q_1	$\emptyset$	$\emptyset$
q_1	$\emptyset$	q_o	q_1

Tabla 2.

El símbolo $\emptyset$ es usado en éste ejemplo para representar la no definición de δ

El grafo dirigido o diagrama de transición asociado al A.F.D. M es dado en la figura 1.2

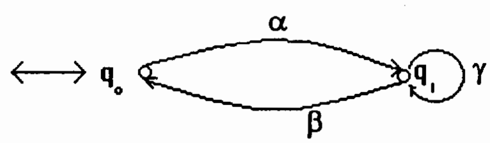

Figura 1.2:

Note que la palabra $\alpha r\beta \in Lac(M)$. En efecto, $\delta(q_o, \alpha) = q_1$; así $\delta(q_o, \alpha r) = \delta(\delta(q_o, \alpha), r) = \delta(q_1, r) = q_1$, de donde $\delta(q_o, \alpha r\beta) = \delta(q_1, \beta) = q_o$, luego $\alpha r\beta \in Lac(M)$. También se puede probar que $Lac(M) = (\alpha r^* \beta)^*$.

Una trayectoria c en un A.F.D. M es una sucesión finita $c := (q_o, r_1, q_1), (q_1, r_2, q_2), \ldots, (q_{k-1}, r_k, q_k)$ de arcos consecutivos. Podemos también usar la notación

$$q_o \xrightarrow{r_1} q_1 \xrightarrow{r_2} q_2 \xrightarrow{r_3} \cdots \xrightarrow{r_k} q_k$$

La trayectoria nula (o trivial) comienza en q y finaliza en q.
Una trayectoria c que comienza en q_o y termina en $q \in F$ es llamada una trayectoria suceso. Por tanto, $Lac(M) = \{c \;/\; c$ es una trayectoria suceso en $M\}$ = comportamiento de M.

Podemos también representar un A.F.D. M con una matriz, llamada matriz de transición. Esta es una matriz cuadrada finita Δ con columnas y filas indizadas por el conjunto de estados Q de M y con entradas $\Delta(p, q)$, donde $\Delta(p, q) = \{a \in \sum : \; \delta(p, a) = q\}$.

Ejemplo 1.1.3 *Consideremos el A.F.D. M cuyo diagrama de transición asociado es dado en la figura* 1.3.

La matriz de transición correspondiente al A.F.D. M es entonces el arreglo rectangular

$$\Delta = \begin{pmatrix} \emptyset & \{a_1\} & \emptyset & \emptyset & \{a_2\} \\ \emptyset & \emptyset & \{\beta\} & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \{\beta\} & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & \emptyset \\ \emptyset & \emptyset & \emptyset & \emptyset & \{\beta\} \end{pmatrix}$$

Introducimos las operaciones entre Autómatas finitos deterministas.
El Autómata finito determinista (A.F.D.) vacío sobre un alfabeto $\sum$, *denotado* $\emptyset_{\sum}$, *es dado por* $\emptyset_{\sum} := (\emptyset, \sum, \emptyset, \emptyset, \emptyset)$. *Claramente* $L(\emptyset_{\sum}) = \emptyset$.

Para la trayectoria trivial el A.F.D. tiene exactamente un estado, es decir, $Q = \{q\}$. *Luego,*

$$Lac(M) = \{r \in \sum^{*} \ / \ \delta(q_o, r) \in F\} = \{\theta\} = L(M).$$

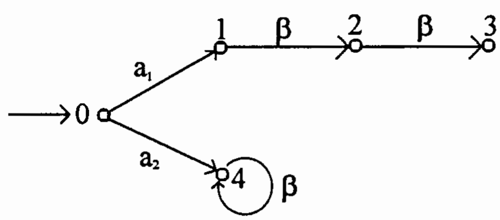

Figura 1.3:

Observación 1.1 *Dado un A.F.D.* $M = (Q, \sum, \delta, q_o, F)$, *podemos extenderlo a un A.F.D* M' *sobre* $\sum'$, *con* $\sum \subseteq \sum'$ *como* $M' = (Q, \sum', \delta', q_o, F)$, *donde* $\delta' : Q \times \sum' \longrightarrow Q$, *es definida por*

$$\delta'(q, r) = \begin{cases} \delta(q, r) & , si \ \ r \in \sum \\ q & , si \ \ r \in \sum' \setminus \sum \end{cases}$$

Ahora, podemos dar las dos definiciones siguientes.

Definición 1.1.6 *Dados dos A.F.D's.* $M_1 = (Q_1, \sum, \delta_1, q_1, F_1)$ *y* $M_2 = (Q_2, \sum, \delta_2, q_2, F_2)$ *tales que* $Q_1 \cap Q_2 = \emptyset$. *La unión de los Autómatas* M_1 *y* M_2, *denotada* $M_1 \cup M_2$, *es el A.F.D. dado por* $M_1 \cup M_2 := (Q, \sum, \delta, q_o, F)$, *donde* $Q = Q_1 \cup Q_2$, $F = F_1 \cup F_2$ *y* $\delta : Q \times \sum \longrightarrow Q$ *es definida por*

$$\delta(q, r) = \begin{cases} \delta_1(q, r), & si \ \ q \in Q_1 \\ \delta_2(q, r), & si \ \ q \in Q_2 \end{cases}$$

De la definición 1.1.6 se sigue que cada trayectoria en $M_1 \cup M_2$ es una trayectoria en M_1 o es una trayectoria en M_2, es decir,

$$L(M_1 \cup M_2) = L(M_1) \cup L(M_2).$$

Definición 1.1.7 *Dados dos A.F.D's* $M_1 = (Q_1, \sum, \delta_1, q_1, F_1)$ *y* $M_2 = (Q_2, \sum, \delta_2, q_2, F_2)$ *tales que* $Q_1 \cap Q_2 = \emptyset$. *La intersección (o producto) de los Autómatas* M_1 *y* M_2, *denotada por* $M_1 \cap M_2$ *o* $(M_1 \times M_2)$, *es el A.F.D. dado por* $M_1 \cap M_2 = (Q, \sum, \delta, q_o, F)$, *donde* $Q = Q_1 \times Q_2$, $q_o = (q_1, q_2)$, $F = F_1 \times F_2$ *y* $\delta : Q \times \sum \longrightarrow Q$ *es definida por* $\delta((p, q), r) = (\delta_1(p, r), \delta_2(q, r))$, *siempre que* $\delta_1(p, r)$ *y* $\delta_2(q, r)$ *estén definidas (en otro caso* δ *no está definida).*

Claramente $L(M_1 \cap M_2) = L(M_1) \cap L(M_2)$, puesto que cada trayectoria $(p', q') \xrightarrow{c} (p'', q'')$ en $M_1 \cap M_2$ puede ser vista como un par $c = (c', c'')$ de trayectorias $p' \xrightarrow{c'} q'$ en M_1 y $p'' \xrightarrow{c''} q''$ en M_2 tales que $|c| = |c'| = |c''|$.

Definición 1.1.8 *Diremos que un A.F.D.* M *es accesible si todo estado de* Q *es alcanzable desde* q_o, *es decir, para cada* $q \in Q$ *existe* $r \in \sum^*$ *tal que* $\delta(q_o, r) = q$.

Si un A.F.D. M no es accesible podemos sin embargo considerar el conjunto de todos los estados accesibles desde q_o, es decir, $Qac := \{q \in Q /$ existe $r \in \sum^*, \ \delta(q_o, r) = q\}$ y poner $Qac_F := Qac \cap F$; de manera que si definimos $\delta ac := \delta / Qac \times \sum$, entonces encontramos un A.F.D. que llamaremos la componente accesible de M, denotado por $Ac(M)$ y definido por

$$Ac(M) := (Qac, \sum, \delta ac, q_o, Qac_F).$$

Note que un A.F.D. M es accesible, si y sólo si, $M = Ac(M)$, es decir, $Q = Qac$.

Definición 1.1.9 *Un A.F.D. M será llamado co-accesible si cada palabra en $L(M)$ puede completarse a un palabra en $Lac(M)$, es decir, $r \in L(M)$ implica que existe $\beta \in \sum^*$ tal que $r\beta \in Lac(M)$.*

Definición 1.1.10 *Diremos que un A.F.D. M es trim, si M es accesible y co-accesible.*

Observación 1.2 *Si $Q = Qco$, donde $Qco := \{q \in Q :$ existe $r \in \sum^*$, $\delta(q,r) \in F\}$, entonces M es co-accesible. Además, si M es trim, entonces $L(M) = Lac(M)$.*

Supongamos que M es un A.F.D. que no es trim, entonces si ponemos $Qtr := Qac \cap Qco$ y $\delta tr := \delta / Qtr \times \sum$ podemos definir un nuevo A.F.D. inducido por M, que denotaremos por $Tr(M)$, como sigue

$$Tr(M) = \begin{cases} (Qtr, \sum, \delta tr, q_o, F \cap Qtr) & ,\text{si} \quad Qtr \neq \emptyset \\ \\ \emptyset_{\sum} & ,\text{si} \quad Qtr = \emptyset \end{cases}$$

Definición 1.1.11 *Dados dos A.F.D's $M_1 = (Q_1, \sum, \delta_1, q_1, F_1)$ y $M_2 = (Q_2, \sum, \delta_2, q_2, F_2)$ trim's tales que $L(M_2) \subseteq L(M_1)$. Diremos que M_2 refina M_1, si para todo $r, \beta \in L(M_2)$ tales que $\delta_2(q_2, r) = \delta_2(q_2, \beta)$, se tiene que $\delta_1(q_1, r) = \delta_1(q_1, \beta)$.*

A continuación probaremos que existe una correspondencia biunívoca entre los A.F.D's y las relaciones de equivalencias sobre $\sum^*$, invariantes a derecha y de índices finitos.

A cada lenguaje $L \subseteq \sum^*$ le asociamos una relación de equivalencia, sobre $\sum^*$, que denotaremos por R_L, vía la equivalencia de NERODE, es decir, para $x, y \in \sum^*$, xR_Ly, si y sólo si, para todo $z \in \sum^*$, $xz \in L \Longleftrightarrow yz \in L$.

Denotaremos por $\|L\|$ al cardinal del conjunto

$$\textstyle\sum^* / R_L \quad (\|L\| := card(\sum^* / R_L)).$$

Por ejemplo, si $L = \emptyset$ o $L = \sum^*$, entonces $\|L\| = 1$.

Definición 1.1.12 *Sean π y ρ dos relaciones de equivalencia sobre $\sum^*$. Diremos que π refina ρ y lo denotamos por $\pi\underline{\alpha}\rho$, si para todo $s, t \in \sum^*$, $s \sim t(mod(\pi))$, implica que $s \sim t(mod(\rho))$.*

Claramente, si $\pi\underline{\alpha}\rho$, entonces $\|\rho\| \leq \|\pi\|$.

Ejemplo 1.1.4 *Sea $\{\ell_\alpha : \alpha \in A\}$ una familia arbitraria no vacía de relaciones de equivalencia sobre $\sum^*$.*
Sea $\ell .= \sup\{\ell_\alpha : \alpha \in A\}$ definida como sigue: $S \equiv S' (mod\ell)$ si existe un entero $k \geq 1$, elementos $\alpha_0, \alpha_1, \ldots, \alpha_k \in A$ y palabras $S_1 \ldots S_k \in \sum^*$ tales que:

$$
\begin{aligned}
&S \equiv S_1 \,(mod\ell_{\alpha_0})\\
&S_1 \equiv S_2 \,(mod\ell_{\alpha_1})\\
&\vdots\\
&S_{k-1} \equiv S_k \,(mod\ell_{\alpha_{k-1}})\\
&S_k \equiv S' \,(mod\ell_{\alpha_k})
\end{aligned}
$$

Si las ℓ_α son relaciones de equivalencia invariantes a derecha, entonces ℓ también lo es.
ℓ es la más fina relación de equivalencia sobre $\sum^*$ que es menos fina que cada ℓ_α, $\alpha \in A$, es decir, $\ell_\alpha\underline{\alpha}\ell$, para todo $\alpha \in A$.

Si $M = (Q, \sum, \delta, q_o, F)$ es un A.F.D., entonces definimos una relación de equivalencia sobre $\sum^*$ inducida por M y denotada por R_M como sigue: para $x, y \in \sum^*$, $xR_My \Longleftrightarrow \delta(q_o, x) = \delta(q_o, y)$.
Si $\delta(q_o, x)$ es indefinida, entonces $\delta(q_o, x)=\delta(q_o, y)$ es también indefinida. Además, es fácil verificar que R_M es invariante a derecha y de índice finito, puesto que cada clase de equivalencia corresponde a algún estado alcanzable desde q_o.

Recíprocamente, si π es una relación de equivalencia invariante a derecha sobre $\sum^*$ de índice finito, entonces π Induce un A.F.D. $M = (Q, \sum, \delta, q_o, F)$, donde $Q = (\bar{r} : r \in \sum^*)$ es el conjunto cuyos elementos son las clases de equivalencia por la relación π,

$$q_o = \bar{\theta}, \quad \delta : Q \times \sum \longrightarrow Q,$$

es definida por $\delta(\bar{r}, a) = \overline{ra}$ y F es escogido arbitrariamente. Claramente $R_M = \pi$.

1.2 Autómata Finito no Determinista

El concepto de No Determinista juega un papel importante en la teoría de computación y la teoría de lenguaje.
Parece natural pensar que cualquier conjunto aceptado por un Autómata finito no determinista (A.F.N.), puede también ser aceptado por un A.F.D., sin embargo existen autómatas cuyas versiones determinísticas son conocidas pero no son equivalentes, y otros autómatas para los cuales la equivalencia es un problema abierto importante y profundo.
Modificamos el A.F.D. de manera que permita ninguna, una o mas transiciones de un estado en el mismo símbolo de entrada. Este módelo es llamado un Autómata Finito no Determinista. Formalmente tenemos la siguiente definición.

Definición 1.2.1 *Un Autómata finito no determinista (A.F.N) es un quíntuple* $(Q, \sum, \delta, q_o, F)$, *donde* $Q, \sum, q_o$ *y* F *son como en el A.F.D., pero* δ *toma valores en* 2^Q $(\delta : Q \times \sum \longrightarrow 2^Q)$, *es decir,* $\delta(q, a)$ *es el conjunto de todos los estados* p, *tales que existe una transición de* q *a* p *etiquetada* a.

Como en los A.F.D.'s. extenderemos a δ como $\hat{\delta} : Q \times \sum^* \longrightarrow 2^Q$, y la definimos como sigue:

- (i) $\hat{\delta}(q, \theta) = \{q\}$, para todo $q \in Q$.
- (ii) $\hat{\delta}(q, \omega a) = \{p \in Q$: existe $r \in \hat{\delta}(q, \omega)$ y $p \in \delta(r, a)\}$, con $\omega \in \sum^*$, $a \in \sum$.

Como $\hat{\delta}(q, \theta a) = \delta(q, a)$, con $a \in \sum$, lo cual nos dice efectivamente que $\hat{\delta}$ es una extensión de δ, entonces usaremos δ en vez de $\hat{\delta}$ en lo que sigue.
Ahora, extenderemos la función δ, a argumentos en $2^Q \times \sum^*$. Acá $\delta : 2^Q \times \sum^* \longrightarrow 2^Q$ es definida por

$$\delta(P, \omega) = \bigcup_{q \in P} \delta(q, \omega), \quad \text{para cada } P \subseteq Q.$$

Definición 1.2.2 *LLamaremos al conjunto* $\{\omega \in \sum^* \ / \ \delta(q_o, \omega)$ *contiene un estado de* $F\}$*, el lenguaje aceptado por un A.F.N* M*, y lo denotaremos por* $Lac(M)$.

Ejemplo 1.2.1 *Consideremos el A.F.N* $M = (Q, \sum, \delta.q_o, F)$*, donde* $Q = \{q_o, q_1, q_2, q_3, q_4\}$, $\sum = \{0,1\}$, $F = \{q_2, q_4\}$ *y* δ *es dada por la figura* 1.4.

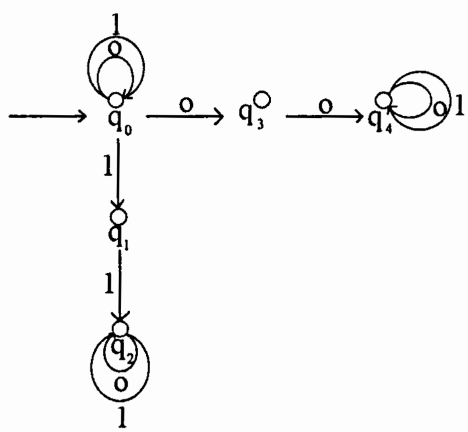

Figura 1.4:

Veamos que la palabra 01001 $\in Lac(M)$. *En efecto, como* $\delta(q_o, 0) = \{q_o, q_3\}$, *entonces* $\delta(q_o, 01) = \delta(\delta(q_o, 0), 1) = \delta(\{q_o, q_3\}, 1) = \delta(q_o, 1) \cup \delta(q_3, 1) = \{q_o, q_1\}$. *Luego,* $\delta(q_o, 010) = \delta(\{q_o, q_1\}, 0) = \delta(q_o, 0) \cup \delta(q_1, 0) = \{q_o, q_3\}$. *Luego,* $\delta(q_o, 0100) = \delta(q_o, 0) \cup \delta(q_3, 0) = \{q_o, q_3, q_4\}$, *finalmente,* $\delta(q_o, 01001) = \delta(\delta(q_o, 0100), 1) = \delta(\{q_o, q_3, q_4\}, 1) = \delta(q_o, 1) \cup \delta(q_3, 1) \cup \delta(q_4, 1) = \{q_o, q_4\}$. *Así* 01001 $\in Lac(M)$:

A continuación introducimos la equivalencia entre los Autómatas finitos deterministas y no deterministas.
Obviamente todo A.F.D es un A.F.N. El teorema siguiente completa la equivalencia entre ambos Autómatas.

Teorema 1.2.1 *Sea* L *el lenguaje aceptado por un A.F.N, entonces existe un A.F.D que acepta* L.

Prueba. Sea $M = (Q, \sum, \delta.q_o, F)$ un A.F.N aceptando L. Construyamos entonces un A.F.D que acepta a L. Para esto, pongamos $Q' = 2^Q$, F' = conjunto de todos los estados en Q' conteniendo un estado final de M.
Denotemos cada elemento de Q' por $[q_1, q_2, \ldots, q_i]$, con $q_1, q_2, \ldots, q_i \in Q$; pongamos ahora $q'_o = [q_o]$ y definamos $\delta' : Q' \times \sum \longrightarrow Q'$ por $\delta'([q_1, q_2, \ldots, q_i], a) = [p_1, p_2, \ldots, p_j]$, si y sólo si, $\delta(\{q_1, q_2, \ldots, q_i\}, a) = \{p_1, p_2, \ldots, p_j\}$.
Afirmación: $\delta'(q'_o, x) = [q_1, q_2, \ldots, q_i]$, si y sólo si, $\delta(q_o, x) = \{q_1, q_2, \ldots, q_i\}$.
En efecto, por inducción sobre la longitud de x, tenemos que si $|x| = 0$, entonces $x = \theta$ y se tiene el resultado deseado. Supongamos que la afirmación es cierta para x tal que $|x| = n$ y sea $r = xa$, donde $a \in \sum$, de acá que $|r| = n + 1$; ahora bien, como $\delta'(q'_o, xa) = \delta'(\delta'(q'_o, x), a)$ y por la hipótesis de inducción $\delta'(q'_o, x) = [p_1, p_2, \ldots, p_j]$, si y sólo si, $\delta(q_o, x) = \{p_1, p_2, \ldots, p_j\}$, se sigue que $\delta'([p_1, p_2, \ldots, p_j], a) = [r_1, r_2, \ldots, r_k]$, si y sólo si, $\delta'(\{p_1, p_2, \ldots, p_j\}, a) = \{r_1, r_2, \ldots, r_k\}$, de donde $\delta'(q'_o, xa) = [r_1, r_2, \ldots, r_k]$, si y sólo si, $\delta(q_o, xa) = \{r_1, r_2, \ldots, r_k\}$. Esto prueba la afirmación. Así se sigue que $\delta'(q'_o, x) \in F'$, si y sólo si, $\delta(q_o, x)$ contiene un estado de F. Luego, $Lac(M) = Lac(M')$.
En conclusión, todo A.F.D. es equivalente a un A.F.N., de manera que usaremos, en lo que sigue, indistintamente los A.F.D's. y los A.F.N's. y hablaremos simplemente de Autómatas finitos (A.F's.).

□

Ejemplo 1.2.2 *Sea $M = (\{q_o, q_1\}, \{0, 1\}, \delta, q_o, \{q_1\})$ un A.F.N., donde δ es definida en la tabla 3.*

Entradas

Estados	0	1
q_o	$\{q_o, q_1\}$	$\{q_1\}$
q_1	$\emptyset$	$\{q_o, q_1\}$

Tabla 3.

Construyamos un A.F.D. $M' = (Q, \{0, 1\}, \delta', [q_o], F)$ que acepte a $Lac(M)$ tal como en el teorema 1.2.1.

$Q = \{[q_o],[q_1],[q_o,q_1],\emptyset\}$. *Como* $\delta(q_o,0) = \{q_o,q_1\}$, *entonces* $\delta'([q_o],0) = [q_o,q_1]$, $\delta'([q_o],1) = [q_1]$, $\delta'([q_1],0) = \emptyset$ *y* $\delta'([q_1],1) = [q_o,q_1]$; *además* $\delta'(\emptyset,0) = \delta'(\emptyset,1) = \emptyset$. $\delta'([q_o,q_1],0) = [q_o,q_1]$, *ya que* $\delta(\{q_o,q_1\},0) = \delta(q_o,0)\cup \delta(q_1,0) = \{q_o,q_1\} \cup \emptyset$ *y* $\delta'([q_o,q_1],1) = [q_o,q_1]$. *Luego,* $F' = \{[q_o],[q_o,q_1]\}$.

1.3 Autómatas Finitos con θ-Movimientos

Nuestro interés se centra ahora en extender los A.F.N. a Autómatas finitos que tiènen movimiento o cambio de estado en la entrada θ.

Definición 1.3.1 *Un Autómata finito no determinista con θ-movimientos es un quíntuple $(Q,\sum,\delta,q_o,F)$, donde $Q,\sum,q_o$ y F son como en los A.F.N's., pero Dom$(\delta) \subseteq Q\times(\sum\cup\{\theta\})$ y δ toma valores en 2^Q ($\delta : Q\times\sum\cup\{\theta\}\longrightarrow 2^Q$), es decir, $\delta(q,a)$ es el conjunto de todos los estados p tales que existe una transición de q a p, etiquetada a. Ésta etiqueta puede ser cualquier símbolo en $\sum$ ó θ.*

Extendemos δ a $\hat{\delta} : Q \times \sum^* \longrightarrow 2^Q$. Esperamos que $\hat{\delta}(q,w)$ sea el conjunto de todos los estados p tales que se pueda ir de q a p a lo largo de una trayectoria etiquetada w, quizás incluyendo arcos etiquetados θ. Para esto es importante conocer el conjunto de estados accesibles a un estado dado q, usando solamente θ-transiciones. Esto es equivalente a la pregunta: ¿Qué vértices pueden ser alcanzados de un vértice dado en un grafo dirigido?. El vértice para el estado q en el diagrama de transición y el grafo dirigido consiste de todos los arcos etiquetados θ. Usaremos la llamada θ-clausura de q, y la denotamos por θ-Clau(q), como el conjunto de todos los vértices p tales que existe una trayectoria de q a p etiquetada θ.

Podemos también definir la θ-Clau(P), donde $P \subseteq Q$, de manera natural como

$$\theta - \mathrm{Clau}(P) := \bigcup_{q\in P} \theta - \mathrm{Clau}(q)$$

Ahora podemos definir $\hat{\delta}$ por:

- (i) $\hat{\delta}(q,\theta) = \theta$-Clau (q).

- (ii) $\hat{\delta}(q,\omega a) = \theta$-Clau (P), donde $P = \{p :$ existe $r \in \hat{\delta}(q,\omega)$ y $p \in \delta(r,a)\}$, para todo $\omega \in \sum^*$ y $a \in \sum$.
  Extendemos δ y $\hat{\delta}$ a conjuntos de estados por:

- (iii) $\delta(R,a) = \bigcup_{q\in R} \delta(q,a)$, con $R \subseteq Q$

- (iv) $\hat{\delta}(R,\omega) = \bigcup_{q\in R} \hat{\delta}(q,\omega)$, con $R \subseteq Q$

Note que $\hat{\delta}(q,a)$ no es igual necesariamente a $\delta(q,a)$, puesto que $\hat{\delta}(q,a)$ incluye las transiciones por θ, pero $\delta(q,a)$ no; además $\hat{\delta}(q,\theta)$ no es tampoco necesariamente igual a $\delta(q,\theta)$. Por tanto es necesario distinguir δ de $\hat{\delta}$ cuando hablemos de los A.F.N. con θ-movimientos. Esto motiva la definición siguiente.

Definición 1.3.2 *Sea $M = (Q,\sum,\delta,q_o,F)$ un A.F.N. con θ-movimiento. El lenguaje aceptado por M, denotado por Lac(M), es Lac$(M) := \{\omega \in \sum^* :$ $\hat{\delta}(q_o,\omega)$ contiene un estado de $F\}$*

Ejemplo 1.3.1 *Sea $M = (Q,\sum,\delta,q_o,F)$ un A.F.N. con θ-movimientos. donde $Q = \{q_o,q_1,q_2\}$, $\sum = \{0,1,2\}$, $F = \{q_2\}$ y δ es dada por la figura* 1.5

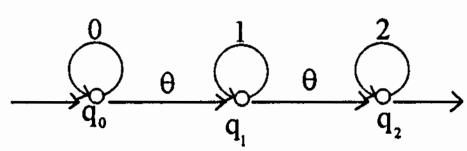

Figura 1.5:

Aca, $\hat{\delta}(q_o,\theta) = \theta\text{-}Clau(q_o) = \{q_o,q_1,q_2\}$, *así*

$$\begin{aligned}
\hat{\delta}(q_o,0) &= \theta - Clau(\delta(\hat{\delta}(q_o,\theta),0)) = \theta - clau(\delta(\{q_o,q_1,q_2\},0)) \\
&= \theta - Clau(\delta(q_o,0) \cup \delta(q_1,0) \cup \delta(q_2,0)) \\
&= \theta - Clau(q_o) = (q_0,q_1,q_2)\,, \text{ de manera que}
\end{aligned}$$

$$
\begin{aligned}
\hat{\delta}(q_o, 01) &= \theta - Clau(\delta(\hat{\delta}(q_o, 0), 1)) \\
&= \theta - Clau(\delta(\{q_0, q_1, q_2\}, 1)) \\
&= \theta - Clau(\delta(q_0, 1) \cup \delta(q_1, 1) \cup \delta(q_2, 1)) \\
&= \theta - Clau(q_1) \\
&= \{q_1, q_2\}. \; Luego\; 01 \in Lac(M).
\end{aligned}
$$

Ahora veremos la equivalencia entre los A.F.N. con θ-movimientos y sin θ-movimientos.
Observemos que los cambios de estados por la entrada θ en los A.F.N. con θ-movimientos permiten que estos ACEPTEN conjuntos no regulares, luego, un A.F.N. con θ-movimientos puede ser simulado por un A.F.N. sin θ-movimientos.

Teorema 1.3.1 *Si $L \subseteq \sum^*$ es aceptado por un A.F.N. con θ-movimientos entonces L es aceptado por un A.F.N. sin θ-movimientos.*

Prueba. Sea $M = (Q, \sum, \delta, q_o, F)$ un A.F.N. con θ-movimientos aceptando $L \subseteq \sum^*$. Definimos $M' := (Q, \sum, \delta', q_o, F')$, donde

$$
F' = \begin{cases} F \cup \{q_o\} & ,\text{si la } \theta - \text{Clau}(q_o) \text{ contiene un estado de } F, \\ F & ,\text{en caso contrario.} \end{cases}
$$

y δ' es definida por $\delta'(q, a) = \hat{\delta}(q, a)$, con $q \in Q$, $a \in \sum$.
Claramente M' así definido es un A.F.N. sin θ-movimientos. Así podemos usar δ' por $\hat{\delta}'$, pero debemos distinguir entre δ y $\hat{\delta}$.
Afirmación. $\delta'(q_o, x) = \hat{\delta}(q_o, x)$, con $x \in \sum^*$, $x \neq \theta$ $(x = \theta \Longrightarrow \delta'(q_o, \theta) = \{q_o\}$, $\hat{\delta}(q_o, \theta) = \theta - \text{Clau}(q_o))$
En efecto, por inducción sobre la longitud de x tenemos que si $|x| = 1$, entonces $x = a$, $a \in \sum$ y $\delta'(q, a) = \hat{\delta}(q, a)$.
Supongamos que la afirmación es verdadera para los x en $\sum^*$ tales que $|x| = m > 1$, y sea $x = \omega a$, $\omega \in \sum^*$, $a \in \sum$, $|\omega| = m$, entonces $|x| = m + 1$ y $\delta'(q_o, \omega a) = \delta'(\delta'(q_o, \omega), a)$. Por lo supuesto tenemos que $\delta'(q_o, \omega) = \hat{\delta}(q_o, \omega)$; ahora, sea $p = \hat{\delta}(q_o, \omega)$. Como

$$
\delta'(P, a) = \bigcup_{q \in P} \delta'(q, a) = \bigcup_{q \in P} \hat{\delta}(q, a) \text{ , entonces } \bigcup_{q \in P} \hat{\delta}(q, a) = \hat{\delta}(q, \omega a),
$$

así

$$\delta'(q_o, \omega a) = \hat{\delta}(q_o, \omega a).$$

Por otro lado, veamos que $\delta'(q_o, x)$ contiene un estado de F. En efecto, si $x = \theta$, se tiene obviamente lo deseado; ahora, si $x \neq \theta$, entonces $x = \omega a$, para algún $a \in \sum$. Si $\hat{\delta}(q_o, x)$ contiene un estado de F, entonces $\delta'(q_o, x)$ contiene el mismo estado en F'.
Recíprocamente, si $\delta'(q_o, x)$ contiene un estado en F' diferente de q_o, entonces $\hat{\delta}(q_o, x)$ contiene un estado de F. Si $\delta'(q_o, x)$ contiene a q_o y $q_o \notin F$, entonces como $\hat{\delta}(q_o, x) = \theta$-Clau $(\delta(\hat{\delta}(q_o, \omega), a))$, el estado en la θ-Clau (q_o) y en F debe pertenecer a $\hat{\delta}(q_o, x)$. Luego, $Lac(M) = Lac(M') = L$.

□

Ejemplo 1.3.2 *Consideremos el Autómata del ejemplo 1.3.1 y construyamos un A.F.N. sin θ-movimientos.*
Como la θ-Clau(q_o) = $\{q_o, q_1, q_2\}$, entonces $M' = (\{q_o, q_1, q_2\}, \{0, 1, 2\}, \delta', q_o, F')$, donde $F' = \{q_o, q_2\}$.
Ahora, $\delta'(q_o, 0) = \hat{\delta}(q_o, 0) = \theta$-Clau $(\delta(\hat{\delta}(q_o, 0), 0)) = \{q_o, q_1, q_2\}$, $\delta'(q_o, 1) = \hat{\delta}(q_o, 1) = \theta$-Clau $(\delta(\hat{\delta}(q_o, 0), 1)) = \theta$-Clau $(\delta(q_o, 1) \cup \delta(q_1, 1) \cup \delta(q_2, 1)) = \theta$-Clau $(q_1) = \{q_1, q_2\}$ y $\delta'(q_o, 2) = \theta$-Clau $(\delta(\hat{\delta}(q_o, \theta), 2)) = \theta$-Clau $(q_2) = \{q_2\}$. Por tanto obtenemos el digrama de transición siguiente:

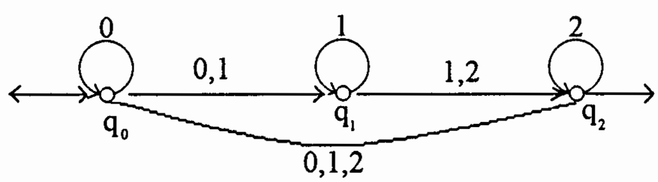

Figura 1.6:

El cual representa el A.F.N. sin θ-movimientos asociado a M.

1.4 Expresiones Regulares

.

Introducimos ahora las llamadas expresiones regulares, las cuales nos servirán para describir a los lenguajes aceptados por lo A.F's.

Definición 1.4.1 *Sea $\sum$ un alfabeto. las expresiones regulares sobre $\sum$ y los conjuntos que estas denotan se definen recursivamente como sigue:*

- *(i) $\emptyset$ es una expresión regular (e.r) y denota al conjunto vacío.*
- *(ii) θ es una e.r que denota al conjunto $\{\theta\}$.*
- *(iii) Para cada $a \in \sum$. $\boldsymbol{a}$ es una expresión regular que denota al conjunto $\{a\}$.*
- *(iv) Si r y s son e.r's denotando los lenguajes R y S respectivamente, entonces $(r+s)$, $(r \cdot s)$ y (r^*) son e.r's que denotan a los conjuntos $R \cup S$, RS y R^* respectivamente.*

Podemos omitir los paréntesis en las *e.r's*, teniendo en cuenta la siguiente jerarquía:
(1) $*$, (2) concatenación y (3) $+$.
Escribimos $rr^* = r^+ = r \cup r^2 \cup r^3 \cup \ldots \cup r^n \cup \ldots$ con r una *e.r.*

Teorema 1.4.1 *Sea r una expresión regular. Entonces existe un A.F.N con θ-transiciones que acepta $L(r)$= lenguaje denotado por r.*

Prueba Procederemos por inducción sobre el número de operaciones de la *e.r* r, y veremos que existe un A.F.N con θ-movimientos M con un solo estado final que no tiene transiciones fuera de dicho estado, y que $Lac(M) = L(r)$.
En efecto, si r no tiene operaciones, entonces r es θ , $\emptyset$ ó $\boldsymbol{a}$, para algún $a \in \sum$. En este caso los Autómatas buscados son dados por los siguientes diagramas de transición:

- (i) $\leftrightarrow q_o$, que corresponde a $r = \theta$.

- (ii) $\rightarrow q_o \quad q_F \longrightarrow$, que corresponde a $r = \emptyset$.
- (iii) $\rightarrow q_o \xrightarrow{a} q_F \longrightarrow$, que corresponde a $r = \boldsymbol{Q}$.

Supongamos ahora que el teorema es verdadero para $e.r's$ con $(i-1)$-operaciones $(i > 1)$ y sea r una $e.r$ con i-operaciones, entonces $r = r_1 + r_2$, $r = r_1 r_2$ ó $r = r_1{}^*$.
En el primer caso, es decir, si $r = r_1 + r_2$, entonces r_i, con $i = 1,2$, debe tener menos de i-operaciones ya que se ha supuesto de entrada que r tiene i-operaciones y que $i > 1$. Luego por la hipótesis de inducción existen A.F.N's con θ-movimientos
$M_1 = (Q_1, \sum_1, \delta_1, q_1, \{f_1\})$ y $M_2 = (Q_2, \sum_2, \delta_2, q_2, \{f_2\})$ tales que $Lac(M_1) = L(r_1)$ y $Lac(M_2) = L(r_2)$.
Supongamos que $Q_1 \cap Q_2 = \emptyset$, y sean q_o un nuevo estado inicial y f_o un nuevo estado final, entonces definimos un Autómata finito no determinista con θ-movimientos como sigue:
$M = (Q_1 \cup Q_2 \cup \{q_o, f_o\}, \sum_1 \cup \sum_2, \delta, q_o, \{f_o\})$, donde δ es definida de la manera siguiente:

- (i) $\delta(q_o, \theta) = \{q_1, q_2\}$
- (ii) $\delta(q,a) = \begin{cases} \delta_1(q,a) & \text{,si } q \in Q_1 \setminus \{f_1\} \text{ , } a \in \sum_1 \cup \{\theta\} \\ \delta_2(q,a) & \text{,si } q \in Q_2 \setminus \{f_2\} \text{ , } a \in \sum_2 \cup \{\theta\} \end{cases}$
- (iii) $\delta(f_1, \theta) = \delta(f_2, \theta) = \{f_o\}$;

Luego el diagrama de transición asociado a M es dado en la figura 1.7.
Nótese que éste diagrama de transición nos dice que una trayectoria de q_o a f_o debe ir de q_o a q_1 ó de q_o a q_2 por la entrada θ y luego seguir de q_1 a f_1 en M_1 ó de q_2 a f_2 en M_2 para finalizar de f_1 a f_o ó de f_2 a f_o por la entrada θ. Con lo cual una trayectoria de q_o a f_o etiquetada x en M existe, si y sólo si, existe una trayectoria de q_1 a f_1 etiquetada x en M_1 ó existe una trayectoria de q_2 a f_2 etiquetada x en M_2, es decir,
$Lac(M) = Lac(M_1) \cup Lac(M_2)$.
En el segundo caso, es decir, si $r = r_1 . r_2$, entonces por la hipótesis de inducción existen M_1 y M_2 como en el caso 1. Ahora, sea $M = (Q_1 \cup Q_2, \sum_1 \cup \sum_2, \delta, \{q_1\}, \{f_2\})$, donde δ se define por:

- (i) $\delta(q,a) = \begin{cases} \delta_1(q_1,a) & ,\text{si } q \in Q_1 \setminus \{f_1\} \ , \ a \in \sum_1 \cup \{\theta\} \\ \delta_2(q_2,a) & ,\text{si } q \in Q_2 \setminus \{f_2\} \ , \ a \in \sum_2 \cup \{\theta\} \end{cases}$
- (ii) $\delta(f_1,\theta) = \{q_2\}$

Así, tenemos gráficamente a M, dada en la figura 1.8.

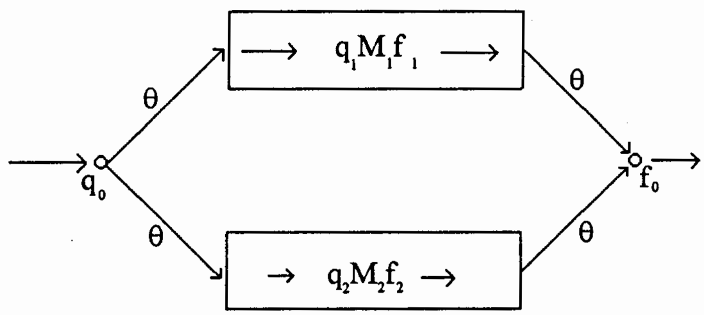

Figura 1.7:

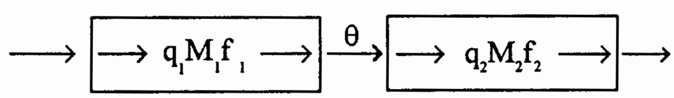

Figura 1.8:

Cada trayectoria de q_1 a f_2 en M, pasa de q_1 a f_1 por alguna etiqueta x en M_1, luego de f_1 a q_2 por la etiqueta θ y finalmente de q_2 a f_2 por una etiqueta y en M_2, es decir,

$$Lac(M) = Lac(M_1) \cdot Lac(M_2) = \{ \ xy \ / \ x \in L(M_1) \ , \ y \in L(M_2) \ \}.$$

Finalmente, si $r = r_1^*$, sea $M_1 = (Q_1, \sum_1, q_1, \delta_1, \{f_o\})$ con $L(M_1) = r_1$ y definamos $M = (Q_1 \cup \{q_o, f_o\}, \sum_1, \delta_1, q_o, \{f_o\})$, donde δ es definida como sigue:

- (i) $\delta(q_o,\theta) = \delta_1(f_1,,\theta) = \{q_1,f_o\}$
- (ii) $\delta(q,a) = \delta_1(q,a)$, si $q \in Q_1 \setminus \{f_1\}$, $a \in \sum_1 \cup \{\theta\}$.

Gráficamente el diagrama de transición para M es dado en la figura 1.9

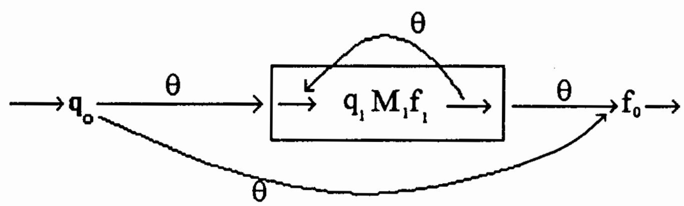

Figura 1.9:

Cada trayectoria de q_o a f_o en M, es una trayectoria de q_o a q_1 etiquetada por θ; luego de q_1 a f_1 tenemos una trayectoria en M_1 etiquetada x, y podemos ir nuevamente con la etiqueta θ a q_1 desde f para llegar nuevamente a f, y así repetir el ciclo cuantas veces queramos y finalmente con la etiqueta θ pasamos de f_1 a f_o, es decir, $Lac(M) = Lac(M_1)^*$.

$\square$

Ejemplo 1.4.1 *Construyamos un A.F.N. con θ-movimientos para la expresión regular* $01^* + 1$. *Pongamos* $r = 01^* + 1 = r_1 + r_2$, *con* $r_1 = 01^*$ *y* $r_2 = 1$.
El Autómata para r_2 *es* $\rightarrow q_1 \xrightarrow{1} q_2 \rightarrow$

Pongamos $r_1 = r_3\, r_4$, con $r_3 = 0$ y $r_4 = 1^*$. Así el Autómata para r_3 es $\rightarrow q_3 \xrightarrow{0} q_4 \rightarrow$; pero $r_4 = r_5^*$, donde $r_5 = 1$, determina que el Autómata para r_5 es $\rightarrow q_5 \xrightarrow{1} q_6 \rightarrow$ y en consecuencia el Autómata para r_4 es dado en la figura 1.10, donde q_7 y q_8 son los estados inicial y final respectivamente agregados en la construcción correspondiente al Autómata M asociado a r_4, por tanto el Autómata para $r_1 = r_3\, r_4$ es dado por la figura 1.11.
Finalmente, el Autómata correspondiente a $r = r_1 + r_2 = 01^* + 1$ es dado en la figura 1.13.

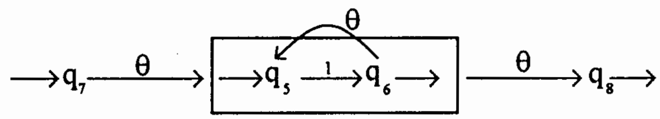

Figura 1.10:

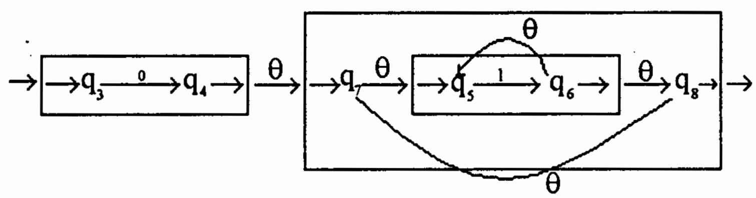

Figura 1.11:

Teorema 1.4.2 *Si L es aceptado por un A.F.D., entonces L es denotado por una expresión regular* (*e.r*).

Del teorema 1.4.2 se deduce el siguiente círculo que muestra las relaciones entre los Autómatas finitos definidos hasta ahora y las expresiones regulares.

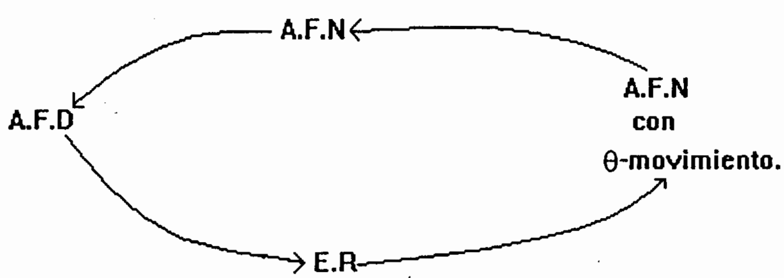

Figura 1.12:

En consecuencia, los únicos conjuntos que aceptan los A.F., son los conjuntos regulares.

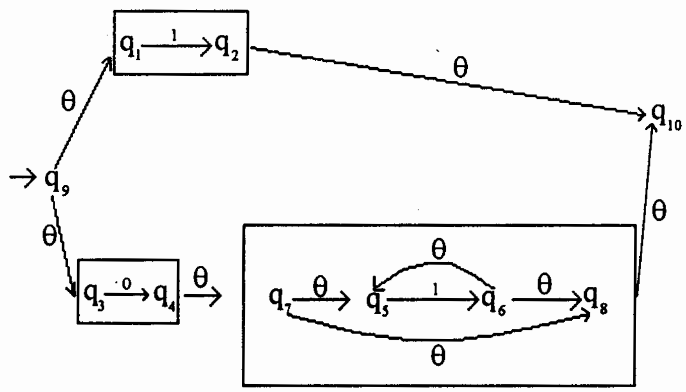

Figura 1.13:

1.5 Ejercicios Propuestos

Ejercicio 1.5.1 Para el Autómata del ejemplo 1.1.2 pruebe que $Lac(M) = (\alpha\, \gamma^*\, \beta)^*$

Ejercicio 1.5.2 Sean M_1 y M_2 A.F's trim. Pruebe que si M_2 refina M_1, entonces existe una única función $h : Q_2 \longrightarrow Q_1$ que satisface

$$h(\delta_2(q_2, r)) = \delta_1(q_1, r)\ ,\quad r \in \overline{L(M_2)}$$

Ejercicio 1.5.3 Sean M_1 y M_2 como en el ejercicio 1.5.2, tal que $L(M_1) = L_1$ y $L(M_2) = L_2$, pruebe que existe un A.F A, tal que $L(A) = L_2$ y A refina M_1.

Ejercicio 1.5.4 Los dos diagramas siguientes representan Autómatas finitos M_i, $i = 1, 2$; en c/u de ellos encontrar: $L(M_i)$, $Lac(M_i)$, $Q^i ac$ $Q^i co$, $i = 1, 2$,

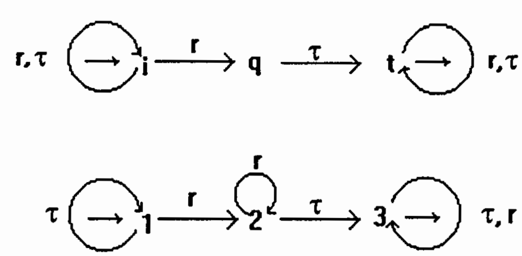

Figura 1.14:

Ejercicio 1.5.5 Pruebe lo siguiente:

$$(a)\ \sum = \{\alpha, \beta\},\quad L = \alpha^* = \{\theta, \alpha, \alpha\alpha, \ldots\} \quad\Longrightarrow ||L|| = 2.$$
$$(b)\ \sum = \{\alpha, \beta\},\quad L = \{\alpha^n \cdot \beta^n : n = 0, 1, 2, \ldots\} \quad\Longrightarrow ||L|| = 0.$$

Ejercicio 1.5.6 Sea δ la función de transición de un A.F.D. probar que para todo $x, y \in \sum^*$, $\delta(q, xy) = \delta(\delta(q, x), y)$

Ejercicio 1.5.7 Describa los conjuntos aceptados por los A.F's cuyos diagramas de transición son dados en las figuras 1.15 y 1.16

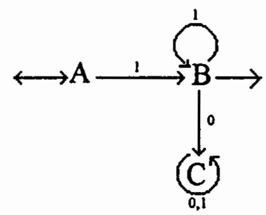

Figura 1.15:

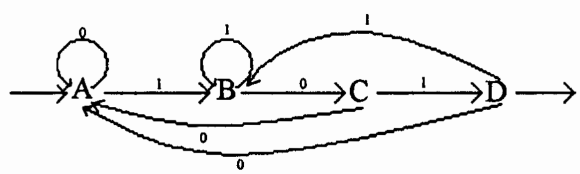

Figura 1.16:

Ejercicio 1.5.8 Construir A.F's. equivalentes a los A.F.N's. siguientes

$$(a)\ (\{p,q,r,s\}\ ,\quad \{0,1\}\ ,\quad \delta_1, p, \{s\}),$$
$$(b)\ (\{p,q,r,s\}\ ,\quad \{0,1\}\ ,\quad \delta_2, p, \{q,s\}),$$

donde δ_1 y δ_2 son dadas respectivamente en las tablas siguientes:

	Entradas	
Estados	0	1
p	$\{p,q\}$	$\{p\}$
q	$\{r\}$	$\{r\}$
r	$\{s\}$	$\emptyset$
s	$\{s\}$	$\{s\}$

Tabla 1.

	Entradas	
Estados	0	1
p	$\{q,s\}$	$\{q\}$
q	$\{r\}$	$\{q,r\}$
r	$\{s\}$	$\{p\}$
s	$\emptyset$	$\{p\}$

Tabla 2.

Ejercicio 1.5.9 Construir A.F's. equivalentes a las siguientes e.r's:

$$\begin{array}{ll} (a) & (11+0)^*(00+1)^*. \\ (b) & (1+01+001)^*(0+0+00). \\ (c) & 10+(0+11)0^*1 \end{array}$$

Ejercicio 1.5.10 Construir e.r's. correspondientes a los diagramas de estados dados en las figuras siguientes

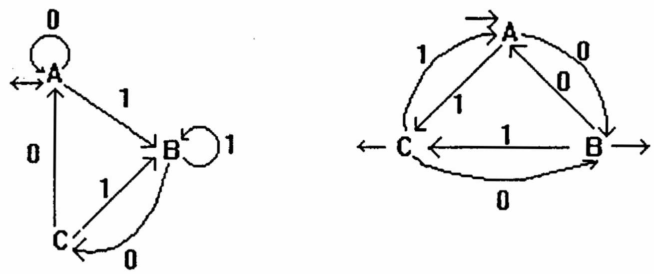

Figura 1.17:

Ejercicio 1.5.11 Pruebe las siguientes identidades para e.r's r, s y t. Aqui, $r = s$ significa $L(r) = L(s)$.

$$\begin{array}{lll} (a) & r+s & = s+r. \\ (b) & (rs)t & = r(st). \\ (c) & (r+s)t & = rt+st \\ (d) & r(s+t) & = rs+rt \\ (e) & \emptyset^* & = \theta \\ (f) & (r^*)^* & = r^* \\ (g) & (\theta+r)^* & = r^* \\ (h) & (r^*s^*) & = (r+s)^*. \end{array}$$

Ejercicio 1.5.12 Sean r y s expresiones regulares. Considere la ecuación $x = rx + s$, donde rx denota la concatenación de r y x, y $+$ denota unión. Suponga que el conjunto denotado por r no contiene θ.
Encuentre la solución para x y pruebe que es única. ¿Cuál sería la solución si $L(r)$ contiene θ?

Capítulo 2

Propiedades de los Conjuntos Regulares

Nuestro interés ahora está centrado en determinar cuando un lenguaje es regular, cuando los conjuntos regulares denotados por diferentes expresiones regulares son los mismos y como hallar un A.F de estado mínimo que denote el mismo lenguaje de un A.F dado, para ello, introducimos en éste capítulo el llamado lema de Pumping y el teorema de Myhill-Nerode junto con las propiedades de clausura de las expresiones regulares.

2.1 Lema de Pumping para Conjuntos Regulares

El lema de pumping es usado para probar que ciertos lenguajes no son regulares y que un A.F acepta un lenguaje infinito bajo ciertas condiciones sobre la longitud de la palabra; además, éste lema es una herramienta útil en el desarrollo de algoritmos para decidir cuando el lenguaje aceptado por un A.F es finito o infinito.

Lema 2.1.1 *(pumping) Sea L un conjunto regular, entonces existe una constante n tal que si $Z \in L$ y $|Z| \geq n$, se tiene que $Z = u.v.w$, con $|uv| \leq n$ y $|v| \geq 1$; más aún, $uv^iw \in L$, $\forall\, i \geq 0$. Además, n nó es mayor que el número de estados del mas pequeño A.F aceptando a L.*

Prueba. Supongamos que $L \subseteq \sum^*$ es un conjunto regular y sea $M = (Q, \sum, \delta, q_o, F)$ un A.F tal que $Lac(M) = L$.
Sea $Z = a_1\, a_2 \ldots a_m \in L$, con $m \geq n$, donde $n = card\,(Q)$.
Para cada $i = 1, 2, \ldots, m$, pongamos $\delta(q_o, a_1\, a_2 \ldots a_i) = q_i$. Así alguno de los q_i se repite, pues $m \geq n$; en consecuencia existen $j, k \in I\!N$, con $0 \leq j < k \leq n$ tales que $q_j = q_k$. Gráficamente este hecho puede ser visto como sigue:

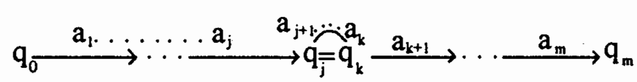

Figura 2.1:

La cual es la trayectoria etiquetada $Z = a_1\, a_2 \ldots a_m$.
Como $j < k$, entonces $a_{j+1} \ldots a_k$ tiene longitud mayor o igual que 1, es decir, si $v = a_{j+1} \ldots a_k$, entonces $|v| \geq 1$; ahora como $k \leq n$, se sigue que $|v| \leq n$.
Pongamos $u = a_1 \ldots a_j$, así $|uv| \leq |n|$. Finalmente si $w = a_{k+1} \ldots a_m$, entonces $Z = a_1\, a_2 \ldots a_j\, a_{j+1} \ldots a_k \quad a_{k+1} \ldots a_m$ tiene una descomposición $Z = uvw$, con $|v| \geq 1$ y $|uv| \leq n$.
Por otro lado, como $q_m = \delta(q_o, a_1 \ldots a_m) \in F$, pues $Z = a_1 \ldots a_m \in L$, entonces $uw \in L$, pues

$$\begin{aligned}
\delta(q_o, uw) &= \delta\,(q_o, a_1 \ldots a_j\, a_{K+1} \ldots a_m) \\
&= \delta\,(\delta\,(q_o, a_1 \ldots a_j), a_{K+1} \ldots a_m) \\
&= \delta\,(q_K, a_{K+1} \ldots a_m) \\
&= q_m.
\end{aligned}$$

Por inducción sobre i se puede probar que $\delta\,(q_o, uv^i w) = q_m$.
Concluimos que $uv^i w \in L$, para todo $i \geq 0$.

$\square$

Observación 2.1 *El lema de pumping nos dice que si un A.F acepta una palabra de longitud mayor o igual que el cardinal de Q, entonces el A.F acepta un conjunto infinito de palabras de la forma uv^iw. En consecuencia el lenguaje aceptado por dicho A.F es infinito. Sin embargo, este lema no nos dice que si z es una palabra suficientemente larga, entonces $Z = uv^iw$, para algún $i \geq 0$.*

Veamos algunas aplicaciones del lema de pumping.

#1. Probaremos que el conjunto $L = \{0^{i^2} : i \geq 1\}$ no es regular.
En efecto, si suponemos que L es regular, entonces por el lema 2.1.1, existe n tal que si $Z \in L$ y $|Z| \geq n$, entonces $Z = uvw$, con $|v| \geq 1$, $|uv| \leq n$ y $uv^iw \in L$, para todo $i \geq 0$.
Escojamos $Z = 0^{n^2} \in L$, entonces $0^{n^2} = uvw$, con $1 \leq |v| \leq n$, $|uv| \leq n$ y $uv^iw \in L$, para todo $i \geq 0$, pero $n^2 < |uv^2w| \leq n^2n < (n+1)^2$, de donde $uv^2w \notin L$, pues uv^2w no es cuadrado perfecto. Esto es una contradicción por tanto L no es regular.

#2. Probaremos que el conjunto $L = \{r^p\gamma r^P : P \geq 0\}$ no es regular.
En efecto, supongamos que L es regular y sea $Z = r^n\gamma r^n \in L$, donde n es la constante del lema de pumping, entonces por el lema 2.1.1 $Z = uvw$, con $|uv| \leq n$, $|v| \leq 1$ y $uv^iw \in L$, para todo $i \geq 0$. De aca que u y v no contienen el símbolo γ, luego $u = r^m$, $v = r^k$ y $w = r^h\gamma r^n$, para algunos $m, k, h, \in R_*$, con $m \geq 0, k \geq 1$, y $h \geq 0$; ahora, como $uv^iw \in L$, para todo $i \geq 0$, entonces en particular, $uv^{2n}w \in L$, es decir $r^m\,(r^K)^{2n}\,r^h\,\gamma\,r^n \in L$, de donde $m + 2kn + h = n$, pero $k \geq 1$ determina una contradicción en ésta última ecuación. Por tanto $uv^{2n}w \notin L$.
Concluimos entonces que L no es regular.

2.2 Propiedades de los Conjuntos Regulares

Existen operaciones con lenguajes que preservan los conjuntos regulares, en el sentido de que esas operaciones aplicadas a conjuntos regulares resultan ser conjuntos regulares. Cuando una operación en particular tiene ésta propiedad sobre una clase de lenguaje diremos que esta es una propiedad de clausura correspondiente a la clase de lenguaje.

Teorema 2.2.1 *Los conjuntos regulares son cerrados bajo unión, concatenación y clausura de Kleene.*

Prueba. Trivial, fundamentada en las expresiones regulares. $\square$

Teorema 2.2.2 *La clase de los conjuntos regulares es cerrada bajo complemento, es decir, si $L \subseteq \sum^*$ es un conjunto regular, entonces su complemento $\sum^* \setminus L$ es también un conjunto regular.*

Prueba. Sean L un conjunto regular en $\sum^*$ y $M = (Q, \sum, \delta, q_o, F)$ un A.F tal que $Lac(M) = L$. Consideremos el A.F. $M' = (Q, \sum, \delta, q_o, Q \setminus F)$, entonces $Lac(M') = \{x \in \sum^* : \delta(q_o, x) \in Q \setminus F\} = \sum^* \setminus \{x \in \sum^* : \delta(q_o, x) \in F\} = \sum^* \setminus L$. Así, $\sum^* \setminus L$ es un conjunto regular, pues es aceptado por M'.

$\square$

Teorema 2.2.3 *Los conjuntos regulares son cerrados bajo intersección.*

Prueba. Sean L_1 y L_2 conjuntos regulares, entonces $L_1 \cap L_2 = L_1^c \cup L_2^c$, donde L_i^c, $i = 1, 2$, denota el complemento con respecto a un alfabeto finito incluyendo los alfabetos de L_1 y L_2. Luego por los teoremas 2.2.1 y 2.2.2, $L_1 \cap L_2$ es regular.

$\square$

Observación 2.2 *Una prueba del teorema 2.2.3 fue dada en el capítulo 1.*

Ejemplo 2.2.1 *Sea $\sum = \{r, \gamma\}$. Para cada $s \in \sum^*$, sea $|s|_r$ el número de $r's$ en s. Entonces $|s|_\gamma = |s| - |s|_r$.*
Afirmamos que el conjunto $C = \{s : |s|_r = |s|_\gamma\}$ no es regular.

En efecto, $r^*\gamma^*$ es un conjunto regular; ahora si suponemos que C es regular, entonces por el teorema 2.2.3 $C \cap r^*\gamma^*$ es regular, pero $C \cap r^*\gamma^* = \{r^p\gamma^p : p \geq 0\}$ no es regular. Por tanto L no es regular.

Definición 2.2.1 *Sean L_1 y L_2 dos lenguajes, el cociente de L_1 y L_2 es el conjunto $\{x : existe\ y \in L_2, xy \in L_1\}$ y lo denotamos L_1/L_2.*

Ejemplo 2.2.2 *Sea* $L_1 = 0^*10^*$ *y sea* $L_2 = 0^*1$, *entonces* $L_1/L_2 = 0^*$, *ya que dado* $x \in 0^*$ *tomamos* $y = 1$ *y así* $xy \in L_1$ *y* $y \in L_2$.

Teorema 2.2.4 *La clase de los conjuntos regulares es cerrada bajo cociente, con conjuntos arbitrarios.*

Prueba. Sea $M = (Q, \sum, \delta, q_o, F)$ un AF tal que $R = Lac(M)$ y sea $L \subseteq \sum^*$, entonces R/L es aceptado por un A.F $M' = (Q, \sum, \delta, q_o, F')$ con comportamiento análogo a M, excepto que los estados finales de M' son todos los estados q de M tal que existe $y \in L$ para el cual $\delta(q, y) \in F$. Así, $\delta(q_o, x) \in F'$, si y sólo si , existe y tal que $\delta(q_o, xy) \in F$, es decir, R/L es aceptado por M'.

□

2.3 Algoritmos de Decisión para Conjuntos Regulares

Para responder algunas preguntas sobre los conjuntos regulares tales como: dado un lenguaje regular $L \subseteq \sum^*$, ¿es L vacío, finito o infinito?, ¿Es L un conjunto regular equivalente a otro?.
Asumiremos que los conjuntos regulares son representados por A.F's. o por expresiones regulares dada la equivalencia que existe entre estos.

Teorema 2.3.1 *Sea* L *el lenguaje aceptado por un A.F con* n *estados. Entonces:*

- *(i)* $L \neq \emptyset$, *si y sólo si, existe* $l \in L$ *tal que* $|l| < n$
- *(ii)* L *es infinito, si y sólo si, existe* $l \in L$ *tal que* $n \leq |l| < 2n$.

Prueba. *i*) Supongamos que existe $l \in L$ tal que $|l| < n$, entonces $L \neq \emptyset$. Recíprocamente, supongamos que $L \neq \emptyset$, entonces si w es tal que $|w| \leq |x|$, para todo $x \in L$, se tiene que $|w| < n$, pues en caso contrario, es decir, $|w| \geq n$ se tendría por el lema 2.1.1 que $w = uvz$ y así $|uv| < |w|$ lo cual contradice lo supuesto de w.

Prueba. Sea $L = (L_1 \cap L_2^c) \cup (L_1^c \cap L_2)$, donde L_i^c, $(i = 1, 2)$, es el complemento de L_i $(i = 1, 2)$ en $\sum^*$, entonces por los teoremas 2.2.1, 2.2.2 y 2.2.3 L es regular. En consecuencia existe un A.F M_3 tal que $Lac(M_3) = L$. Por tanto, $x \in L$, si y sólo si, $L_1 \neq L_2$, luego por el teorema 2.3.1 podemos decidir si $L_1 = L_2$.

□

2.4 Teorema de Myhill-Nerode y Minimización de Automatas Finitos Deterministas

El teorema de Myhill-Nerode caracteriza los conjuntos regulares y en consecuencia nos permite determinar la regularidad o no regularidad de un lenguaje dado.
Sea L un conjunto regular de $\sum^*$. Podemos preguntarnos acerca de la existencia de un A.F. M_o con $Lac(M_o) = L$ tal que para cualquier otro A.F. M existe una transformación de estado $\emptyset : M \longrightarrow M_o$. El A.F. M_o con esta propiedad es único salvo isomomorfismo y es llamado minimal. Su existencia puede ser establecida de dos formas diferentes. El primer método consiste en considerar un A.F.D. con comportamiento L definiendo una relación de equivalencia E sobre el conjunto de estados y construyendo un A.F. cociente M/E para ésta relación. Se puede probar que salvo isomomorfismo este cociente M/E es independiente de la escogencia de M y así es un A.F. minimal para el conjunto L. El segundo método, más elegante y algebraico, consiste de una construcción directa de un A.F. M para L y demostrar su minimalidad.

Definición 2.4.1 *Sean $M_1 = (Q, \sum, \delta, q_o, F)$ y $M_2 = (Q', \sum, \delta', q_o', F')$ dos A.F's.. Un Morfismo (o transformación de estados) entre M_1 y M_2 es una función $\emptyset : Q \longrightarrow Q'$ sastisfaciendo:*

- *(i)* $\emptyset(q_o) = q_o'$.
- *(ii)* $\delta'(\emptyset(q), r) = \emptyset(\delta(q, r))$, *para todo* $r \in \sum^*$.

- (iii) $\emptyset^{-1}(F') \subseteq F$.

Teorema 2.4.1 *(Myhill-Nerode). Las siguientes condiciones son equivalentes:*

- (i) *El conjunto $L \subseteq \sum^*$ es aceptado por un A.F.*
- (ii) *L es la unión de algunas de las clases de equivalencia de una relación de equivalencia invariante a derecha de índice finito.*
- (iii) *La relación de equivalencia R_L es de índice finito.*

Prueba $(i) \Longrightarrow (ii)$ Supongamos que $L \subseteq \sum^*$ es aceptado por un A.F. $M = (Q, \sum, \delta, q_o, F)$ y consideremos la relación de equivalencia invariante a derecha inducida por M, es decir, R_M. Como se sabe R_M es de índice finito, mas aún, si $n = \text{card}(Q)$, entonces $ind(R_M) \leq n$. Además, obviamente por la definición de R_M, $L = \bigcup_{x \in F} \bar{x}$ con $\delta(q_o, x) \in F$.

$(ii) \Longrightarrow (iii)$ Supongamos que E es una relación de equivalencia invariante a derecha de índice finito tal que L es la unión de algunas clases de equivalencia de E. Afirmamos que E es un refinamiento de R_L. En efecto si $x\ E\ y$, entonces, por lo supuesto, se tiene que para cada $z \in \sum^*$, $xz\ E\ yz$, en consecuencia $yz \in L$, si y sólo si, $xz \in L$, es decir, xR_Ly; de donde se sigue que la clase de x en E está contenida en alguna clase de equivalencia de R_L. Por tanto, se tiene que la afirmación es verdadera; en consecuencia, cada clase de equivalencia de E está contenida en alguna clase de equivalencia de R_L, con lo cual $\|R_L\| \leq \|E\|$, es decir, $ind(R_L) \leq ind(E)$.
Luego, R_L es de índice finito.

$(iii) \Longrightarrow (i)$ Supongamos que la relación R_L es de índice finito, y construyamos un A.F. como sigue:
$Q' = \{\bar{x} : x \in \sum^*\}$; pongamos $q'_o = \bar{\theta}$ y $F' = \{\bar{x} : x \in L\}$; definimos ahora a δ' por $\delta'(\bar{x}, a) = (\bar{xa})$. Por tanto $M' = (Q', \sum, \delta', q'_o, F')$ es bien definido; además, como $\delta'(q'_o, x) = \bar{x}$, entonces $x \in Lac(M')$, si y sólo si, $\bar{x} \in F'$, de donde M' es tal que $Lac(M') = L$.

$\square$

Teorema 2.4.2 *El A.F. de estado mínimo aceptando un conjunto $L \subseteq \sum^*$ es único salvo isomorfismo y es definido por M' en el teorema 2.4.1.*

Prueba Sea $M = (Q, \sum, \delta, q_o, F)$ un A.F que acepta a L, entonces por el teorema 2.4.1 tenemos que $card(Q) \geq card(Q')$, donde Q' es el conjunto de estados correspondientes al A.F. M', definido en el teorema 2.4.1.
Supongamos que $card(Q) = card(Q')$, entonces hay una identificación exacta entre los estados de M y los estados de M', es decir, si $q \in Q$, entonces debe existir $x \in \sum^*$ tal que $\delta(q_o, x) = q$, pues de lo contrario q puede ser quitado de Q dando lugar a un A.F. mas pequeño. Identifiquemos $q \in Q$ con el estado $\delta(q_o', x)$ de M'. Esta identificación es consistente. Si $\delta(q_o, x) = \delta(q_o, y) = q$, entonces por la prueba del teorema 2.4.1. x e y están en la misma clase de equivalencia de R_L. Así, $\delta'(q_o', x) = \delta'(q_o', y)$. Por tanto M es isomorfo a M'.
□

Definición 2.4.2 *Dos estados q_1, q_2 de un A.F. M son equivalentes, si y sólo si, para todo $r \in \sum^*$, se tiene que $\delta(q_1, r) \in F \Longleftrightarrow \delta(q_2, r) \in F$.
En éste caso escribimos $q_1 \; E \; q_2$ (ó $q_1 \equiv q_2$).*

Definición 2.4.3 *Dos estados q_1, q_2 de un A.F. M son llamados distinguibles si existe $r \in \sum^*$ tal que $\delta(q_1, r) \in F$ y $\delta(q_2, r) \notin F$ o viceversa.*

Dados dos estados cualesquiera q_1 y q_2 es importante saber decidir si $q_1 \; E \; q_2$ ó no. Para esto definamos relaciones de equivalencias E_p, $p \geq 0$ como sigue:
$q_1 \; E_p \; q_2$ si $(\delta(q_1, r) \in F \Longleftrightarrow \delta(q_2, r) \in F)$, para todo $r \in \sum^*$, $|r| \leq p$.

Es clara la siguiente cadena de inclusiones:

$$E \subseteq \ldots \subseteq E_p \subseteq \ldots \subseteq E_2 \subseteq E_1 \subseteq E_o; \quad \text{además} \quad E = \bigcap_{p=1}^{\infty} E_p.$$

Afirmación. $q_1 \; E_{p+1} \; q_2 \Longleftrightarrow$ para todo $r \in \sum, q_1 \; E_o \; q_2$ y $\delta(q_1, r) \; E_p \; \delta(q_2, r)$. En efecto, $q_1 \; E_{p+1} \; q_2$ significa que para todo $w \in \sum$, con $|w| \leq p + 1$, $\delta(q_1, w) \in F \Longleftrightarrow \delta(q_2, w) \in F$.
Tomemos $w = \theta$ y $w = rt$, con $|t| \leq p$ y así la afirmación queda probada.
De la Afirmación se sigue que si $E_{p+1} = E_p$, entonces $E_{p+2} = E_{p+1}$. Así, si $E_{p+1} = E_p$, entonces $E = E_p$.

Sea e_p el número de clases de equivalencias de la relación de equivalencia E_p, entonces:
$e_o \leq e_1 \leq \ldots \leq e_p \leq \ldots \leq card(Q)$; además, si excluimos los casos triviales $F = \emptyset$ y $F = Q$, entonces E_o tiene exactamente dos clases de equivalencia, a saber F y $Q \backslash F$. Así, $e_o = 2$. Por consiguiente debemos tener para algún $p \leq card(Q) - 2$ que $e_p = e_{p+1}$. De acá que $E_p = E_{p+1}$.
En consecuencia $E_p = E$. Luego, hemos probado la proposición siguiente.

Proposición 2.4.1 *En un A.F M dos estados son equivalentes, si y sólo si, para todo $r \in \sum^*$ tal que $|r| < card(Q) - 1$, $\delta(q_1, r) \in F \Longleftrightarrow \delta(q_2, r) \in F$.*

Corolario 2.4.1 *La equivalencia de dos estados en un A.F.D es decidible.*

Prueba: El algoritmo es dado en la proposición 2.4.1 □

Veamos ahora el método algebraico para la minimización de Autómatas finitos.

Sea L un lenguaje regular y sea $M = (Q, \sum, \delta, q_o, F)$ un A.F.D. tal que $Lac(M) = L$.
Consideremos $M_L = (Q', \sum, \delta', q'_o, F')$, donde $Q' = \{q \in Q/$ existe $r \in \sum^*,\ \delta(q_o, r) = q\}$, los elementos de Q' los denotaremos por $[q]$, $F' = \{[q]/q \in F\}$, $\delta'([q], a) = [\delta(q, a)]$. δ' está bien definida. En efecto, si $p \equiv q$, entonces $\delta(q, a) = \delta(p, a)$, esto es, si $\delta(q, a)$ es distinguible de $\delta(p, a)$ por x, entonces ax distingue q de p; además $\delta'([q_o], x) = [\delta(q_o, x)]$ lo cual puede probarse por inducción sobre la longitud de x. Por tanto, $Lac(M) = Lac(M') = L$. Finalmente es fácil probar que M' no tiene más estados que el índice de R_L donde $L = Lac(M)$. En consecuencia obtenemos la minimalidad de M'.

□

2.5 Ejercicios Propuestos

Ejercicio 2.5.1 Pruebe que los conjuntos siguientes no son regulares.

$$\begin{array}{lll} (a) & L & = \{r^p \gamma^p \ / \ p \geq 0\}. \\ (b) & L & = \{r^p \gamma^q \ / \ p \leq q\}. \end{array}$$

Ejercicio 2.5.2 $Lac(M)$ es finito, si y sólo si, M no tiene trayectorias cerradas de longitud mayor que cero (M es un A.F.)

Ejercicio 2.5.3 Pruebe que cualquier A.F. aceptando el conjunto $\{r^n\gamma^n \ / \ 0 \leq n \leq N\}$ debe contener al menos $2N + 1$ estados.

Ejercicio 2.5.4 Pruebe que el lenguaje aceptado por el A.F. de la figura siguiente es $L = r^*\gamma^*$

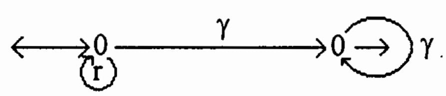

Figura 2.2:

Ejercicio 2.5.5 Pruebe que $L = \{s/ \ |s|_t \leq |s|_\gamma\}$ no es regular.

Ejercicio 2.5.6 Sea M un A.F. con n estados y $Lac(M) = L$. Entonces L es finito, si y sólo si, para todo $s \in L$, $|s| < n$.

Ejercicio 2.5.7 Cuales de los siguientes conjuntos son regulares:

(a) $\{0^{2n} : \ n \geq 1\}$
(b) $\{0^m 1^n 0^{m+n} : \ m \geq 1 \ , \ n \geq 1\}$.
(c) El conjunto de palabras con igual número de ceros y unos.
(d) $\{r^p\gamma^q : \ q \leq p\}$

Ejercicio 2.5.8 Pruebe la extensión del lema de Pumping para conjuntos regulares: sea L un conjunto regular. Entonces existe una constante n tal que para cada z_1, z_2, z_3, con $z_1, z_2, z_3 \in L$ y $|z| = n$, z_2 puede ser escrito como $z_2 = uvw$, $|v| \geq 1$ y para todo $i \geq 0$, $z_1uv^iwz_2 \in L$.

Ejercicio 2.5.9 Use el ejercicio 2.5.8 para probar que el conjunto $\{0^i\, 1^m\, 2^m : m, i \geq 1\}$ no es regular.

Ejercicio 2.5.10 Pruebe que el conjunto $A = \{a_1\ a_3\ a_5\ \ldots a_{2n-1}\ /\ a_1 a_2\ a_3 a_4 \ldots a_{2n} \in L\}$, es regular, donde L es un conjunto regular.

Ejercicio 2.5.11 ¿Cuales son las clases de equivalencia de R_L en el teorema de Myhill-Nerode para $L = \{0^n 1^n :\ n \geq 1\}$?.

Ejercicio 2.5.12 Sean $\sum_1, \sum_2$ alfabetos y consideremos ${\sum^*}_1, {\sum^*}_2$. Sea L un subconjunto de ${\sum^*}_1, \times {\sum^*}_2$. Entonces L es regular, si y sólo si, L es la unión de conjuntos de la forma $L_1 \times L_2$, donde L_1 es un subconjunto regular de ${\sum^*}_1$ y L_2 es un subconjunto regular de ${\sum^*}_2$.

Ejercicio 2.5.13 Un subconjunto L del monoide $\sum^*$ es regular, si y sólo si, existen subconjuntos de $\sum^*$ $L_1, \ldots L_n$, $B_1, \ldots B_n$ tales que $L = \cup\ L_i B_i$, y si $st \in A$, entonces $s \in L_i$, $t \in B_i$, para algún $1 \leq i \leq n$.

Ejercicio 2.5.14 Pruebe que si L es un conjunto regular de $\sum^*$ también lo es el conjunto $B = \{(x, y) : x.y \in L\} \subseteq \sum^* \times \sum^*$. Pruebe que si B es regular, entonces L es la unión finita de conjuntos de la forma CD, con $C, D \in \sum^*$ regulares.

Ejercicio 2.5.15 Pruebe que los siguientes subconjuntos de $\{r, \gamma\}^*$ no son regulares. $A = \{r^n \gamma^n\ /\ n \in X\}$, $B = \{r^n \gamma r^n\ /\ n \in X\}$, donde X es cualquier subconjunto infinito de $I\!N$.

Capítulo 3

Maquinas Secuenciales

Las maquinas secuenciales que se estudian en este capítulo son las llamadas maquinas de MOORE y maquinas de MEALY. Estas maquinas de estados tienen características análogas a los Autómatas finitos deterministas, pero involucran una función parcial adicional que determina la salida de la máquina. Las salidas de la máquina de Moore dependen de los estados y las salidas de la máquina de Mealy, dependen tanto de los estados como de las entradas. Demostraremos que los dos tipos de máquina, antes mencionadas, producen la misma transformación de salida. Dada esta equivalencia nos referiremos a los Autómatas de Moore (o de Mealy) como Autómatas finitos. Definiremos la transformación de entrada- salida y realización de un A.F., dando algunas propiedades como isomorfismo entre A.F's., distinguibilidad, minimalidad, etc. Finalmente daremos algunas técnicas usando códigos para describir los A.F's. y algunas nociones de complejidad, donde veremos que los A.F's. reducidos son de complejidad finita.

3.1 Maquinas de Moore y Maquinas de Mealy

Definición 3.1.1 *Una máquina de Moore es un sextuple* $M = (Q, \sum, \gamma, \delta, \lambda, q_o)$*, donde* $\sum, Q, \delta,$ *y* q_o *son como en los A.F.D's.,* γ *es un alfabeto de salida y* λ *es una función parcial de* Q *en* $\gamma(\lambda : Q \longrightarrow \gamma)$*, es decir,* $\lambda(q)$ *es la salida de la máquina asociada al estado* q*.*

Definición 3.1.2 *Una máquina de Mealy es un sextuple* $M = (Q, \sum, \gamma, \delta, \lambda, q_o)$*, donde* M *es como en la máquina de Moore con la diferencia de que las salidas dependen tanto de las entradas como de los estados* $(\lambda : Q \times \sum \longrightarrow \gamma)$*; así,* $\lambda(q, a)$ *es la salida asociada con la transición del estado* q*, en la entrada* a*.*

Nuestro problema consiste ahora en extender la función parcial λ de la máquina de Moore y la máquina de Mealy. Para las maquinas de Mealy tenemos que $\lambda : Q \times \sum \longrightarrow \gamma$ es la función parcial de salida. Extendemos λ como sigue:
$(*)$ $\lambda : Q \times \sum^* \longrightarrow \gamma^*$ Satisface:

- (i) $\lambda(q, \theta) = \theta$.
- (ii) $\lambda(q, st) = \lambda(q, s)\lambda(qs, t), s, t \in \sum^*$, donde $qs = \delta(q, s)$. Y se define inductivamente como $\lambda(q, \theta) = \theta$, $\lambda(q, s)\lambda(qs, a) = \lambda(q, sa)$.

Veamos que (ii) se tiene. Para esto procederemos por inducción sobre la longitud de $t \in \sum^*$.
Si $|t| = 0$, entonces $t = \theta$, en consecuencia $\lambda(q, s\theta) = \lambda(q, s)\lambda(qs, \theta)$ (recuerde que $\lambda(qs, \theta) = \lambda(\delta(q, s), \theta) = \theta$).

Suponga ahora que (ii) es verdadera para $t \in \sum^*$, $|t| = n$ y sea $t = ua$, con $a \in \sum$, $|u| = n$, entonces $|t| = n + 1$, así:

$$\begin{aligned}
\lambda(q, st) &= \lambda(q, sua) = \lambda(q, su)\lambda(qsu, a) \\
&= \lambda(q, s)\lambda(qs, u)\lambda(qsu, a) \\
&= \lambda(q, s)\lambda(qs, ua) \\
&= \lambda(q, s)\lambda(qs, t)
\end{aligned}$$

En las maquinas de Mealy un arco lo denotamos por $p \xrightarrow{r/a} q$, con $p, q \in Q$, $r \in \sum$, $a \in \gamma$, lo cual significa que $\delta(p, r) = q$ y $\lambda(p, r) = a$.
Ahora, si $c : p \longrightarrow q$ es una trayectoria de longitud n en la máquina M y $r_1/a_1 \ldots r_n/a_n$ es una sucesión de etiquetas de c, entonces poniendo $s = r_1 \ldots r_n$ y $a = a_1 a_2 \ldots a_n$, tenemos que $\delta(p, s) = q$ y $\lambda(p, s) = a$; en consecuencia la trayectoria puede ser denotada por $p \xrightarrow{s/a} q$.

Definición 3.1.3 *Sea M una máquina de Mealy. La función calculada por M (0 el resultado de M) es una función parcial $F_M : \sum^* \longrightarrow \gamma^*$, definida por $F_M(s) = \lambda(q_o, s)$.*

Así, $F_M\ (r\beta) = F_M\ (r)\lambda(\delta(q_o, r), \beta)$, para todo $r, \beta \in \sum^*$.

Definición 3.1.4 *Una función parcial $F : \sum^* \longrightarrow \gamma^*$ se llama Secuencial, si existe una máquina de Mealy M tal que $F = F_M$.*

Observación 3.1 . *Es claro que si λ y δ son verdaderas funciones, entonces la función extendida definida en $(*)$ es una verdadera función. En este caso diremos que la máquina de Mealy es completa.*

Para calcular $F_M(s)$, con $s = r_1 r_2 \ldots r_n$, basta calcular los estados $q_o, q_1, \ldots q_n$, con $q_k = \delta(q_{k-1}, r_k)$ y las salidas $a_k = \lambda(q_{k-1}, r_k)$, $1 \leq k \leq n$.
Así $F_M(s) = a_1 a_2 \ldots a_m$

Si para algún k, $\delta(q_{k-1}, r_k) = \emptyset$, entonces la máquina de Mealy se bloquea $F_M(s) = \emptyset$. Nótese que si $|r| = n$, con $r = r_1 \ldots r_n$, entonces $|F_M(r)| = n$. De la misma manera como se extendio λ para las maquinas de Mealy se extiende para las maquinas de Moore. Así la respuesta o salida a la palabra de entrada $a_1 a_2 \ldots a_n$ es $(**)\ \lambda(q_o)\lambda(q_1)\ldots\lambda(q_n)$, donde $q_i = \delta(q_{i-1}, a_i)$, $1 \leq i \leq n$
Note que $(**)$ tiene longitud $n+1$ y que cualquier máquina de Moore dá la salida $\lambda(q_o)$, en respuesta a la entrada θ.

Ahora estamos preparados para dar la equivalencia entre las maquinas de Moore y de Mealy.
Recordemos que si M y M' son maquinas de Moore y Mealy respectivamente, entonces podemos considerar $F_M(w)$ y $F_{M'}(w)$, para cada $w \in \sum^*$, y se tiene que $|F_{M'}(w)| < |F_M(w)|$ para cada $w \in \sum^*$. En consecuencia $F_M \neq F_{M'}$. Esto genera nuestro primer problema en cuanto al planteamiento de equivalencia entre las dos maquinas. A pesar de esto, podemos resolver nuestro problema observando la respuesta de la máquina de Moore en la entrada θ y decir que las maquinas M y M' son equivalentes si para toda entrada t se tiene que $bF_{M'}(t) = F_M(t)$, para algún $b \in \gamma$ de M, para su estado inicial.

Teorema 3.1.1 *Sea* $M_1 := (Q, \sum, \gamma, q_o, \delta_1, \lambda)$ *una máquina de Moore, entonces existe una máquina de Mealy* M_2 *equivalente a* M_1.

Prueba. Sea $M_2 = (Q, \sum, \gamma, \delta, \lambda', q_o)$, donde $\lambda' : Q \times \sum \longrightarrow \gamma$, es definida como $\lambda'(q, a) = \lambda(\delta(q, a))$, para todo $q \in Q$, $a \in \sum$. Con M_2 definida de esta manera se tiene entonces que M_1 y M_2 concluyen en la misma sucesión de estados con la misma entrada, y con cada transición M_2 emite la salida que M_1 asocia con el estado que ha entrado.

$\square$

Teorema 3.1.2 *Sea* $M_1 = (Q, \sum, \gamma, \delta, \lambda, q_o)$ *una máquina de Mealy. Entonces existe una máquina de Moore* M_2 *equivalente a* M_1

Prueba. Sea $M_2 = (Q \times \gamma, \sum, \gamma, \delta', \lambda', [q_o, b_o])$, donde b_o es un elemento arbitrario en γ. Definimos $\delta' : (Q \times \gamma) \times \sum \longrightarrow Q \times \gamma$ por $\delta'([q, r], a) = (\delta(q, a), \lambda(q, a))$ y definimos $\lambda' : Q \times \gamma \longrightarrow \gamma$ por $\lambda'([q, r]) = r$.

$\square$

Las funciones parciales definidas en el teorema 3.1.2 dicen que la segunda componente de un estado $[q, r]$ de M_2 es la salida realizada por M_1 en alguna transición en el estado q. Solamente la primera componente de los estados de M_2 determinan el movimiento hecho por M_2. Podemos afirmar que si M_1 entra a los estados $q_o, q_1, \ldots, q_n$ en la entrada $a_1 \ldots a_n$ y emite las salidas $b_1, b_2, \ldots, b_n$, entonces M_2 entra a los estados $[q_o, b_o], \ldots, [q_n, b_n]$ y emite las salidas $b_o, b_1, \ldots, b_n$.

Ejemplo 3.1.1 *Sea* M_1 *la máquina de Mealy de la figura* 3.1. *Podemos tomar* $b_o = n$ *y así* $[q_o, b_o]$ *es el estado inicial de* M_2. *Ahora por el teorema 3.1.2 los estados de* M_2 *son* $[q_o, y], [q_o, n], [p_o, y], [p_o, n], [p_1, y]$, $[p_1, n]$ *y atendiendo a las definiciones de* λ' *y* δ' *del teorema 3.1.2, tenemos que* M_2 *queda determinado por la figura* 3.2

En lo que sigue hablaremos indistintamente de Autómatas de Moore o Mealy, dada la equivalencia entre estas maquinas y nos referimos a estos solo como Autómatas finitos.

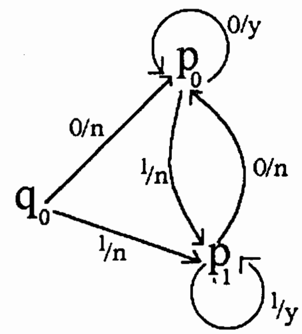

Figura 3.1:

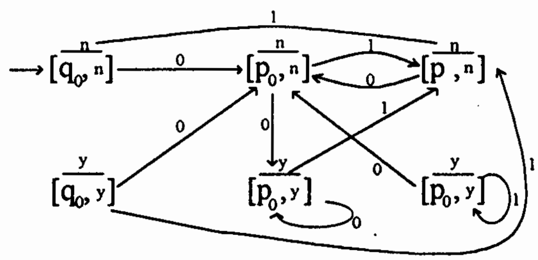

Figura 3.2:

3.2 Descripción del Comportamiento de un Autómata Finito

Definición 3.2.1 *Sean P una partición de $\sum^*$ e Y un conjunto finito. Una transformación de entrada-salida es una aplicación $F : \sum^*/P \longrightarrow Y$ biyectiva.*

Note que $\text{ind}(P) = |Y| < \infty$, pues F es una biyección. Podemos denotar entonces al número de clases de equivalencia por la relación P como $|\Sigma^*/P\,|$.

En lo que sigue asumiremos que los Autómatas de Moore son accesibles y que sus funciones de salidas son sobreyectivas.

Definición 3.2.2 *Sean* $M_1 = (Q_1, \sum, \gamma_1, \delta_1, \lambda_1, q_1)$ *y* $M_2 = (Q_2, \sum, \gamma_2, \delta_2, \lambda_2, q_2)$ *dos Autómatas finitos. Diremos que* M_1 *y* M_2 *son isomorfos si existen funciones biyectivas* $\varphi : Q_1 \longrightarrow Q_2$ *y* $\xi : \gamma_1 \longrightarrow \gamma_2$*, tales que:*

- (i) $\varphi(q_1) = q_2$
- (ii) $\varphi(\delta_1(q,r)) = \delta_2(\varphi(q), r)$ *, para todo* $q \in Q_1$, $r \in \sum$
- (iii) $\xi(\lambda_1(q)) = \lambda_2(\varphi(q))$ *, para todo* $q \in Q_1$.

Y diremos que el par (φ, ξ) *es un isomorfismo entre* M_1 *y* M_2*. Ahora, si* φ *es sobre, entonces diremos que el par* (φ, ξ) *es un homomorfismo de* M_1 *sobre* M_2*.*

Definición 3.2.3 *Un Autómata* M *es llamado simple (o Reducido) si cada homomorfismo de* M *es un isomorfismo.*

Definición 3.2.4 *Sea* (φ, ξ) *un homomorfismo de* M_1 *sobre* M_2 *tal que* M_1 *y* M_2 *tienen el mismo conjunto* γ*. Si* ξ *es la aplicación identidad de* γ*, diremos entonces que* φ *es un homomorfismo de estados y que* M_2 *es la imagen homomórfica de estados de* M_1*.*

Definición 3.2.5 *Sea* $M := (Q, \sum, \gamma, \delta, \lambda, q_o)$ *un Autómata finito. Dadas dos palabras de entrada* r_1 *y* r_2 *. Diremos que* r_1 *y* r_2 *son equivalentes, si y solo si,*

$$\lambda(\delta(q_o, r_1)) = \lambda(\delta(q_o, r_2)).$$

Podemos probar que la relación dada en la definición 3.2.5 es una relación de equivalencia sobre $\sum^*$ y la denotamos por P.

Consideremos ahora a $\sum^*/P$ y definamos $F : \sum^*/P \longrightarrow \gamma$ por

$$F(\bar{r}) = \lambda(\delta(q_o, r)).$$

Afirmación: F es una biyección. En efecto, si $F(\bar{r}) = F(\bar{r'})$, es decir, $\lambda(\delta(q_o, r)) = \lambda(\delta(q_o, r'))$, entonces r es equivalente a r' y asi, $\bar{r} = \bar{r'}$; en consecuencia F es inyectiva. La sobreyectividad de F es inmediata recordando que se ha supuesto que M es accesible y λ es sobre.

Definición 3.2.6 *Un Autómata* $M = (Q, \sum, \gamma, \delta, \lambda, q_o)$ *es llamado una Realización de una transformación de entrada-salida* $F : \sum^*/P \longrightarrow \gamma$, *si para todo* $r \in \sum^*$, $F(\bar{r}) = \lambda(\delta(q_o, r))$.

Proposición 3.2.1 *Si un Autómata* M_2 *es imagen isomorfica del Autómata* M_1, *entonces ellos inducen transformaciones de entrada-salida isomorficas.*

Prueba. Supongamos que un Autómata M_2 es imagen isomórfica de un Autómata M_1, digamos $M_1 = (Q_1, \sum, \gamma_1, \delta_1, \lambda_1, q_1)$ y $M_2 = (Q_2, \sum, \gamma_2, \delta_2, \lambda_2, q_2)$, entonces de la definición 3.2.2. se sigue que $\varphi(\delta_1(q_1, r)) = \delta_2(\varphi(q_1), r) = \delta_2(q_2, r)$ y $\lambda_2(\delta_2(q_2, r)) = \lambda_2(\delta_2(\varphi(q_1), r)) = \lambda_2(\delta_2(q_2, r)) = \lambda(\varphi(\delta_1(q_1, r))) = \xi(\lambda_1(\delta_1(q_1, r)))$, es decir, $(***)$ $\lambda_2(\delta_2(q_2, r)) = \xi(\lambda_1(\delta_1(q_1, r)))$.
Ahora, como ξ es biyectiva y $F_2(\bar{r}) = \xi\ (F_1(\bar{r}))$, entonces los Autómatas M_1 y M_2 inducen transformaciones de entrada-salida isomorficas.

□

Corolario 3.2.1 *Si* M_2 *es imagen isomorfica de estados de* M_1, *entonces* M_1 *y* M_2 *realizan la misma transformación de entrada-salida.*

Prueba. De la proposición 3.2.1. se sigue que

$$F_2(\bar{r}) = \lambda(\delta_2(q_2, r)) = \xi(\lambda_1(\delta_1(q_1, r))) = \lambda_1(\delta_1(q_1, r)) = F_1(\bar{r}).$$

Sea P una partición de $\sum^*$. Definamos una partición sobre $\sum^*$ denotada $m(P)$ como sigue: $r \equiv \beta(mod\, m(P)) \Longleftrightarrow$ para todo $z, rz \equiv \beta z(mod\ P)$, con $r, \beta, z \in \sum^*$.

□

Teorema 3.2.1 *Sea* P *una partición de* $\sum^*$. *Denotamos por* N_P *al conjunto de todos los Autómatas finitos* M *tal que la relación de equivalencia inducida por* M *sea igual a* P, *es decir,* $N_P = \{M\ A.F : R_M = P\}$.
Si $N_P \neq \emptyset$, *entonces* N_P *contiene un Autómata reducido* M_o, *único salvo isomorfismo, que es imagen homomórfica de cada elemento de* N_P.

Prueba. Supongamos que $N_P \neq \emptyset$, así $ind(P) < \infty$. Construimos M_o de la manera siguiente: escogemos a las clases $mod\ (m(P))$ como los estados, ponemos $q_o^* = [\theta]$, definimos $\delta_o : Q_o \times \sum \longrightarrow Q_o$ por $\delta_o(q, x) = \delta_o([p], x) =$

$[px]$, $p \in \sum^*, x \in \sum$.
La función de salida $\lambda_o : Q_o \longrightarrow \gamma$ la definimos por $\lambda_o(a) \equiv \lambda_o(b)$, solamente si $p \equiv q(mod(P))$, donde $a = [p]$ y $b = [q]$. Así, hemos construido $M_o := (Q_o, \sum, \gamma, \delta_o, \lambda_o, q_o^*)$ y claramente es único salvo isomorfismo.

Afirmación: M_o así definido está en N_P.
En efecto, por inducción se prueba que para cada $p \in \sum^*$, $\bar{p}$ corresponde a $\delta_o(q_o^*, p)$, así $p \equiv q\ (mod(P))$ y $\lambda_o(\delta_o(q_o^*, p)) = \lambda_o(\delta_o(q_o^*, q))$ son equivalentes.

Sea M un elemento arbitrario de N_P. Veamos que existe un homomorfismo de M sobre M_o. Para esto primero veamos que la función de transición δ satisface que $\delta(q_o, r)) = \delta(q_o, \beta) \Rightarrow r \equiv \beta\ mod(m(P))$

En efecto supongamos que el lado derecho de $(***)$, en la prueba de la proposición 3.2.1., es cierta, entonces $r \equiv \beta\ mod(P)$, pues $M \in N_P$. Además $\delta(q_o, r) = \delta(q_o, \beta)$ determina una congruencia a derecha de $\sum^*$, la cuál es un refinamiento de P. La asignación $\delta(q_o, r) \longrightarrow \delta_o(q_o^*, r)$ es una sobreyección de M sobre $M_o(\varphi : Q \longrightarrow Q_o)$.

Finalmente, sea M_o' imagen homomorfica de M_o y denotemos su conjunto de estados como Q_o', entonces $|Q_o'| \leq |Q_o|$; por otro lado, $M_o' \in N_P$ implica que $|Q_o'| \geq |Q_o|$, de acá que $|Q_o'| = |Q_o|$ lo cuál es contradictorio, salvo que M_o' y M_o sean isomorfos, por tanto M_o es reducido o simple.

□

Corolario 3.2.2 *Sea* $F : \sum^*/P \longrightarrow Y$ *una tranformación de entrada-salida arbitraria. Entonces las siguientes condiciones son equivalentes:*

- (i) $ind(m(P)) < \infty$
- (ii) *Existe un A.F. realizando* F.
- (iii) *Existe un A.F. reducido (único salvo isomorfismo) realizando* F.

Prueba. Es dejada como ejercicio. □

Definición 3.2.7 *Una partición* P *de* $\sum^*$ *es llamada hiperfina si* $m(P)$ *es de índice finito.*

Definición 3.2.8 *Si el par* (φ, ξ) *es un isomorfismo y un homomorfismo de estados, diremos que* (φ, ξ) *es un isomorfismos de estados.*

Lema 3.2.1 *Supongamos que* M_1 *y* M_2 *son dos Autómatas isomorfos, los cuales inducen la misma transformación de entrada-salida. Entonces* M_1 *y* M_2 *determinan un isomorfismo de estados.*

Prueba. Pongamos $M_1 = (Q_1, \sum, \gamma, \delta_1, \lambda_1, q_1)$, $M_2 = (Q_2, \sum, \gamma, \delta_2, \lambda_2, q_2)$, $\varphi : Q_1 \longrightarrow Q_2$ y $\xi : \gamma \longrightarrow \gamma$.

Sea $r \in \sum^*$ y sea p el estado $p = \delta_1(q_1, r)$, entonces

$$\begin{aligned}
\lambda_1(p) &= \lambda_1(\delta_1(q_1, r)) = F_1(\bar{r}) = F_2(\bar{r}) \\
&= \lambda_2(\delta_2(q_2, r)) = \lambda_2(\delta_2(\varphi(q_1), r)) \\
&= \lambda_2(\varphi(\delta_1(q_1, r))) = \lambda_2(\varphi(p)) \\
&= \xi(\lambda_1(p)).
\end{aligned}$$

Así, ξ es la transformación identidad. En consecuencia M_1 y M_2 determinan un isomorfismo de estados.

□

Definición 3.2.9 *Dos estados* p *y* q *de un Autómata* M *son llamados distinguibles, si existe* $r \in \sum^*$ *tal que* $\lambda(\delta(p, r)) \neq \lambda(\delta(q, r))$. *En caso contrario,* p *y* q *son llamados indistinguibles.*

Es fácil probar que la relación de indistinguibilidad dada en la definición 3.2.9. es de equivalencia y será denotada por π_{max}.

3.3 Códigos y Precódigos

En lo sucesivo N_i^j denotará el conjunto de los enteros entre i y $j (i \leq j)$ (ambos inclusive), es decir, $N_i^j = \{x \in \mathbb{Z} \ : \ i \leq x \leq j\}$
Claramente la cardinalidad de N_i^j, denotada por $|N_i^j|$, es $j - i + 1$.

Definición 3.3.1 *Un precódigo es un sextuple* $D = (r, s, \beta, \vartheta, \mu, \varphi)$*, donde* r *y* s *son enteros no negativos y* β, ϑ, μ *y* φ *son funciones con dominios y contradominios (también llamados objetivos) especificados como sigue:*

$$\begin{array}{ll} \beta : N_2^{r+s+1} \longrightarrow N_1^{r+1}, & \vartheta : N_2^{r+s+1} \longrightarrow N_1^{n}, \\ \mu : N_1^{r+1} \longrightarrow N_1^{r+1}, & \varphi : N_{r+2}^{r+s+1} \longrightarrow N_1^{r+1}. \end{array}$$

Estas funciones satisfacen las siguientes condiciones:

- (i) $\beta(2) = 1$. Si $i \in N_3^{r+1}$, entonces valen $(a) \wedge [(b) \vee (c)]$, donde

$$\begin{array}{ll} (a) & \beta(i-1) \leq \beta(i) < i, \\ (b) & \beta(i-1) < \beta(i), \\ (c) & \vartheta(i-1) < \vartheta(i), \end{array}$$

- (ii) Si $i \in N_1^{r+1}$, entonces

$$\mu(i) - 1 \in \{0, \mu(1), \mu(2), \ldots, \mu(i-1)\}$$

- (iii) Si $i \in N_{r+2}^{r+s+1}$, entonces $(\beta(i), \vartheta(i))$ es el par más pequeño, lexicográficamente, para el cuál

$$j \in N_2^{i-1} \Longrightarrow (\beta(i) \neq \beta(j)) \vee (\vartheta(i) \neq \vartheta(j)) \text{ para cada } j.$$

- (iv) Si $i \in N_{r+2}^{r+s+1}$, entonces se tiene $\varphi(i) = 1$ ó $(d) \wedge [(e) \vee (f)]$, donde

$$\begin{array}{ll} (d) & \beta(\varphi(i)) \leq \beta(i) \\ (e) & \beta(\varphi(i)) < \beta(i) \\ (f) & \vartheta(\varphi(i)) < \vartheta(i) \end{array}$$

Observación 3.2 *Cualquier precódigo puede representarse en una tabla de tamaño* $(r+s+1)\times 4$ *(filas y columnas), en la cuál se especifícan los valores* $\beta(i)$*,* $\vartheta(i)$*,* $\mu(i)$ *y* $\varphi(i)$*, para cada* i*, de acuerdo a sus respectivos dominios.*

Ejemplo 3.3.1 *A continuación se muestra un precódigo en una tabla bidimensional para* $n = 2$*,* $r = 5$*,* $s = 7$*.*

i	$\beta(i)$	$\vartheta(i)$	$\mu(i)$	$\varphi(i)$
1	$-$	$-$	1	$-$
2	1	1	2	$-$
3	1	2	1	$-$
4	2	1	3	$-$
5	2	2	2	$-$
6	3	2	4	$-$
7	3	1	$-$	4
8	4	1	$-$	2
9	4	2	$-$	1
10	5	1	$-$	3
11	5	2	$-$	5
12	6	1	$-$	6
13	6	2	$-$	1

Proposición 3.3.1 *Si las formulas* $i \in N_2^{r+s+1}$, $j \in N_2^{r+s+1}$, $\beta(i) = \beta(j)$ *y* $\vartheta(i) = \vartheta(j)$ *son validas (para un precódigo), entonces* $i = j$.

Demostración. Procediendo por el absurdo veamos que $2 \leq j < i \leq r + s + 1$.
Implica que $\beta(i) \neq \beta(j) \vee \vartheta(i) \neq \vartheta(j)$.

Caso 1. $i \leq r + 1$. Si $\beta(j) = \beta(i)$, entonces tenemos que $\beta(i) = \beta(i-1) = \beta(i-2) = \ldots = \beta(j)$ y $\vartheta(i) > \vartheta(i-1) > \ldots > \vartheta(j)$.

Caso 2. $i \geq r+2$. De (iii) inmediatamente se sigue que $2 \leq j < i \leq r+s+1$ implica que $\beta(i) \neq \beta(j) \vee \vartheta(i) \neq \vartheta(j)$.

Sean $D_1 = (r_1, s_1, \beta_1, \vartheta_1, \mu_1, \varphi_1)$ y $D_2 = (r_2, s_2, \beta_2, \vartheta_2, \mu_2, \varphi_2)$ dos precodigos. Sea la relación $D_1 < D_2$ es verdadera si $(r_1 \leq r_2 \wedge s_1 = 0) \vee (r_1 = r_2 \wedge s_1 \leq s_2)$ y $\beta_2, \vartheta_2, \mu_2, \varphi_2$ es una extensión de $\beta_1, \vartheta_1, \mu_1, \varphi_1$ respectivamente. La relación $<$ es una relación de orden parcial sobre todos los precódigos (n es fijo). Si $D_1 < D_2$ y $r_1 + s_1 + 1 = r_2 + s_2$ se tienen, entonces escribiremos $D_1 \alpha D_2$ (esto significa que tenemos D_1 si borramos la última fila de D_2).

□

Observación 3.3 *Se puede demostrar que* $s \leq rn + n - r$ *es válida para cada precódigo; igualmente se tiene para los códigos y solamente para ellos.*

Definición 3.3.2 *Si* D_1 *es un precódigo y no existe precódigo* D_2 *con* $D_1 < D_2$*, entonces a* D_1 *se le llamará código.*

Es fácil verificar que el precódigo del ejemplo 3.3.1. es un código.
Sea $C = (r, s, \beta, \vartheta, \mu, \varphi)$ un código arbitrario. Determinamos un Autómata $\psi(c) = A = (A, X, Y, \delta, \lambda, a^*)$ por las reglas siguientes de (a) a (e).

- (a) $A = \{a_1, a_2, \ldots a_{r+1}\}$
- (b) $a^* = a_1$ es el estado inicial de A.
- (c) $Y = \{y_1, y_2, \ldots, y_t\}$, donde $t = max(\mu(1), \mu(2), \ldots, \mu(r+1))$
- (d) Para cada $i\ (\in N_2^{r+s+1})$, definimos δ por

$$\delta(a_{\beta(i)},\ x^{(\vartheta(i))}) = \begin{cases} a_i & ,\text{si } i \leq r+1 \\ a_{\varphi(i)} & ,\text{si } i \geq r+2 \end{cases}$$

- (e) Para cada $i\ (\in N_2^{r+1})$, definimos λ por $\lambda(a_i) = y_{\mu(i)}$.

Observación 3.4 *La transición* δ *es consistente y está bien definida pues* (iii) *fué estipulada, la proposición 3.3.1. se tiene y* C *es un código.*

Observación 3.5 *Si* $D < C$ *es válida para un precódigo* D*, entonces podemos asignar a* D *un sub-Autómata parcial de* $\psi(c)$ *de una manera natural.*

3.4 Nociones de Complejidad

Como hemos visto, los códigos dan una descripción de todos los A.F's. de Moore. La noción de código está demasiado extendida, por lo tanto queremos restringir nuestra atención a los códigos C, para los cuales los Autómatas $\psi(c)$ son simples.

Sean a y b dos estados de un A.F de Moore A. Entenderemos por el número de distinguibilidad $w(a,b)$ de a y b, la longitud $|p|$ de la palabra más corta p, tal que $\lambda(\delta(a,p)) \neq \lambda(\delta(b,p))$.
(Por supuesto, $w(a,b) = \infty$ si $\lambda(\delta(a,p)) = \lambda(\delta(b,p))$, para todo $p(\in \sum^*)$. Evidentemente, $w(a,a) = \infty$ y también $w(a,b) = w(b,a)$ valen. Convendremos que máx $w(a,b)$ se llama complejidad del Autómata A, y la denotaremos por $\Omega_A(A)$; acá (a,b) recorre todos los pares de estados de A, tales que $a \neq b$ ($\Omega_A(A) = 0$, si A tiene un solo estado). La complejidad de un código se define por

$$\Omega_C(C) = \Omega_A(\psi(C))$$

Lema 3.4.1 *Si a, b y c son estados arbitrarios de un A.F., entonces $w(b,c) \geq min\ \{w(a,b), w(a,c)\}$.*

Prueba. Sea p la palabra más corta tal que $\lambda(\delta(b,p)) \neq \lambda(\delta(c,p))$.

Denotemos $\lambda(\delta(a,p))$ por y_a, la notación y_b y y_c tienen significado análogo. Si $y_a \neq y_b$, entonces $w(a,c) \leq w(b,c)$.

□

Proposición 3.4.1 *Sea $a_1, a_2,$ y a_3 estados arbitrarios de un A.F. de Moore. Entonces, existe una permutación π del conjunto $\{1,2,3\}$, tal que $w(a_{\pi(1)}, a_{\pi(2)}) = w(a_{\pi(2)}, a_{\pi(3)}) \leq w(a_{\pi(1)}, a_{\pi(3)})$.*

Prueba. Obviamente existe una permutación π que satisface $w(a_{\pi(1)}, a_{\pi(2)}) = w(a_{\pi(2)}, a_{\pi(3)}) \leq w(a_{\pi(1)}, a_{\pi(3)})$. Si $w(a_{\pi(1)}, a_{\pi(2)}) < w(a_{\pi(2)}, a_{\pi(3)})$ es verdadera, entonces tenemos una contracción con el lema 3.4.1. (con $a = a_{\pi(3)}$, $b = a_{\pi(2)}$, $c = a_{\pi(1)}$).

□

Lema 3.4.2 *Sean b y c dos estados de un A.F A. $w(b,c) = \infty \Longleftrightarrow$ existe un homomorfismo (α_A, α_Y) de A tal que $\alpha_A(b) = \alpha_A(c)$.*

Prueba. Necesidad. Supóngase que $w(b,c) = \infty$. Introcucimos una operación binaria Λ (que depende de b y c) en el conjunto de estados de

A como sigue: $\Lambda(a, a^+)$ es verdadera precisamente cuando existe una sucesión de estados $(a =)a_o, a_1, a_2, \ldots, a_k(= a^+)$ y una sucesión de palabras $p_1, p_2, \ldots, p_k$ (k es común) tal que $\{\delta(b, p_i), \delta(c, p_i)\} = \{a_{i-1}, a_i\}$ se tiene para cada escogencia de $i(1 \leq i \leq k)$.
Podemos demostrar que Λ es una relación de equivalencia; esto determina una partición R del conjunto de estados. El Autómata factor con respecto a R puede introducirse de una manera consecuente. De aquí el par (α_A, α_Y), donde α_A es la asignación natural asociada a la partición y α_Y es la permutación identidad del alfabeto de salida, es un homomorfismo.

$$\lambda'(\alpha_A(\delta(b,p))) = \lambda(\delta'(\alpha_A(b),p)) = \lambda(\delta'(\alpha_A(c),p)) = \lambda'(\alpha_A(\delta(c,p))),$$

donde δ' y λ' significa lo mismo en la imagen homomórfica. Para cada escogencia de p, consecuentemente $\lambda(\delta(b,p)) = \lambda(\delta(c,p))$, ya que $\alpha_{\underline{Y}}$ es una biyección.

□

Proposición 3.4.2 *Sea A un A.F. de Moore. Entonces A es simple, si y solo si $\Omega_A(A) < \infty$.*

Prueba. Consideremos las siguientes afirmaciones:

- (i) A no es reducible.
- (ii) A tiene un homomorfismo que no es isomorfismo
- (iii) A tiene dos estados diferentes b y c y un homomorfismo (α_A, α_Y) tal que $\alpha_A(b) = \alpha_A(c)$.
- (iv) A tiene dos estados diferentes b y c tal que $w(b,c) = \infty$.
- (v) $\Omega_A(A) = \infty$

Las equivalencias $(i) \Longleftrightarrow (ii)$, $(ii) \Longleftrightarrow (iii)$, $(iv) \Longleftrightarrow (v)$, son evidentes. La equivalencia $(iii) \Longleftrightarrow (iv)$ se estableció en lema 3.4.2. De aquí (i) y (v) son equivalentes.

□

Proposición 3.4.3 *Las siguientes condiciones son equivalentes, donde A es un A.F. de Moore.*

- (a) *La función de salida* λ *de* A *es una biyección.*
- (b) $\Omega_A(A) = 0$.

Prueba. (b) y (a) son equivalentes del hecho evidente de que las proposiciones $\lambda(a) \neq \lambda(b)$ y $w(a,b) = 0$ son equivalentes (a y b son estados diferentes de A).

□

3.5 Ejercicios Propuestos

Ejercicio 3.5.1 Dada una máquina de Moore M. Dé la regla para la función parcial computada por $M\,F_M$ y la función de salida extendida λ.

Ejercicio 3.5.2 Pruebe que un A.F.D. es un caso especial de una máquina de Moore, donde el alfabeto de salida es $\{0,1\}$ y que el estado q es aceptado, si y solo si, $\lambda(q) = 1$.

Ejercicio 3.5.3 Probar lo siguiente:
(i) $m(P) \subseteq P$.
(ii) $m(P)$ es invariante a la derecha.
(iii) $P^* \subseteq P$ implica que $P^* \subseteq m(P)$, para cada P^* invariante a derecha de $\sum^*$.

Ejercicio 3.5.4 Pruebe que $N_P \neq \emptyset$ (en el teorema 3.2.1) implica que $ind(P) < \infty$.

Ejercicio 3.5.5 Pruebe el corolario 3.2.2.

Ejercicio 3.5.6 Sea $\sum = \{r\}$, $\gamma = \{r, \tau\}$. Considere la máquina de Mealy de la figura siguiente, donde $Card(Q) = n$.

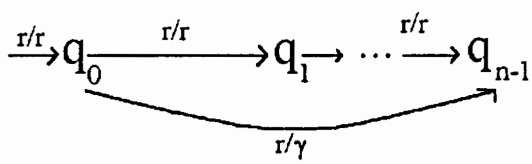

Figura 3.3:

$$\text{Pruebe que}\quad \lambda(q_i, r^j) = \begin{cases} r^j & ,\text{ si } i+j < n \\ r^{j-1}\tau & ,\text{ si } i+j = n \end{cases},$$

Calcule $F_M(r^k)$ y encuentre un Autómata de Moore equivalente a M.

$$(k = pn + u,\ 0 \leq u < n,\ p \geq 0,\ p \in \mathbb{Z})$$

Ejercicio 3.5.7 Sea $\sum = \gamma = \{r, \tau\}$. Considere la máquina de Mealy M dada por la figura

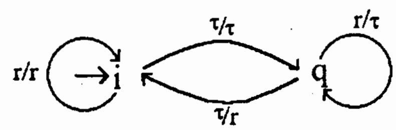

Figura 3.4:

Encuentre una máquina de Moore M' equivalente a M.

Ejercicio 3.5.8 Sean $\sum = \{a, b, c\}$, $\gamma = \{x, y\}$. Encuentre una máquina de Moore equivalente a la máquina de Mealy dada en la figura 3.5.8

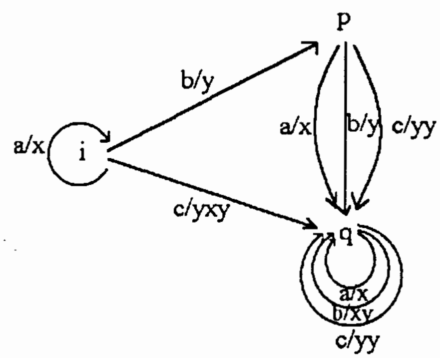

Figura 3.5:

Capítulo 4

Comportamiento al Infinito de los Autómatas Finitos

En éste capítulo consideraremos el comportamiento de los Autómatas finitos con entradas infinitas, es decir, con entradas que son sucesiones en el sentido topológico y cuyos valores estan en algún alfabeto $\sum$. Veremos que el conjunto de todas las sucesiones en el alfabeto dado $\sum$ es un espacio métrico, lo cuál nos proveerá de una noción importante para determinar propiedades de continuidad en las aplicaciones secuenciales.

4.1 El Conjunto $\sum^{\mathbb{N}}$

Si $\sum$ es un alfabeto finito, entonces podemos considerar el conjunto $\{x/x : \mathbb{N} \longrightarrow \sum\}$; denotaremos este conjunto por $\sum^{\mathbb{N}}$, es decir, $\sum^{\mathbb{N}}$ es el conjunto de todas las sucesiones en $\sum$. También podemos identificar las x en $\sum^{\mathbb{N}}$, como $x := x(0)x(1)\ldots x(n)\ldots$ o $x := x_0x_1x_2\ldots x_n\ldots$.

Definición 4.1.1 *Sean $x \in \sum^{\mathbb{N}}$ y $n \in \mathbb{N}$. Llamaremos a x_n el $(n+1)-$ésimo elemento de x y a $x^n = x_0x_1\ldots x_{n-1} \in \sum^*$ el segmento inicial de x de longitud n. Si $n = o$, convendremos que $x^o = \theta$.*

Definición 4.1.2 *Sea $u \in \sum^*$. Diremos que u es un prefijo de $x \in \sum^{\mathbb{N}}$ si existe $n \in \mathbb{N}$ tal que $u = x^n$. En este caso pondremos $u \underline{\alpha}\, x$.*

Proposición 4.1.1 *Dada una sucesión creciente* $u_1 < u_2 < \ldots < u_n < \ldots$ *de elementos de* $\sum^*$, *existe un único elemento* $x \in \sum^{\mathbb{N}}$ *tal que* $x^j = u_k$, *con* $j = |u_k|$, *para todo* $k \in \mathbb{N}$.

Prueba. La sucesión $x : \mathbb{N} \longrightarrow \sum$, definida por $x_j = x(j) = u_k(j) \in \sum$ satisface la proposición.

□

Llamaremos a x el limite de $\{u_k\}$. En particular, para cada $x \in \sum^{\mathbb{N}}$,
$x = \lim_{n\to\infty} x^n$.
Definimos ahora una multiplicación externa en $\sum^{\mathbb{N}}$, $\cdot : \sum^* \times \sum^{\mathbb{N}} \longrightarrow \sum^{\mathbb{N}}$ definida por

$$u \cdot w = \begin{cases} u(i) & , si \;\; i \leq |u| \\ w(i - |u|) & , si \;\; |u| < i \end{cases}$$

y pondremos simplememte uw. Nótese que uw también se puede definir por $uw = \lim_{n\to\infty} uw^n$.
Nuestro próximo paso consiste en definir una distancia sobre $\sum^{\mathbb{N}}$. Para esto definimos sobre $\sum^{\mathbb{N}}$ una aplicación $\rho : \sum^{\mathbb{N}} \times \sum^{\mathbb{N}} \longrightarrow \mathbb{R}$ dada por

$$\rho(x,y) = \begin{cases} 1/j, & si \;\; x^{j-1} = y^{j-1}, x^j \neq y^j \\ 0, & si \;\; x = y \end{cases} \tag{4.1}$$

la cuál, se puede probar, es una métrica sobre $\sum^{\mathbb{N}}$ y así el par $(\sum^{\mathbb{N}}, \rho)$ es un espacio métrico.

Proposición 4.1.2 *Para cada* $x \in \sum^{\mathbb{N}}$ *y cada entero* $k \geq 0$, x *puede ser expresada como* $x = ux'$, *con* $u \in \sum^*$ *y* $x' \in \sum^{\mathbb{N}}$, *con* $|u| = k$.

Prueba. Basta tomar $u = x^k$. □

El elemento x' de la proposición 4.1.2, se le llamará k- truncación de x y será denotado por $\tau^k(x)$.

Sea $F : \sum^* \longrightarrow \gamma^*$ una función que satisface:

- (i) F preserva el segmento inicial

- (ii) Para todo $r \in \sum^*$, $|r| \leq |F(r)|$

Una función con ésta propiedad, induce una función $F^{\mathbb{N}} : \sum^{\mathbb{N}} \longrightarrow \gamma^{\mathbb{N}}$, definida por $F^{\mathbb{N}}(x) = \lim_{n\to\infty} F(x^n)$ y ésta es llamada la prolongación o extensión de F. Afirmamos que $F^{\mathbb{N}}$ es continua. En efecto, si $\rho(x,y) < 1/n$, entonces $x^n = y^n$ y así $F(x^n) = F(y^n)$, de donde $\lim_{n\to\infty} F(x^n) = \lim_{n\to\infty} F(y^n)$, es decir, $F^{\mathbb{N}}(x) = F^{\mathbb{N}}(y)$, por tanto $[F^{\mathbb{N}}(x)]^n = [F^{\mathbb{N}}(y)]^n$. En consecuencia $\rho(F^{\mathbb{N}}(x), F^{\mathbb{N}}(y)) < 1/n$, es decir $F^{\mathbb{N}}$ es continua.

Recordando ahora que si tenemos un Autómata de Moore o Mealy, la función F_M preserva segmentos iniciales y para todo $r \in \sum^*$, $|r| \leq |F(r)|$, entonces F_M induce una aplicación $F_M^{\mathbb{N}} : \sum^{\mathbb{N}} \longrightarrow \gamma^{\mathbb{N}}$ que es continua. Las funciones que se obtienen de esta manera serán llamadas SECUENCIALES.

Podemos establecer una biyección entre $\sum^{\mathbb{N}}$ y $(\sum^k)^{\mathbb{N}}$ para todo $k \geq 1$ como sigue: si $x \in \sum^{\mathbb{N}}$, entonces particionamos a $x = x_0 x_1 \ldots x_k x_{k+1} \ldots x_{2k-1} x_{2k} \ldots$ en bloques de longitud k, y así obtenemos un elemento x' en $(\sum^k)^{\mathbb{N}} = (\sum^{\mathbb{N}}, \sum^{\mathbb{N}}, \ldots, \sum^{\mathbb{N}})$. Se puede probar que esta aplicación es una biyección que es un homomorfismo, por tanto $(\sum^k)^{\mathbb{N}} \cong \sum^{\mathbb{N}}$.

4.2 Sucesiones Fundamentalmente Periodicas

Definición 4.2.1 *Una sucesión $x : \mathbb{N} \longrightarrow \sum$ es llamada periódica si existe un entero $p > 0$ tal que $x(n+p) = x(n)$, para todo $n \in \mathbb{N}$.*

En la definición 4.2.1, poniendo $S = x^p \in \sum^+ = \sum^* \backslash \{\theta\}$, se tiene obviamente que $x = \lim_{n\to\infty} (S)^n$.

Definición 4.2.2 *Una sucesión $x \in \sum^{\mathbb{N}}$ será llamada fundamentalmente periódica, si existen enteros $p > 0$, $M_o \geq 0$ tal que $x(n+p) = x(n)$, para todo $n \geq M_o$.*

Nótese que la definición 4.2.2, es equivalente a decir que $x = t \lim_{n\to\infty}(S)^n$ para algún $t \in \sum^*$, $S \in \sum^*$.

Proposición 4.2.1 *La sucesión* $x : I\!N \longrightarrow \sum$ *es fundamentalmente periódica, si y solo si, para cada* $r \in \sum$ *el conjunto* $A_r = \{n/x(n) = r\} = x^{-1}(r)$ *es un subconjunto regular de* $I\!N$.

Prueba. Supongamos que x es fundamentalmente periódica, es decir, $x(n + p) = x(n)$, para algún $p > 0$ y todo $n \geq n_o$ (p y n_o los de la definición). Entonces, $n + p \in A_r$, si y solo si, $n \in A_r$, para todo $n \geq n_o$. Luego por el ejercicio propuesto 4.3.8 en la sección de ejercicios correspondiente a éste capítulo, tenemos que A_r es regular.

Recíprocamente, suponga que cada A_r es regular, es decir, es fundamentalmente periódica. Entonces existen enteros $p_r > 0$ y $n_r > 0$ tal que $n + p_r \in A_r$, si y solo si, $n \in A_r$, para todo $n \geq n_r$. Ahora, si p es el mínimo común múltiplo de los enteros p_r y n_o y tomamos el máximo de los n_r, entonces para todo $r \in \sum$, $n + p \in A_r$, si y solo si, $n \in A_r$, para todo $n \geq n_o$, así A_r es fundamentalmente periódica, es decir, $x(n + p) = x(n)$, para todo $n \geq n_o$, en consecuencia x es fundamentalmente periódica.

□

Definición 4.2.3 *Sea* $A \subseteq \sum^*$, *llamaremos la clausura de* A, *denotada* $\overline{A}$, *al conjunto* $\overline{A} := \{x : x \in \sum^{I\!N}, x^j \in A$ *para infinitos* $j \in I\!N\}$.

Observación 4.1 *Note que* $x \in \overline{A}$, *si y solo si,* $x = \lim_{n\to\infty} a_n$, *con* $\{a_n\}$ *una sucesión creciente en* A.

Definición 4.2.4 *Sea* $M = (Q, \sum, \delta, q_o, F)$ *un A.F. y sea* $x \in \sum^{I\!N}$. *Una trayectoria en* M, *con etiqueta* x, *es una sucesión* $P : I\!N \longrightarrow Q$, *tal que* $P_n \xrightarrow{x_n} P_{n+1}$ *es un arco en* M, *para cada* $n \in I\!N$.

Definición 4.2.5 *Sea* P *una trayectoria en un A.F.* $M = (Q, \sum, \delta, q_o, F)$, *y sea* $I_n(P) := \{q : q \in Q,\ q = P_n$ *para infinitos* $n \in I\!N\}$. *Diremos que la trayectoria* P *es aceptada por* M *si* $P_o = q_o$ *y* $I_n(P) \cap F \neq \emptyset$.

Denotemos por $||M||$ al conjunto de todas las etiquetas de trayectorias aceptadas por M, es decir, $||M|| = \{x \in \sum^{\mathbb{N}} :$ existe una trayectoria en M etiquetada x que es aceptada por $M\}$.

Proposición 4.2.2 *Para cada Autómata M se tiene que*

$$||M|| \subseteq \overline{Lac(M)}.\ \textit{Más aún, si } M \textit{ es un A.F.D. entonces}$$

$$||M|| = \overline{Lac(M)}.$$

Prueba. Sea $M = (Q, \sum, \delta, q_o, F)$ un A.F. y sea P una trayectoria con etiqueta $x \in \sum^{\mathbb{N}}$ que es aceptada por M, entonces $P_o = q_o$ y $I_n(P) \cap F \neq \emptyset$.
Ahora, para cada $n \in \mathbb{N}$, tenemos obviamente que

$q_o \xrightarrow{x_o} P_1 \xrightarrow{x_1} P_2 \xrightarrow{x_2} \ldots \xrightarrow{x_{n-1}} P_n$ es aceptada por M y su etiqueta es x^n. Por tanto $x^n \in Lac(M)$ para infinitos $n \in \mathbb{N}$, de donde $x \in \overline{Lac(M)}$, luego $||M|| \subseteq \overline{Lac(M)}$. Finalmente, si M es un A.F.D. y $x \in \overline{Lac(M)}$, entonces $x^n \in Lac(M)$ para infinitos $n \in \mathbb{N}$. Ahora, poniendo $P_j = \delta(q_o, x^j)$ para cada $j \in \mathbb{N}$, tenemos una trayectoria P aceptada por M con etiqueta x. Por tanto, $x \in ||M||$ y así $||M|| = \overline{Lac(M)}$.

$\square$

4.3 Ejercicios Propuestos

Ejercicio 4.3.1 Pruebe que ρ es una métrica en $\sum^{I\!N}$, donde ρ es la función [4.1] definida en $\sum^{I\!N}$

Ejercicio 4.3.2 Pruebe que para todo $a \in \sum^*$ fijo, la función $\varphi : \sum^{I\!N} \longrightarrow \sum^{I\!N}$ definida por $\varphi_u(x) = ux$ es continua.

Ejercicio 4.3.3 Pruebe lo siguiente:
(a) $\rho(x_1, x_2) < \frac{1}{n+k} \Longrightarrow \rho(\tau^k(x_1), \tau^k(x_2)) < \frac{1}{n}$
(b) La aplicación $\tau^k : \sum^{I\!N} \longrightarrow \sum^{I\!N}$ es continua.

Ejercicio 4.3.4 Pruebe que $\sum^{I\!N}$ es un espacio topológico compacto, es decir, cada sucesión infinita de elementos de $\sum^{I\!N}$ contiene una subsucesión convergente. Pruebe que la topología de $\sum^{I\!N}$ dada por la distancia ρ, coincide con la topología del producto cartesiano de $\sum^{I\!N}$, visto como producto de una sucesión de copias del espacio discreto $\sum$.

Ejercicio 4.3.5 Dada una función $F : \sum^{I\!N} \longrightarrow \gamma^{I\!N}$, y dado $u \in \sum^*$ definamos $F_o u : \sum^{I\!N} \longrightarrow \gamma^{I\!N}$ por $(F_o u)(s) = F_o \tau^{|u|}(us)$. Pruebe que:
(i) $F_o \theta = F$; $F_o(uv) = (F_o u)_o v$;
(ii) si F es continua, entonces $F_o u$ es continua.

Ejercicio 4.3.6 Llamamos a la función $F : \sum^{I\!N} \longrightarrow \gamma^{I\!N}$ finita si la familia de funciones $\{F_o u / u \in \sum^*\}$ es finita. Pruebe que F es secuencial, si y solo si, F es finita y se tiene que $\rho(F(x), F(y)) \leq \rho(x, y)$ para todo $x, y \in \sum^{I\!N}$.

Ejercicio 4.3.7 Pruebe que para cada función $F : \sum^{I\!N} \longrightarrow \gamma^{I\!N}$ las propiedades siguientes son equivalentes:
(i) F es finita y continua.
(ii) F es finita y existe un entero $k \geq 1$ tal que $\rho(x, y) < \frac{1}{n+k}$ implica que $\rho(F(x), F(y)) < \frac{1}{n}$.
(iii) $F = q\tau$, donde $q : \sum^{I\!N} \longrightarrow \gamma^{I\!N}$ es secuencial y $k \geq 1$ es un entero.

Ejercicio 4.3.8 Pruebe que para cualquier subconjunto A de $\mathbb{N}$, las condiciones siguientes son equivalentes:
(i) A es regular.
(ii) A es fundamentalmente periódica, es decir, existen enteros $n_o, p \in \mathbb{N}$ tal que $n \in A \Longleftrightarrow n + p \in A$, para todo $n \geq n_o$.

Ejercicio 4.3.9 Sea $F : \sum^{\mathbb{N}} \longrightarrow \gamma^{\mathbb{N}}$ una función secuencial. Si $x \in \sum^{\mathbb{N}}$ es fundamentalmente periódica, entonces $F(x) \in \gamma^{\mathbb{N}}$ es fundamentalmente periódica.

Ejercicio 4.3.10 Si $A, B \subseteq \sum^*$, entonces $\overline{A \cup B} = \overline{A} \cup \overline{B}$.

Ejercicio 4.3.11 Sea $\sum = \{r, \tau\}$ y sea $A \subseteq \sum^{\mathbb{N}}$, con $A = \sum^* r\tau^w$, donde τ^w denota una sucesión infinita. Considere el A.F. M de la figura 4.1, pruebe que $\|M\| = A$

Figura 4.1:

Ejercicio 4.3.12 Sean $\sum = \{r, \tau\}$, $F = \{p, q\}$. Considere el A.F. de la figura 4.2, hallar $\|M\|$

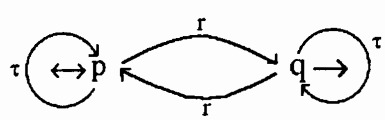

Figura 4.2:

Ejercicio 4.3.13 Pruebe que para cualquier subconjunto A de $\sum^{\mathbb{N}}$ las condiciones siguientes son equivalentes:
(i) A es un abierto en $\sum^{\mathbb{N}}$
(ii) $A = B\sum^{\mathbb{N}}$, para algún $B \subseteq \sum^*$.

Capítulo 5

Generalización de los A.F's y Sistemas Lineales con Ecuaciones de Lenguajes

En este capítulo generalizamos la noción de Autómata finito, dada en el capítulo 1, e introducimos un método eficiente algebraico para determinar el comportamiento de estos, el cuál depende del estudio de las ecuaciones lineales. Para ello damos algunas definiciones algebraicas y algunos otros conceptos que nos permitiran la construcción de tal método.

5.1 K-Subconjuntos

.

Definición 5.1.1 *Un semianillo* K *es un triple* $(k, +, .)$, *donde* K *es un conjunto no vacío,* $(K, +)$ *es un monoide conmutativo (para* $x, y \in K$, $x + y = y + x$*) con unidad* 0, $(K, .)$ *es un monoide con unidad* $\mathbf{1}$ *y se tienen los siguientes axiomas: para* $x, y, z \in K$,

- (i) $x \cdot (y + z) = x \cdot y + x \cdot z$,
- (ii) $(x + y) \cdot z = x \cdot z + y \cdot z$, *y*
- (iii) $x \cdot 0 = 0 \cdot x = 0$

Ejemplo 5.1.1 $B = \{0,1\}$ *con la adición dada por* $1+1=1$, $0+0=0$, y $1+0=0+1=1$ *y con la multiplicación dada por* $1\cdot 1=1$ y $1\cdot 0 = 0\cdot 1 = 0\cdot 0 = 0$ *es un semianillo.*

Ejemplo 5.1.2 $I\!N = \{0,1,2,3,\ldots\}$ *con la suma y la multiplicación usual es un semianillo.*

Consideremos la familia $\{x_i : i \in I\}$ de elementos de un semianillo K. Si I es finito, entonces la suma (5.1) $\sum_{i\in I} x_i$ es definida y es un elemento de K. Esta suma tiene las siguientes propiedades:

(5.2) Si I tiene un solo elemento i, entonces $\sum_{i\in I} x_i = x_i$

(5.3) Si $I = \bigcup_{j\in J} I_j$ es una partición disjunta de I, entonces

$$\sum_{i\in I} x_i = \sum_{j\in J}\left(\sum_{i\in I_j} x_i\right),\quad z.\left(\sum_{i\in I} x_i\right) = \sum_{i\in I} z\cdot x_i, \quad \text{para todo } z\in K \text{ y}$$

$$\left(\sum_{i\in I} x_i\right)\cdot z = \sum_{i\in I} x_i\cdot z, \quad \text{para todo } z\in K$$

(5.4) Si $I = \emptyset$, entonces $\sum_{i\in I} x_i = 0$.

Si adoptamos (5.1) como una noción básica en lugar de la adición $x+y$ y consideramos $(5.2), (5.3)$ y $(k,\cdot)$ un monoide como axiomas, entonces podemos definir $x_1 + x_2$ como $\sum_{i\in I} x_i$, con $I = \{1,2\}$ y definir 0 por (5.4) dando lugar a que K es un semianillo.

Definición 5.1.2 *Un semianillo* K *es llamado completo si* $\sum_{i\in I} x_i$ *es un elemento de* K*, para cualquier conjunto de indices* I*, y se tienen los axiomas* $(5.2), (5.3)$ y $(k,\cdot)$ *un monoide.*

Ejemplo 5.1.3 $\beta = \{0,1\}$ *con las operaciones dadas en el ejemplo 5.1.1 es un semianillo completo.*

Definición 5.1.3 *Sea X un conjunto no vacio y sea K un semianillo conmutativo (para $x, y \in K$, $x \cdot y = y \cdot x$) no trivial* $(0 \neq 1)$.
Un K-subconjunto A de X es una función $A : X \longrightarrow K$.

Si $A : X \longrightarrow K$ es un K-subconjunto de X y los únicos valores que A toma son 0 y 1, entonces diremos que el K-subconjunto A de X es no ambiguo.

Como $0 \neq 1$ en K, los subconjuntos no ambiguos A de X pueden identificarse, en el sentido usual, con el subconjunto $\{x : A(x) = 1\}$ de X. En particular si $K = \beta = \{0, 1\}$, entonces todos los K-subconjuntos de X son no ambiguos.
$X : X \longrightarrow K$, $\emptyset : X \longrightarrow K$ y $x : X \longrightarrow K$ $(x \in X)$, definidos respectivamente por $X(x) = 1$, para todo $x \in X$, $\emptyset(x) = 0$, para todo $x \in X$ y

$$x(y) = \begin{cases} 1, & \text{si } y = x \\ \\ 0, & \text{si } y \neq x \end{cases} \qquad \text{son } K-\text{subconjuntos no ambiguos de } X.$$

Los K-subconjuntos no ambiguos x son llamados individuales.

Ahora centramos nuestra atención a las operaciones con K-subconjuntos. Para cualquier familia indizada $\{A_i : i \in I\}$ de K-subconjuntos de X definimos la Suma (o Unión) $\bigcup\limits_{i \in I} A_i : X \longrightarrow K$ por

$$\left(\bigcup_{i \in I} A_i\right)(x) = \left(\sum_{i \in I} A_i\right)(x) = \sum_{i \in I} A_i(x)$$

Esta definición no requiere comentarios si K es un semianillo completo. Ahora, si K no es completo asumiremos que la familia $\{A_i : i \in I\}$ es localmente finita, es decir, para cada $x \in X$, $A_i(x) \neq 0$ solo para un número finito de elementos $i \in I$. Si $I = \{1, 2, \ldots, n\}$, entonces usaremos la notación $A_1 \cup A_2 \cup \ldots \cup A_n$ ó $A_1 + A_2 + \ldots + A_n$ en lugar de $\bigcup\limits_{i \in I} A_i$ ó $\sum\limits_{i \in I} A_i$.

Definimos la multiplicación de un K-subconjunto A de X por un elemento $k \in K$ $kA : X \longrightarrow K$, por $(kA)(x) := k \cdot A(x)$.
Claramente, de las operaciones de multiplicación y unión, de sigue que:
$1 \cdot A = A$, $0 \cdot A = \emptyset$, $(k_1 \cdot k_2) \cdot A = k_1(k_2 A)$, $\left(\sum_{i \in I} k_i\right) \cdot A = \sum_{i \in I} k_i \cdot A$ y $k \cdot \left(\sum_{i \in I} A_i\right) = \sum_{i \in I} k \cdot A_i$.

La intersección $A \cap B$ de dos K-subconjuntos es definida por $(A \cap B)(x) := A(x) \cdot B(x)$. Esta también es válida si B es un K-subconjunto y A es un β-subconjunto $(\beta = \{0,1\})$, por simple consideración de A como un K-subconjunto no ambiguo. En este caso,

$$(A \cap B)(x) = \begin{cases} B(x) & ,\text{si } \ x \in A \\ 0 & ,\text{si } \ x \notin A \end{cases}$$

($x \in A$ y $A(x) = 1$ tienen el mismo significado)
Podemos observar que para cada K-subconjunto A de X tenemos que $A = \sum_{x \in X} A(x) \cdot x$. El lado derecho de esta expresión es llamada la expansión de A (en términos de individuales). Este es un diseño formal útil en la manipulación de K-subconjuntos. Por ejemplo $kA = \sum_{x \in X} k \cdot A(x) \cdot x$ y $A \cap B = \sum_{x \in X} A(x) \cdot B(x) \cdot x$

5.2 Monoides y Matrices

Sea $(S, .)$ un semigrupo y sean A, B K-subconjuntos de S. Nuestra primera tarea es definir el K-subconjunto $A \cdot B$ de S. Si A y B son los individuales x e y, entonces $x \cdot y$ es definda por la multiplicación en S. Como esperamos que $A \cdot B$ sea bilineal y tenemos que $A = \sum_{x \in S} A(x) \cdot x$, $B = \sum_{y \in S} B(y) \cdot y$, entonces $A \cdot B = \sum_{x \in S} A(x) \cdot B(y) \cdot xy = \sum_{z \in S} \sum_{x \cdot y = z} A(x) \cdot B(y) \cdot z$ sugiere la fórmula de convolución $(A \cdot B)(z) = \sum_{x \cdot y = z} A(x)B(y)$.

Esta fórmula puede ser usada ciertamente como una definición de $A.B$ cuando K es completo. De esta forma $A.B$ es bilineal, es decir,

$$\left(\sum_{i\in I} A_i\right) \cdot B = \sum_{i\in I} A_i \cdot B\ , \quad A\left(\sum_{i\in I} B_i\right) = \sum_{i\in I} A \cdot B_i \quad \text{y}$$

$(k \cdot A) \cdot B = k \cdot (A \cdot B) = A \cdot (k \cdot B)$. Más aún $A \cdot B$ es asociativa.

Observación 5.1 *Si M es un monoide, entonces el conjunto de todos los K-subconjuntos de M, K^M, es un semianillo (no necesariamente conmutativo).*

Sean P y Q conjuntos finitos. Un K-subconjunto A de $P \times Q$ será referido como una matriz de filas indizadas por los elementos de P, con columnas indizadas por los elementos de Q, y con entradas en K. Las entradas de la matriz $A(p,q)$ serán denotadas por A_{pq} y la matriz por $A = [A_{pq}]$. La adición de matrices está definida usando suma de K-subconjuntos. Así, si $A, B \in K^{P\times Q}$ (conjunto de todas las $P \times Q$ matrices), entonces $(A+B)_{pq} = A_{pq} + B_{pq}$.
Una nueva operación es la multiplicación. Dadas las matrices $A \in K^{P\times Q}$, $B \in K^{Q\times R}$ el producto $A \cdot B \in k^{P\times R}$ es definido por $(A \cdot B)_{pr} = \sum_{q\in Q} A_{pq} B_{qr}$.
Si $P = Q$, entonces $(K^{P\times P}, +, \cdot)$, donde $+$ y $\cdot$, son las operaciones antes definidas, es un semianillo con unidad 1_p definida por

$$(1_p)_{pp'} = \begin{cases} 1\ , & \text{si} \quad p = p' \\ 0\ , & \text{si} \quad p \neq p' \end{cases}$$

Si A es una $P \times Q$-matriz y P es un conjunto con un solo elemento, entonces A es llamada vector fila. Si Q tiene un solo elemento, entonces A es llamada vector columna.

5.3 $+-$ Algebras

Definición 5.3.1 *Sea* K *un semianillo conmutativo. Un álgebra sobre* K *(ó* K*-álgebra) es un conjunto* A *equipado con cuatro operaciones: dos binarias que asignan a cada par* $(a,b) \in A \times A$ *los elementos* $a+b$ *y* $a \cdot b$ *de* A*, una mixta que asigna a cada par* $(k,a) \in K \times A$ *el elemento* $k \cdot a \in A$ *y una operación que asigna a cada elemento de* A *un elemento nulitario* $\emptyset$ *de* A*. Cumpliendo los siguientes axiomas:*

- (3.1) $a+b=b+a$, *para todo* $a,b \in A$.
- (3.2) $a+(b+c)=(a+b)+c$, *para todo* $a,b,c \in A$.
- (3.3) $(k_1k_2)a = k_1(k_2a)$, *para todo* $k_1,k_2 \in K$, *para todo* $a \in A$.
- (3.4) $1a = a$, *para todo* $a \in A$.
- (3.5) $0a = \emptyset$, *para todo* $a \in A$.
- (3.6) $(k_1+k_2)a = k_1a + k_2a$, *para todo* $k_1,k_2 \in K$, *para todo* $a \in A$.
- (3.7) $k(a+b) = ka + kb$, *para todo* $k \in K$, *para todo* $a,b \in A$.
- (3.8) $a(bc) = (ab)c$, *para todo* $a,b,c \in A$.
- (3.9) $(a+b)c = ac + bc$, *para todo* $a,b,c \in A$.
- (3.10) $a(b+c) = ab + ac$, *para todo* $a,b,c \in A$.
- (3.11) $k(ab) = (ka)b = a(kb)$, *para todo* $k \in K$, *para todo* $a,b \in A$.

Como en el caso de los semianillos. Si $\{a_i : i \in I\}$, con I finito, es una familia de elementos de A, entonces la operación $a+b$ puede ser reemplazada por $\sum_{i\in I} a_i$ y los axiomas pueden ser reformulados.

Definición 5.3.2 *Sea* K *un semianillo conmutativo completo. Una* K*-álgebra* A *es llamada completa si* $\sum_{i\in I} a_i$ *es definida para cualquier familia* $\{a_i : i \in I\}$ *de elementos de* A.

Definición 5.3.3 *Una $+-$álgebra sobre K (ó K-$+-$álgebras) es una K-álgebra A con una operación unitaria a^+.*

La operación a^+ sirve para representar la suma infinita $a+a^2+a^3+\ldots+a^n+\ldots$ consecuentemente, si K es completo y A es una K-álgebra completa, entonces A se convierte en una K-$+-$ álgebra poniendo $a^+ = \sum_{n=1}^{\infty} a^n$.

Definición 5.3.4 *Sea A una K-$+-$álgebra. Un subconjunto no vacío B de A es llamado una sub-álgebra de A si para cualesquiera $b, b' \in B$ y $k \in K$, los elementos $b+b'$, $b \cdot b'$, kb y b^+ estan en B.*

De la definición 5.3.4, se sigue que la intersección de cualquier familia de sub-álgebras de A es también una sub-álgebra de A.

Definición 5.3.5 *Sea $B \subseteq A$, con A una K-$+-$álgebra. Llamaremos la clausura de B y la denotamos por $\overline{B}$ al conjunto de $\overline{B} := \cap C$, donde c recorre todas las sub-álgebras de A que contienen a B.*

Sea K un semianillo conmutativo completo y sea S un semigrupo. El conjunto K^S de todos los K-subconjuntos de S es un K-álgebra completa con las operaciones $\sum_{i \in I} A_i$, $k \cdot A$ y $A \cdot B$ definidas como antes. Además, con $A^+ = \sum_{n=1}^{\infty} A^n$, entonces K^s es también un K-$+-$álgebra.

Estamos interesados en una sub-álgebra la cuál es la clausura de la clase de todos los individuales de S y la que denotamos por $Rat_K S$. Los K-subconjuntos de S pertenecientes a $Rat_K S$ son llamados regulares.

5.4 K - Autómatas

Sean $\sum$ un alfabeto finito y K un semianillo conmutativo. Un K-Autómata es un quíntuple $M_K := (Q, \sum, I, E, T)$, donde Q es un conjunto finito, I y T son K-subconjuntos de Q y E es un K-subconjuntos de $Q \times \sum \times Q$.

Análogamente, como en los A.F's. podemos asociar a un K-Autómata M_K un diagrama de transición. Si $E(p,r,q) = k \neq 0$, entonces diremos que el arco $p \xrightarrow{kr} q$ está en M_K y kr es la etiqueta de la arco.
Como en el caso de los A.F's. consideramos las trayectorias $c : p \longrightarrow q$; si c es la trayectoria

$$p \xrightarrow{k_1 r_1} q_1 \longrightarrow \ldots \longrightarrow q_{n-1} \xrightarrow{k_n r_n} q \ ,$$

entonces su etiqueta es $|c| = ks$, con $k = k_1 \ldots k_n$, $s = r_1 r_2 \ldots r_n$ y su longitud es n.

El comportamiento de M_K es el K-subconjunto de $\sum^*$, definido por $||M_K|| = \sum_{p,q \in Q} \sum_c (I(p))\ |c|\ (T(q))$, con c recorriendo todas las trayectorias $c : p \longrightarrow q$.

Debido a que para cada $s \in \sum^*$, existe solamente un número finito de trayectorias con etiqueta ks, $k \in K$, la sumatoria es localmente finita y en consecuencia $||M_K||$ está bien definida, sin asumir que K sea un semianillo completo. Las únicas trayectorias de longitud cero son las trayectorias triviales $q \longrightarrow q$ con etiqueta θ. Por lo tanto $||M_K||\ (\theta) = \sum_{q \in Q} (I(q))(T(q)) = IT$, donde IT es el producto del vector fila I por el vector columna T.

El K-subconjunto E de $Q \times \sum \times Q$ es una aplicación, como es sabido, $E : Q \times \sum \times Q \longrightarrow K^{\sum}$, así escribimos $E(p,r,q) = Epq(r)$ con lo cuál Epq es un K-subconjunto de $\sum$. Por tanto E puede ser visto como una matriz $E : Q \times Q \longrightarrow K^{\sum}$, llamada matriz de transición de M_K. Ahora, como cada K-subconjunto de $\sum$ puede ser visto como un K-subconjunto de $\sum^*$ (con valor 0 sobre cada $s \notin \sum$), entonces E puede ser visto también como una función $E : Q \times Q \longrightarrow K^{\sum^*}$, es decir, como una $Q \times Q$ matriz con entradas en $K^{\sum^*}$.

Como $K^{\sum^*}$ es un semianillo, entonces podemos introducir la multiplicación de matrices; así, para $n \in I\!N$, las matrices $E^n : Q \times Q \longrightarrow k^{\sum^*}$ pueden ser definidas, con $E^o = 1_Q$, $E^1 = E$, ya que $E^n pq(s) = 0$, si $|s| \neq n$ se sigue que la familia $\{E^n pq,\ n \in I\!N\}$ es localmente finita y podemos definir

$E^*pq = \sum_{n=0}^{\infty} E^n pq$, de acá resulta la matriz $E^* : Q \times Q \longrightarrow K^{\sum^*}$ $(E^* = 1_Q + E + E^2 + E^n + \ldots)$ llamada matriz de transición extendida de M_K. Para cada $s \in \sum^*$ consideremos la matriz $E^*(s) = [E^*pq(s)] \in K^{Q\times Q}$, si $S = r_1 r_2 \ldots r_n$, entonces $E^*(s) = E^n(s) = (E(r_1))(E(r_2))\ldots(E(r_n)) = (E^*(r_1))(E^*(r_2))\ldots(E^*(r_n))$.

Proposición 5.4.1 *Para cualesquiera $p, q \in Q$ el K-subconjunto E^*pq es la suma de todas las etiquetas de trayectorias $c : p \longrightarrow q$ en M_K.*

Prueba. Es suficiente probar que para cada $n \in I\!N$, el K-subconjunto $E^n pq$ es la suma de todas las etiquetas de trayectorias $c : p \longrightarrow q$ de longitud n. Para $n = 0$ esto es claro ya que $E^o pq = 1$ si $p = q$ y $E^o pq = 0$ en otro caso, para $n = 1$ el resultado se sigue del hecho de que $E'pq = Epq$ y de la definición de Epq. Para $n > 1$ el resultado se sigue inductivamente de la formula $E^n pq = \sum_{r\in Q} Epr E^{n-1} rq$.

□

Corolario 5.4.1 *El comportamiento de M_k es $||M_k|| = I \; E^* \; T$, con I considerado como un vector fila y T como un vector columna.*

5.5 Ecuaciones Lineales

Para calcular el comportamiento de un K-Autómata M_K introducimos un método esencialmente algebraico. Este método depende del estudio de las ecuaciones lineales.

Consideremos un sistema de n ecuaciones con n incognitas $X_i := \sum_{j=1}^{n} E_{ij} X_j + T_i$, $1 \leq i \leq n$, donde $E_i j$ y T_j son K-subconjuntos de $\sum^*$ y X_i son las incognitas. En notación matricial el sistema toma la forma (5.1) $X = EX + T$, donde X y T son vectores columna.

Proposición 5.5.1 *El vector $X = E^*T$ es una solución del sistema* (5.1).

Prueba. Escribiendo 1_n como la matriz identidad $n \times n$ tenemos $E^*T = (1_n + EE^*)T = E(E^*T) + T$.

$\square$

Proposición 5.5.2 *Si* $E_{ij} \subset \sum^+$*, para todo* $1 \leq i,\ j \leq n$*, entonces el sistema* (5.1) *tiene una única solución.*

Prueba. Sean X e Y dos vectores de K-subconjuntos de $\sum^*$. Veamos que $X_i(s) = Y_i(s)$, para todo $1 \leq i \leq n$ y todo $s \in \sum^*$. Para esto procederemos por inducción sobre la longitud de s ($|s|$).
Si $|s| = 0$, es decir, si $s = \theta$, entonces $E_{ij}(\theta) = 0$, por tanto $X_i(\theta) = T_i(\theta) = Y_i(\theta)$. Ahora, supongamos que la proposición es válida para $s \in \sum^*$, con $|s| > 0$, entonces $X_i(s) = \sum_j (E_{ij}X_j)(s) + T_i(s) = \sum_j \sum_{uv=s} (E_{ij}(u))(X_j(v)) + T_i(s)$. Análogamente, $Y_i(s) = \sum_j \sum_{uv=s} (E_{ij}(u))(Y_j(v)) + T_i(s)$. Como $E_{ij}(u) = 0$, siempre que $u = \theta$, podemos excluir el caso $u = \theta$, $v = s$ de la sumatoria y considerar solamente el caso en que $|v| < |s|$. Como $X_j(v) = Y_j(v)$, por la hipotesis de inducción, entonces tenemos que $X_i(s) = Y_i(s)$. Luego, la solución del sistema (5.1) es única.

$\square$

Proposición 5.5.3 *Si* $E_{ij} \subset \sum^+$*, para todo* $1 \leq i, 1 \leq n$ *y* $E_{ij}, T_{ij} \in Rat_K\sum^*$*, para todo* $1 \leq i, j \leq n$*, entonces la única solución de* (5.1) *satisface que* $X_1, X_2, \ldots, X_n \in Rat_K\sum^*$.

Prueba. Si $n = 1$, entonces $X_1 = E_{11}\ T_1 = T_1 + E_{11}T_1$, es una solución y está en $Rat_K\sum^*$. Ahora, procediendo por inducción, asumimos $n > 1$ y escribimos la n-ésima ecuación como:

$$X_n = E_{nn}X_n + C + T_n, \quad \text{con} \quad C = E_{n1}X_1 + \ldots + E_{n,n-1}\ X_{n-1}.$$

Debido a que $E_{nn} \subset \sum^+$, se sigue de las dos proposiciones anteriores que $X_n = E_{nn}^*(C + T_n)$. Sustituyendo ésta expresión en las $n-1$ primeras ecuaciones obtenemos el sistema (5.2) $X = E'X + T'$ de $n-1$ ecuaciones con $n-1$ incognitas, con $E'_{ij} = E_{ij} + E_{in}E_{nn}^*E_{nj}$ y $T'_i = T_i + E_{in}E_{nn}^*T_n$. Así, el sistema (5.2) satisface que $E'_{ij}, T'_i \in Rat_K\sum^*$, para $1 \leq i, j \leq n$ y $E_{ij} \subset \sum^+$, para $1 \leq i, j \leq n$ y de la hipótesis de inducción su única solución

$X_1, X_2, \ldots, X_{n-1}$ está en $Rat_K\sum^*$. Sustituyendo en $C = E_{n1}X_1 + \ldots + E_{n,n-1}\ X_{n-1}$ obtenemos que $C \in Rat_K\sum^*$ y en consecuencia $X_n \in Rat_K\sum^*$. $\square$

El procedimiento de la prueba de la proposición 5.5.3, dá un algoritmo para expresar las soluciones $X_1, X_2, \ldots, X_n$ como expresiones regulares en los coeficientes E_{ij}, T_i. Estas expresiones dependen del número de ecuaciones.

Sea $M_K = (Q, \sum, I, E, T)$ un K-Autómata y asumamos que $Q = \{1, 2, 3, \ldots, n\}$. Sea E la matriz de transición correspondiente a M_K y pongamos $X_i = |(Q, i, T)|$, entonces por el colorario 5.4.1. $X_i = (E^*T)_i$; así $X = E^*T$.

Ya que $E_{ij} \subset \sum$, la condición $E_{ij} \subset \sum^+$, para todo $1 \leq i, j \leq n$ se satisface y así X es la única solución del sistema de ecuaciones $X = EX + T$. Ahora como todos los coeficientes estan en $Rat_K\sum^*$, entonces $X_1, X_2, \ldots, X_n$ estan en $Rat_K\sum^*$. Ya que $||M_K|| = \sum_{i=1}^{n} I_i X_i$, donde $I_i = I(i)$ es el valor de I en el estado i, se sigue que $||M_K|| \in Rat_K\sum^*$. Así tenemos el siguiente teorema.

Teorema 5.5.1 *Sea* $M_K = (Q, \sum, I, E, T)$ *un* K*-Autómata, con* $Q = \{1, 2, \ldots, n\}$ *y con matriz de transición* E*. Entonces* $||M_K|| = \sum_{i=1}^{n} I_i X_i$ *se verifica con la única solución* $X_1, X_2, \ldots, X_n$ *del sistema de ecuación* $X = EX + T$.

Ejemplo 5.5.1 *Consideremos el Autómata cuyo diagrama de transición es dado en la figura* 5.1.
Las ecuaciones son

$$X_1 = rX_1 + sX_2$$
$$X_2 = (r+s)X_2 + \theta$$

Resolviendo la segunda ecuación tenemos que $X_2 = (r+s)^*$*, así la primera ecuación se transforma en* $X_1 = rX_1 + s(r+s)^*$*. Luego* $X_1 = r^*s(r+s)^*$ *es el comportamiento del Autómata.*

Ejemplo 5.5.2 *Consideremos el Autómata cuyo diagrama de transición es dado en la figura* 5.2.
Las ecuaciones son $X_1 = rX_1 + sX_2 + \theta$
$$X_2 = sX_1 + rX_2$$

De la segunda ecuación obtenemos que $X_2 = r^*sX_1$*, luego* $X_1 = (r + sr^*s)X_1 + \theta$*. Por tanto* $X_1 = (r+sr^*s)^*$ *es el comportamiento del Autómata.*

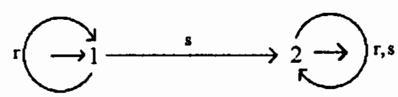

Figura 5.1:

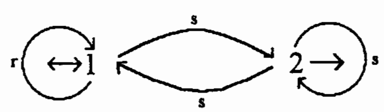

Figura 5.2:

Bibliografía

[1] Beauquier, J. and M. Nivat, "Aplication of formal language theory to problems of Security and Synehronization, in formal language theory-perpective and open problems". R.V. Book, ed., Academic press, New York, 1980, p.p.407-454.

[2] Park, D. "Concurrency and Automata on infinite Secuences, in theoretical Computer Science". lecture Notes in Computer Science 104,1983, Springer-Verlas, New York, p.p.167-183.

[3] Eilenberg, S. "Automata, languages, and Machines". Vol. A, 1974, Academic press, New York.

[4] Harrison, M.A. "Introduction to Switchins and Automata theory". 1965, Mc. Graw-Hill, New York.

[5] Hopcroft, J.E. and Ullman, J.D. "Introduction to Automata theory, languages, and Computatión". 1979, Addison-Wesley, Readins, M.A.